

REVIEW ARTICLE

AI Safety Requirements: A Perspective From the Automotive World

Sangeeth Kochanthara^{1,*}, Loek Cleophas^{1,a}, Yanja Dajsuren^{1,b}, Mark van den Brand^{1,c}¹Eindhoven University of Technology, Eindhoven, The Netherlands^aEmail: l.g.w.a.cleophas@tue.nl^bEmail: y.dajsuren@tue.nl^cEmail: m.g.j.v.d.brand@tue.nl**ABSTRACT**

Artificial Intelligence (AI) is advancing at a pace never seen before. The technology is now being rapidly adopted at scale in all potential cross sections of society, while the safety implications are not being considered. This work presents a systematic literature review on the elicitation of safety requirements on a combination of AI and traditional software from the automotive domain. We focus on the era before Generative Pretrained Transformer (GPT). Automotive is one of the industries that has adopted AI at scale with technologies such as adaptive cruise control and lane assist, which are leading to autonomous driving. There are many parallels to the current rapid development in AI in the automotive world. These include the move towards automated driving, high competition, frequent release cycles and the price-sensitive nature. These characteristics set the automotive industry apart from other safety-critical industries. Ensuring safety in the automotive industry starts with safety requirements. A plethora of safety requirements elicitation processes and techniques for the automotive domain have been proposed. To the best of our knowledge, no study characterizes them. This article characterizes the state-of-the-art in eliciting safety requirements via a systematic literature review. We selected 102 primary studies from 2097 related articles. We identified and compared nine distinct processes for safety requirement elicitation. We constructed taxonomies of 38 distinct techniques used to conduct the different steps in each of the processes. This article can act as a guide and ‘cheat sheet’ for beginners and practitioners to choose processes and techniques for their projects. For researchers, this study provides an overview of the field, research gaps and future research opportunities.

ARTICLE DATA**Article History**

Received 28 August 2025

Revised 5 December 2025

Accepted 5 January 2026

Keywords

AI safety

Safety

Gen-AI

Automotive software
engineering

Safety engineering

Functional safety

Safety requirement elicitation

Safety of intended functionality

ISO 26262

ISO 21448

1. INTRODUCTION

Artificial Intelligence (AI), especially Generative AI (Gen-AI), is rapidly getting adopted across domains while its societal impact especially on the safety aspects is not well studied [1]. A domain that has strict safety standards and has seen adoption of AI at scale is automotive. With an estimated 1.4 billion cars on the road and a direct market capitalization of 3 trillion dollars¹, it has seen adoption of AI before the GPT showed its disruptiveness². This article focuses on how safety of automotive software and the electronics that run the

software was handled pre-GPT era. In the automotive world, these safety aspects are referred to as *functional safety* [2] and *safety of intended functionality* [3].

There is an inadequacy in safety of automotive software and electronics that run it, evidenced by software and related defects leading to the recall of 7.5 million and 5.5 million vehicles in the United States in 2020 and 2021 respectively. These recalls dominated the top reasons for recalls both in the number of recalls and the number of affected vehicles³. Another example is the infamous Uber automated driving vehicle crash, which

*Corresponding author. Email: s.kochanthara@tue.nl

© 2026 Eindhoven University of Technology. Published by Athena International Publishing B.V.

This is an open access article distributed under the CC BY-NC 4.0 license (<https://creativecommons.org/licenses/by-nc/4.0/>).

¹ <https://www.bloomberg.com/opinion/articles/2021-12-29/cars-are-suddenly-worth-3-trillion-and-it-s-not-all-tesla>

² https://timelines.issarice.com/wiki/Timeline_of_ChatGPT

³ https://www.recallmasters.com/wp-content/uploads/2021/05/Infographic_2020_smaller.png

led to the death of a pedestrian⁴. NTSB's⁵ investigation found that software and inadequate safety culture in developing software and related systems were among the reasons for this crash⁶. Such inadequacies in ensuring safety can cause fatalities, economic losses, brand damage, destruction of traffic infrastructure, and indirect (economic) losses. A fundamental step for safer automotive software systems is incorporating safety into the automotive product life cycle right from the requirement elicitation stage.

There are many kinds of safety requirements based on the underlying cause of the requirement. For instance, safety requirements caused by deficiencies in specified driving behavior [4], safety requirements relating to failure or malfunction of components (also referred to as *functional safety* [2]), safety requirements resulting from functional insufficiencies of the intended functionality (also referred to as *safety of intended functionality* [3]). This article focuses on the latter two types of safety requirements, in the context of systems, software, and hardware that runs the software. In the rest of this article, safety requirements refer to these two types.

Our *goal* is to characterize the state-of-the-art in safety requirement elicitation processes and techniques in the automotive context via a Systematic Literature Review (SLR) in the pre-GPT era (until mid-2021).

Secondary studies on safety requirement elicitation focused on: (a) the broader safety-critical systems domain [5]; (b) practices and challenges in the development of embedded systems [6]; (c) integration between requirement and safety engineering [7]; (d) managing safety in mobile robotic systems [8]; and (e) security in the context of product lines [9]. However, to our knowledge, there are no secondary studies on safety requirement elicitation for automotive systems.

A secondary study on safety requirement elicitation for automotive systems can consolidate dispersed knowledge and provide structured insights into what processes and techniques are most effective for capturing safety needs in this uniquely complex and high-stakes domain. Unlike other safety-critical fields, automotive systems depend on the operator (driver) who is not trained to handle safety-critical issues. Other safety-critical domains like aviation, space, and nuclear always rely on highly trained operators. Furthermore, the industry is moving towards automated driving, thereby eliminating the operator from the loop. Thus, introducing the scenario of autonomous systems working among humans and non-automated driving vehicles.

The secondary study can also help current industry practice because without synthesized evidence on best-known elicitation practices, organizations risk repeating mistakes, ultimately impacting safety assurance, regulatory compliance, and timely development of reliable vehicle software.

This article presents the first SLR on safety requirement elicitation for automotive software and systems. Specifically, we focus on the technical aspects of safety requirement elicitation, including different processes, their steps, techniques to perform these steps, and use cases for each process.

We translate our goal into the following research questions:

RQ1: What processes are used for or applicable to safety requirement elicitation in the automotive domain?

By answering RQ1, we intend to identify, summarize, and compare the various safety requirement elicitation processes.

RQ2: What techniques are used for safety requirement elicitation in the automotive domain?

In RQ2, we dive deeper into the techniques (used for different steps in the processes) and compare and taxonomize them.

Our primary contributions are:

- A summary, analysis and synthesis of the body of knowledge in safety requirement elicitation for the automotive domain through an SLR over 102 primary studies.
- Empirical validation of the need for such an SLR via a systematic qualitative analysis.
- Taxonomies of techniques for safety requirement elicitation in the automotive domain.

This study targets practitioners and researchers alike. For researchers, this study outlines the automotive safety requirements elicitation research field, research gaps and future research opportunities. For practitioners, this article provides a concise guide toward choosing one or more processes and techniques for safety requirement elicitation in their projects.

The rest of this article is structured as follows. [Section 2](#) presents this study's planning phase and design choices. [Section 3](#) describes an overview of the research landscape via qualitative metrics. [Sections 4 and 5](#) answer our research questions and discuss our findings. [Section 6](#) elaborates implications of this study for research and practice, while [Section 7](#) presents validity threats. Related work is outlined in

⁴ <https://www.nts.gov/investigations/Pages/HWY18MH010.aspx>

⁵ National Transportation Safety Board (NTSB) is a U.S. government agency for civil transportation accident investigation.

⁶ <https://www.nts.gov/investigations/accidentreports/reports/har1903.pdf>

Section 8. Finally, **Section 9** concludes the article. Note that in the rest of the article the terms AI and ML are used interchangeably to denote the same underlying set of technologies.

2. STUDY DESIGN

The different steps in conducting an SLR can be organized into three phases: planning, conducting and reporting [10]. This section primarily discusses the study's planning phase and our design choices in detail. Reporting includes drawing conclusions, considering threats and disseminating results which are covered in later sections of the article.

The planning phase of this study is divided into the following 5 stages (based on various guidelines [10,11,12,13,14,15]):

- Evaluate the *need for this SLR* (Garner et al. [11]);
- Form a *search strategy* (Kitchenham et al. [10], Petticrew et al. [12], and Petersen et al. [13]);
- Create a *primary studies' selection* procedure (Kitchenham et al. [10]);
- Identify *quality assessment* criteria for the primary studies (Kitchenham et al. [10], Tiwari et al. [14], and Wieringa et al. [15]); and
- *Extract and synthesize data* and insights from primary studies (Kitchenham et al. [10]).

The rest of this section explains each of these stages in detail.

2.1. Need for SLR

To evaluate the need for this study, first we conduct an initial search for secondary studies, followed by a qualitative empirical evaluation.

For the initial search, we use the search string: “functional safety” AND (automotive* OR vehic*) AND (“systematic map” OR “systematic mapping” OR “systematic literature”). The search string is created by combining the topic (“functional safety”), domain (automotive* OR vehic*) and the kind of studies we are looking for (“systematic map” OR “systematic mapping” OR “systematic literature”). Note that we used the term “functional safety” instead of “safety” since the former resulted in a low signal-to-noise ratio. *Functional safety* refers to safety concerning (malfunction of) software and related systems. The term is universally adopted in the automotive domain [2,3].

Our Google Scholar search (on 10 November 2020) did not identify any secondary study that focuses on safety requirement elicitation in the automotive domain. However, we found an SLR by Martins et al. [5] on

approaches to elicit, model, specify and validate safety requirements in the broader context of safety-critical systems. In this SLR, automotive formed 5.29% (8 out of 151) of all the primary studies [5]. Given the study's broader scope and rigor, we assumed that primary studies until 2013 are covered (since the primary studies search was conducted in 2014). We consider this study by Martins et al. [5] as a basis to evaluate the need for our SLR.

We evaluate the need in two steps: (1) An initial analysis of the trend in the number of relevant publications since 2014 as shown in Fig. 1, which indicates a positive trend; and (2) A systematic approach for qualitative empirical evaluation, presented in the rest of this section.

We use the 3PDF framework [11] to validate the relevance of conducting this SLR empirically. The 3PDF framework is an empirical framework consisting of three sequential phases. A positive outcome of all three phases ascertains the need for an SLR. Note that the 3PDF framework [11] was originally designed to address the relevance of repeating an existing SLR. Meanwhile, we use it to identify the significance of this study using the SLR by Martins et al. [5] as a basis. In the rest of this section, we explain the execution of the 3 phases of the 3PDF framework.

- *Phase 1: Assess currency*, aims to identify whether the research questions are already answered by available evidence or no longer considered relevant [11,16]. This phase consists of the following three *yes/no* questions and is passed if and only if **all** of them are answered positively.

1. *Does the published SLR still address a current question?*

Yes. The study by Martins et al. [5] focuses on safety requirement elicitation for safety-critical systems with ≈5% of their primary studies from the automotive domain.

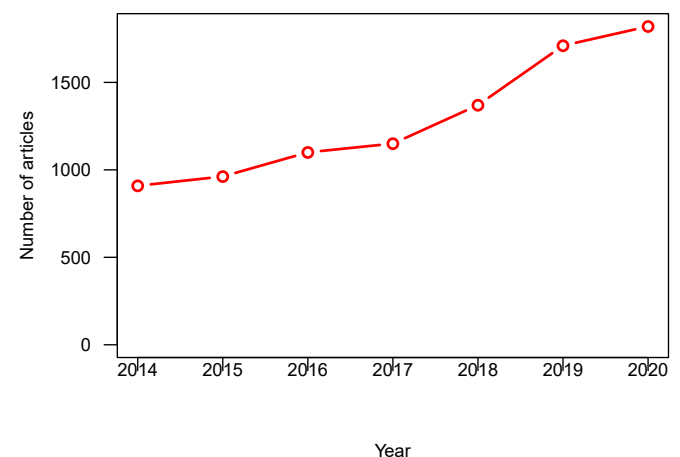


Figure 1. Number of articles in the result of Google Scholar search of query: “functional safety” AND (automotive* OR vehic* OR driv* OR automobile* OR AUTOSAR OR car). The query was performed for articles until and including July 2021.

2. Has the SLR had good access or use?

Yes. The prior SLR [5] has a yearly average citation count of 15.5 (with a total citation count of 62 when checked via Google Scholar on 10 November 2020). Citation count is a measure of access, use and relevance [17,18]. In the software engineering domain, a yearly average citation count of 6.82 or above is judged as having had good access or use [17].

3. Has the SLR used valid methods and was it well-conducted?

Yes. Martins et al. [5] followed the well-established guidelines of Kitchenham [10] for conducting the SLR and the work has been published in a top-tier peer-reviewed journal from the domain.

Since all the questions are answered *yes*, we proceed to the next phase.

- *Phase 2: Identify relevant new methods, studies and other information.* This phase focuses on whether new information is not covered by the existing study, including study design, evidence synthesis and new primary studies. The phase consists of two *yes/no* questions and proceeding to the next phase needs **at least one** question to be answered positively.

1. Are there any new relevant methods (in conducting the SLR)?

Yes. In addition to the approaches used in the study design of the prior SLR [5], we add the following new methods: (a) full-text search; and (b) both forward and backward snowballing.

2. Are there any new studies or new information?

Yes. The period of our initial search is between the end of Martins et al.'s study (2014) and 2020. This ensures that every primary study we considered is not included in their research. Furthermore, this period experienced landscape shifts in the automotive industry with automated and connected driving enabled by software-intensive sub-systems [19].

Both the questions are answered with *yes*; therefore, we advance to the next phase.

- *Phase 3: Assess the effect of updating the review.* This phase aims to assess whether the information from the new primary studies influences the conclusion compared to the base SLR. A **Yes** answer to **any** of the two following questions empirically validates the need for a new study.

1. Will the adoption of new methods (for conducting the SLR) change the findings, conclusions, or credibility?

Maybe. The new methods that we adopted were full-text search and snowballing. Our initial set of primary studies is disjoint from the set of primary studies considered in the prior SLR [5]. Also, snowballing has resulted in identifying new techniques

and wider adoption of some of the processes and techniques for safety requirement elicitation, which were not evident otherwise.

2. Will the inclusion of new studies, information or data change findings, conclusions, or credibility?

Yes. Only 5.29% of primary studies in Martins et al. [5] are from the automotive domain. We scope our work specifically to the automotive domain. This makes a direct comparison of our study with theirs inaccurate. Also, the study does not differentiate or taxonomize processes and techniques or present challenges specific to the automotive context.

Thus, the execution of the 3PDF framework empirically establishes the need for our SLR.

2.2. Search Strategy

Our search strategy consists of identifying search keywords and multiple iterations to compose a search string followed by automatic search. We perform both forward and backward snowballing to widen the set of primary studies beyond the initial search.

The search string was constructed from two sets of strings, one for scoping: (*automotive, vehicle, vehicular, drive, driving*) and another related to the intervention: (*functional safety, hazard, accident, risk*). The final search string was formed by iterative refining (via piloting) to reduce the amount of noise while covering as much relevant literature as possible. The following search string was formed after several iterations:

The term "*functional safety*" is searched within keywords, title, and abstract *AND* the following terms:

(*automotive OR vehicle OR vehicular OR drive OR driving*)
AND
(*hazard OR risk OR accident*)

were searched in the full text of publications.

To identify and compose the search string, we use the PICOC (Population, Intervention, Comparison, Outcome, Context) method [10,12,13] as detailed below.

- *Population:* peer-reviewed publications describing safety requirement elicitation processes and techniques as well as application of such approaches to the automotive domain [10,12,13].
- *Intervention:* processes or techniques for safety requirement elicitation [10,12].
- *Comparison:* compare the different processes and techniques of safety requirement elicitation by means of identifying the different strategies used, and their context of application [10,12,13].

- **Outcome:** safety requirement elicitation process, different stages in the processes, techniques used to conduct each stage, and the following aspect of each process/technique: (a) context of use, abstraction level of application, and applicable components [10,12,13].
- **Context:** any phase in the automotive product life cycle that comprises safety requirement elicitation [10].

We use the same search databases as in the related studies [5,7]. The databases included are IEEE Xplore, ACM Guide to Computing Literature, ScienceDirect, and SpringerLink. Except for SpringerLink, automatic search is directly performed in the corresponding database. Since SpringerLink does not have a feature for the intended search string, we used broader search criteria (searching in the whole body of publications rather than title, tags, and abstract), with which a bibliography is retrieved. A further refined search is performed within this bibliography using the reference manager Mendeley.

Once the initial set of primary studies is finalized based on full-text reading, we applied snowballing to gather additional studies. We applied the guidelines by Wohlin et al. [20] to conduct backward and forward snowballing. For backward snowballing, we checked the references of primary studies (using titles only) until no new studies were found. Likewise, for forward snowballing, we looked at the articles (titles only) citing our primary studies until no further studies were found. For forward snowballing, we used the 'cited by' feature of Google Scholar and went through the citations to every primary study. The number of studies considered in each of the steps mentioned above is presented in Fig. 2.

2.3. Study Selection

We create inclusion-exclusion criteria tailored to focus on the technical aspects of safety requirement elicitation, which is the focus of this study. We excluded studies on other dimensions of safety requirement elicitation. Some examples are: (a) social and human-related factors that play a role in eliciting requirements like meetings,

reviews, communication among different parties; (b) a combination of technical, social, and human-related factors; (c) processes and techniques that merge safety requirement elicitation with requirement elicitation for other quality attributes like security; and (d) influences of agile and develops processes on safety requirements elicitation.

Our inclusion and exclusion criteria are as follows:

Inclusion criteria:

- 11 Any study that presents, compares, or discusses approaches (techniques, models, frameworks, methods, processes, or methodologies) to (help) elicit safety requirements, either used in or usable for the automotive domain.
- 12 Studies relating to safety requirements in the context of safety analysis, hazard analysis, or safety-critical standards from the automotive domain.

The **exclusion criteria** cover secondary studies; articles that are not written in English; non-peer-reviewed articles (gray literature); short articles (< 4 pages); studies below a quality threshold of 50% according to the quality assessment criteria detailed in Section 2.4 below; and studies that do not explicitly specify or are not from the automotive domain.

To ensure reproducibility, we conducted an inter-rater agreement. Before the first author selected primary studies, the rest of the authors evaluated the selection criteria. To assess the quality of the selection process, the second and third authors independently used the selection criteria on two disjoint random samples of the initial set of studies. The first author independently evaluated these two sets of studies employing the same criteria, resulting in the inter-rater agreement measured to 0.8 and 1 with the second and third authors, respectively, according to Cohen's kappa statistics [21]. This shows the highest level of inter-rater agreement in both cases⁷. Each disagreement between two researchers was discussed and resolved with the intervention of a third researcher.

We followed a five-step study selection procedure as presented in Fig. 2. We incrementally apply the inclusion-exclusion criteria in steps 1, 3, 4 and 5.

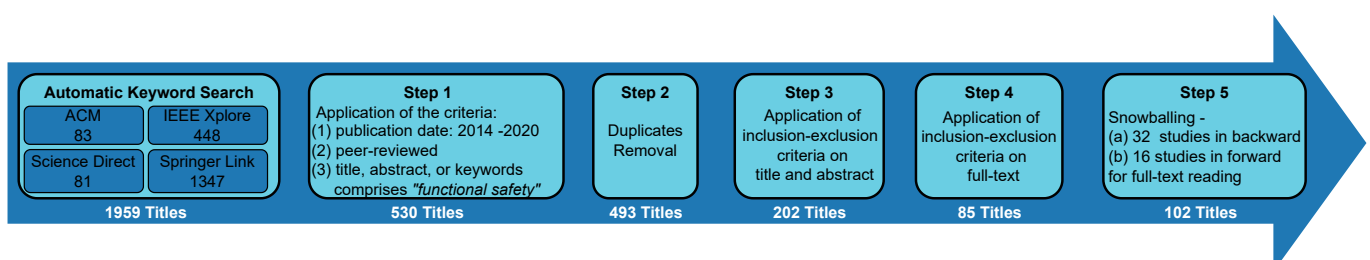


Figure 2. Procedure to select primary studies.

⁷ Since Cohen's Kappa statistic being at least 0.80 is considered best agreement [22,23].

2.4. Quality Assessment

Quality assessment of primary studies is crucial (i) “to investigate whether quality differences provide an explanation for differences in study results”; (ii) as a “means of weighting the importance of individual studies when results are being synthesised”; and (iii) “to guide recommendations for further research” [10].

We derived the quality assessment criteria from the guidelines of Kitchenham et al. [10], Tiwari et al. [14], and Wieringa et al. [15], as summarized in the first column of Table 1. We chose those questions from the guidelines that apply to our list of primary studies. For example, the question “Was there any control group present with which the treatments can be compared” [14] does not apply to studies that present the application of a requirement elicitation technique to an automotive component.

All the questions that form our assessment criteria have three possible answers “Yes”, “Partially,” and “No,” with a score of 1, 0.5, and 0, respectively. The score of each primary study is the sum of scores for every pertinent question (see Table 1). We use this scoring method to gauge the primary studies’ credibility, completeness, and relevance.

2.5. Data Extraction and Synthesis

We iteratively created a digital data extraction form. We created an initial set of attributes to be extracted from the primary studies and applied this to 10% of the initial set of primary studies. This form was iterated based on data synthesis at 30%, 50%, and 70% (of the initial set of primary studies) based on the categories and information emerging from data extraction. We applied a backward pass on the prior studies in cases where extra attributes were added to the data extraction form during the process. Finally, the following categories of data were extracted from primary studies:

Percentage	Yes	Partially	No
Aim clearly presented	100%	0%	0%
Approach clearly explained	83%	17%	0%
Clarity of application context	31%	63%	6%
Threats to validity taken into consideration	6%	1%	93%
Presence of discussion on results	46%	31%	23%
Limitations/scope discussed	6%	9%	85%
Related work discussed	64%	27%	9%

Table 1. Quality assessment summary of primary studies. The bold face part shows two aspects that only a few articles report.

- *Administrative information:* Article ID; Title; and Source.
- *Literature characteristics:* Authors; Year; Venue type (journal, symposium, conference, or workshop); Venue;
- Data pertaining to RQ1: *What processes are used for or applicable to safety requirement elicitation in the automotive domain?*
 - What process(es) are employed, compared, or discussed?
 - What is the motivation or reason to choose a specific process (or how a process compares with other processes)?
 - What are the steps followed in executing the process?
 - Which component or setting is the process applied to?
- Data related to RQ2: *What techniques are used for FSR elicitation in the automotive domain?*
 - What are the techniques employed, compared, or discussed?
 - Which high-level step (of a process) is accomplished using the specific techniques used or discussed?
 - What is the motivation or reason to choose a specific technique (comparison among techniques)?
 - Which component or setting is the technique applied to?

The data extraction form is a table with one column for each of the above categories and a row for each article.

Data synthesis was performed after aggregating the information collected using digital forms. The data synthesis is achieved by cross-reading each column to answer the research questions.

3. CHARACTERISTICS OF PRIMARY STUDIES

Our study selection process resulted in 102 primary studies [P1,P2,P3,P4,P5,P6,P7,P8,P9,P10,P11,P12,P13,P14,P15,P16,P17,P18,P19,P20,P21,P22,P23,P24,P25,P26,P27,P28,P29,P30,P31,P32,P33,P34,P35,P36,P37,P38,P39,P40,P41,P42,P43,P44,P45,P46,P47,P48,P49,P50,P51,P52,P53,P54,P55,P56,P57,P58,P59,P60,P61,P62,P63,P64,P65,P66,P67,P68,P69,P70,P71,P72,P73,P74,P75,P76,P77,P78,P79,P80,P81,P82,P83,P84,P85,P86,P87,P88,P89,P90,P91,P92,P93,P94,P95,P96,P97,P98,P99,P100,P101,P102]. This section presents an overview of the publication landscape, quality, and a

preliminary analysis of the primary studies. We analyze the publication trend across venues. We also classify the studies based on their domain and on whether the study is a contribution from industry, academia, or both.

Quality assessment of primary studies shows that most existing studies do not report limitations and scope of their solution. We assessed the quality of each study according to the criteria summarized in Table 1. On application of our quality assessment criteria, we found that only a few articles (at least partially) report the following two aspects (highlighted with boldface in Table 1): (1) threats to validity, taken into account in 7% (7 out of 102) of primary studies; and (2) limitations, discussed in 15% (15 out of 102) primary studies. The first observation is not surprising since only a few studies (4 out of 102) report empirical analyses. However, with a few studies reporting scope or limitations makes the reuse and replication of a majority of studies difficult. Our advice for future articles is to explicitly state the limits and scope of proposed solution.

Quality assessment of primary studies: Most existing studies do not report limitation and scope, further limiting our ability to reuse. We advise future studies to report it.

Most studies in safety requirement elicitation are published at conferences. We classified studies based on the type of venue as shown in Fig. 3a. Most of the primary studies (66 out of 102) are published at conferences and symposiums. Twenty studies are published in workshops and sixteen in journals.

The publication landscape of safety requirement elicitation has substantial contributions from industry. We classified the studies according to industry, academia, or industry-academia collaboration contributions. Two intuitive means to identify the source of contributions are (1) the affiliation of authors and (2) the source of case studies and data. The latter is not feasible in our

context since many primary studies do not explicitly specify the source of the case study, data, or the examples they use. Therefore, we choose to classify the source of the study based on the author's affiliation into three categories: (1) industry; (2) academia; and (3) industry-academia collaboration. If all the authors are affiliated with the industry, then the study is considered from industry and similarly for academia. If a study has author affiliations from both industry and academia, it is classified as industry-academia collaboration. The resulting classification is presented in Fig. 3b. This categorization shows that most of the primary studies (54 out of 102) have some contributions from industry, making the safety requirement elicitation publication landscape one with a solid industrial contribution.

Publication landscape: A majority of studies are published in conferences and symposiums with 53% of all studies having contributions from industry.

Safety requirement elicitation is a multi-disciplinary field of research. We examined the domain of each primary study. We identified the domains by research areas listed on the web page of the publication venue of each primary study. When a venue represented one domain, publications were classified to that domain. There were also cases where a venue represented more than one domain. Here, we chose to report the domains together if most of the venues listed two or more areas together, like reliability engineering and safety engineering. Otherwise, we counted the study in both areas. For this analysis, we excluded venues like the International Conference for Convergence in Technology, which does not have specific research areas, or venues like the International Conference on Networks, Communication, and Computing, which specify a wide variety of unrelated domains. This does not affect our classification since less than 1% of the primary studies are from such venues. All the domains that cumulatively covered less than 5% of the publications were classified as 'other' in

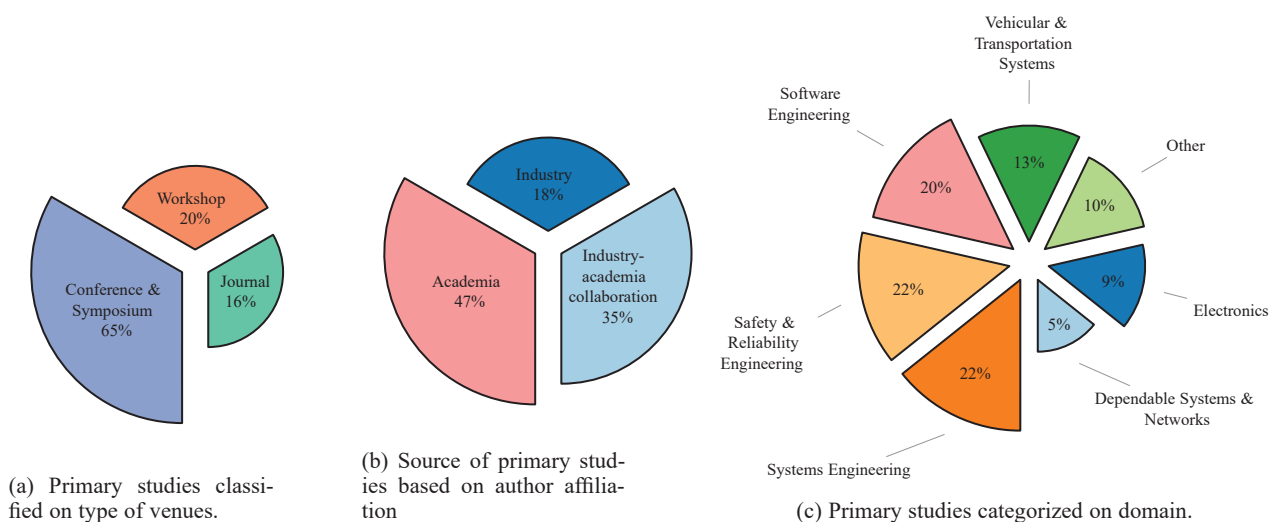


Figure 3. An overview of the publication, domain, and contribution landscapes of the primary studies.

the final list of domains. The resultant set of domains is presented in Fig. 3c. The set of domains depicted shows the multi-disciplinary nature of safety requirement elicitation research.

Multi-disciplinarity: Primary studies span across different disciplines with a domination of software, systems, reliability and safety engineering.

4. SAFETY REQUIREMENT ELICITATION PROCESSES (RQ1)

In this section, we identify, summarize, and compare processes (also referred to as methodologies [P32,P59]) used or discussed in the primary studies for safety requirement elicitation in the automotive context. In our context, processes or methodologies refer to the high level steps that describe the elicitation of safety requirements [2,3,24,P20,P40,P46,P59,P77,P86]. For example, the safety requirement elicitation process prescribed by the industry-standard ISO 26262 consists of four high-level steps as shown in Fig. 4.

We organize the rest of this section into two parts. Section 4.1 compiles the safety requirement elicitation processes proposed, used, or discussed in the primary studies. Section 4.2 analyzes the application of the

processes reported in the literature, their temporal trend, the associated research gaps, and the upcoming domain trends.

4.1. Findings

The primary studies mention 9 unique processes for safety requirement elicitation. We organize them into the following 7 categories (① – ⑦).

There are 9 unique processes for safety requirement elicitation in the automotive domain.

① *ISO 26262*: The ISO 26262 standard [2] forms the basis for safety requirement elicitation in the automotive domain. One focus area of the standard is risks from systematic and random hardware failures in automotive electronic systems and the software that runs them (also termed functional safety). The standard is an adaptation of IEC 61508 [25] to the automotive domain, the latter being a generic standard that outlines safety guidelines for developing *any* electronic and programmable systems that carry out safety functions.

The safety requirement elicitation process outlined by the standard (ISO 26262: part-3 [2]), highlighted by the

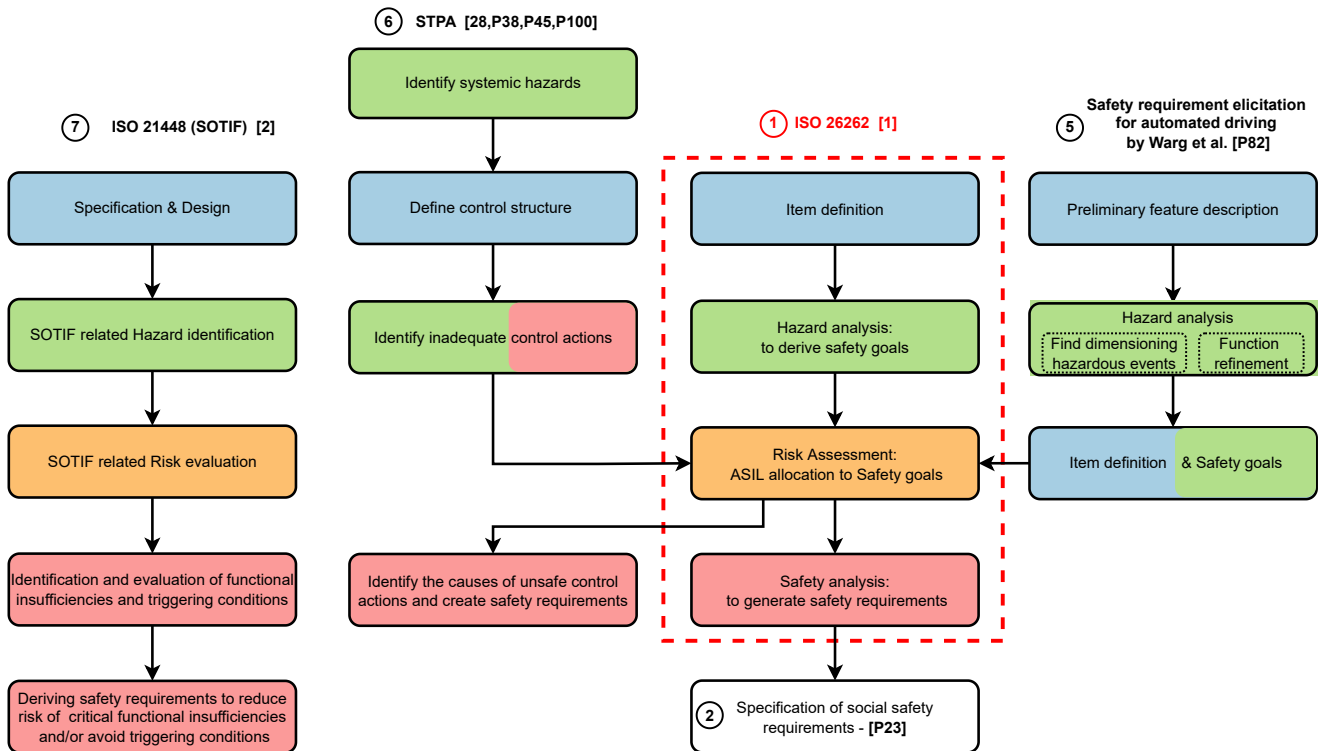


Figure 4. Different safety requirement elicitation processes from the automotive domain. The ISO 26262 process (highlighted in red) forms the basis for safety requirement elicitation in the domain. The circled numbers (①, ②, ⑤–⑦) point to the part of Section 4.1 in which the corresponding methodology is discussed. Similar steps across different processes are color-coded the same. The methodologies proposed by Schönemann et al. [P59], Saberi et al. [P86], and Kochanthara et al. [P32], described in ③ and ④ in Section 4.1 use the entire ISO 26262 process without any modification (with the primary difference of partitioning the scenarios space before starting the ISO 26262 process). Therefore, we have not presented them in the figure.

dashed red rectangle in Fig. 4, comprises four steps: item definition, hazard analysis, risk assessment, and safety analysis. The item definition step specifies the system and its boundaries on which the rest of the steps will be performed. The hazard analysis step first identifies possible situations that can be a safety risk, followed by safety goals to prevent harm in those situations. The risk assessment step assesses the level of risk for each safety goal based on three factors:

- (a) Exposure (frequency or probability of the safety goal violation);
- (b) Controllability (in situations of safety goal violation by the driver); and
- (c) Severity (of harm on violation of the safety goal). It then allocates a score from A through D, indicating the importance of covering a safety goal during further development steps, with D indicating the highest risk level and A the lowest. This score is called the Automotive Safety Integrity Level (ASIL) score. Note that these safety goals have a system-wide scope. Finally, the safety analysis step maps these safety goals to safety requirements for individual sub-systems or components, which can then be used in developing individual sub-systems.

The above process, prescribed by the ISO 26262 standard, forms the basis of safety requirement elicitation in the automotive domain. Note that we do not differentiate between the 2018 and 2011 versions of ISO 26262 or its regional variants (for example the Chinese GB/T 34590 safety standard, used by Zhou et al. [P85]) since the fundamental concepts and high-level steps do not differ among them. The other processes from the primary studies that are described in this section build on or complement ISO 26262 in various ways. They fundamentally differ from ISO 26262's process either in its concept, model, or in the high-level steps.

Basis: The process outlined by ISO 26262 (part-3) forms the basis of all safety requirement elicitation processes in the automotive domain.

The rest of this section is organized as follows. Parts ② – ④ describe five processes that extend ISO 26262 requirement elicitation. After those we elaborate on three methodologies proposed as replacement for ISO 26262 in parts ⑤ – ⑥. Finally, we present a process (⑦) that complements the ISO 26262 elicitation process.

② *Social safety requirements:* Gharib et al. [P21] argue that ISO 26262 does not consider safety requirements specific to driver behavior, which they term as “*social safety requirements*”. An example of a social safety requirement is “*identify available information concerning the driver state (e.g., head pose and motion, hands and foot location and motions) at any point in time*” [P21]. Gharib et al. [P21] propose to add a step to elicit social

safety requirements at the end of ISO 26262 requirement elicitation, as shown as a white box below the ISO 26262 process flow in Fig. 4. They also present an example of the proposed extension on a maneuver assistance system to detect and respond to drivers' unintended maneuvers. However, they did not describe any systematic method to elicit social safety requirements.

Social safety requirements are safety requirements specific to driver behaviour, proposed by Gharib et al. [P21]. Details on how to elicit these requirements are not available.

③ *Safety requirements for connected driving:* Connected driving refers to multiple vehicular systems and traffic infrastructure communicating and working as a single system. This forms a system of systems and enables collective traffic optimizations. Such a system of systems perspective is missing in ISO 26262 [P32,P86], thus making ISO 26262 unsuited for use in the connected driving context. Saberi et al. [P86] and Kochanthara et al. [P32] propose augmentations to the ISO 26262 process for this context.

The process by Saberi et al. [P86] uses the steps for safety requirement elicitation from ISO 26262 but is executed separately, from a system of a systems perspective. Their extension to ISO 26262 is inspired by hazard analysis for the system of systems from other domains [26]. Saberi et al.'s [P86] also partially outlines the usage of their method in the context of a connected driving use case of trucks, where a lead truck is driven by a driver and a sequence of other trucks autonomously follows the leader.

Kochanthara et al. [P32] suggest a two-step extension to the ISO 26262's process, considering the heterogeneity of connected systems, i.e. traffic infrastructure and multiple kinds of vehicles (for example, trucks and cars or different types of cars) forming a connected system. Their first step is partitioning the scenarios for connected driving operations into sets of scenarios specific to each different system (vehicle) and those common to or involving the entire connected system. Thus a connected driving system consisting of n distinct types of vehicles will have $n + 1$ sets of scenarios. Then, the ISO 26262 process is applied to each of the n distinct types of vehicles separately. The partitioning and applying ISO 26262 process on each of the n distinct types of vehicles, is the first step. In the second step, the scenarios specific to the connected system, i.e., common to the entire connected system or involving more than one vehicle, are considered. A connected system architecture is created using the individual systems' (distinct types of vehicles' and traffic infrastructure's) components. The connected system architecture should show the possible interactions across the individual systems' components. Now, the ISO 26262 method should be applied to the entire connected system using its architecture and the scenarios

specific to the connected system. They also show the applicability of their approach in a similar use case as in Saberi et al.'s [P86].

Connected driving refers to multiple vehicular systems and traffic infrastructure communicating with each other and working as a single connected system. To elicit safety requirements for connected driving, Saberi et al. [P86] and Kochanthara et al. [P32] extends the ISO 26262 process to cover both individual-vehicle perspective(s) and a connected system perspective.

④ *Scenario-based safety analysis for automated driving*: Schönemann et al. [P59] argue that the number of operating situations to be considered for safety requirement elicitation for automated driving might be unlimited, making the ISO 26262 process infeasible. Their proposal extends the ISO 26262 process for automated driving with the abstraction of the system's behavior to limit the number of parameters. The proposed process starts with decomposing the system's functional behavior into a higher abstraction of functional scenarios and then performing ISO 26262 safety requirement elicitation specifically for each functional scenario. Thus the steps (other than decomposing the system's functional behavior into functional scenarios) are the same as ISO 26262.

⑤ *New requirement elicitation process for automated driving*: Warg et al. [P77] argue that ISO 26262 assumes a driver for fallback in case of a malfunction or failure of a component. At the same time, there is no driver to fall back to in the case of entirely automated driving. To address this gap, Warg et al. [P77] present an approach based on the ideology of adequately specifying the system and its function iteratively using their version of hazard analysis. This process ensures that the automated driving functions are adequately specified. It also ensures that all the relevant hazardous events related to all functions that enable automated driving are covered. Their process differs from the one by Schönemann et al. [P59] (see ④ above) to automated driving in two aspects: (1) Schönemann et al. [P59] uses the ISO 26262 process as is, while Warg et al. [P77] proposes a new iterative process to replace it; and (2) Schönemann et al. [P59]'s process is aimed to scale the ISO 26262 process to an infeasibly high number of operating situations via abstraction. At the same time, Warg et al.'s ideology is based on iteratively defining a function and minimal representative set of hazardous conditions.

Warg et al. proposed a new process as shown as the rightmost flow in Fig. 4. It differs from the ISO 26262 process in the first two steps: preliminary feature description and new hazard analysis. The preliminary feature description step describes the proposed feature's anticipated benefits and initial scope. The hazard analysis step consists of two sub-steps: finding dimensioning hazardous events and function refinement. The dimensioning hazardous events are the sets

of hazardous events that are sufficient to identify all critical safety goals. The function refinement sub-step aims to elicit requirements for the intended nominal functionality and define the scope of each function. Therefore the hazard analysis step results in (ideally) a minimal set of hazardous events and refined functionality from the preliminary feature description.

Another significant difference between this process and ISO 26262 is that the definition of the system and its boundaries (item definition) is an intermediate step in Warg et al.'s [P77] process, yet it is the starting step in ISO 26262 (see Fig. 4).

Automated driving refers to a vehicle taking over (part of the) driving and eliminating the need for a human for (some) driving tasks. Schönemann et al.'s [P59] and Warg et al.'s [P77] proposes processes to address two limitations of the ISO 26262 process in an automated driving context: (a) the possibility of unlimited number of conditions [P59] and (b) the assumption of driver fallback which leads to inadequate specification of functionalities, respectively.

⑥ *Systems Theoretic Process Analysis (STPA)*: The primary difference between STPA and ISO 26262 is that STPA treats accidents as a control problem rather than a failure problem.

STPA is proposed for safety requirement elicitation in the general context of safety-critical systems from a system theoretic point of view [24]. In literature, STPA has been used in the automotive domain in two contexts: (1) as a methodology for safety requirement elicitation that complies with the ISO 26262 standard [P33,P40,P94]; and (2) as a technique for the steps (similar to) hazard analysis and safety analysis [3,P89], from the ISO 26262 and ISO 21448 (described in ⑦) processes. In this section, we discuss the former context.

STPA intends to prevent accidents by enforcing constraints on component behavior and interactions. The underlying model of STPA promises to cover more causes of accidents than component failures, like design errors and flawed requirements [24]. Therefore, two dominant reasons to advocate STPA over the ISO 26262 process are: (1) the wide variety of error types it covers (ISO 26262 only covers random hardware failures and systematic failures) [P33]; and (2) less dependence on expert knowledge [P33,P89]. The error types STPA covers include component failures, inadequate component interactions, software failures, human error, and system failure [P33]. Another advantage of STPA is that expert knowledge is not always required for requirement elicitation [P33,P89].

However, the original STPA process [24] lacks a risk assessment step. Mallya et al. [P40] showed that the STPA process could be augmented to include a risk assessment step from ISO 26262 as shown in flow ⑥ STPA) in Fig. 4. The STPA safety requirement elicitation process itself consists of 4 steps, as shown in Fig. 4. The first step

(identify systemic hazards) identifies the possible accidents and hazards that can cause these accidents and is similar to the hazard analysis part of ISO 26262. The second step of defining a functional architecture (control structure in STPA's original terminology) includes defining the system's interaction with the environment and stakeholders in addition to defining the system and its boundaries as is done in the ISO 26262 process. The third step, identifying unsafe control actions using the functional architecture and hazards from the previous steps, is similar to a partial merge of the hazard analysis and safety requirement elicitation steps in ISO 26262. We mention partial merge here since identifying hazards (possible accidents) from hazard analysis step and identifying safety requirements from safety analysis step of ISO 26262 is not a part of identifying unsafe control actions step in STPA. These two parts from hazard and safety analysis comes in first and last step of STPA respectively.

After third step in STPA, Mallya et al.'s augmentation [P40] adds the risk assessment from ISO 26262. The final step is similar to the last step from ISO 26262 (safety analysis). It identifies safety requirements based on the unsafe control actions (and their corresponding risk level in Mallya et al.'s augmentation [P40]).

System Theoretic Process Analysis (STPA) originates from system theory rather than control theory on which ISO 26262 is based. STPA promises inclusion of requirements beyond systematic and hardware failures (which is the scope of ISO 26262) including inadequate component interactions and human errors.

⑦ *ISO 21448*: The standard ISO 21448 [3] alternatively known as Safety of Intended Functionality (SOTIF), is introduced to complement ISO 26262 in contexts “where proper situational awareness is essential to safety and where such situational awareness is derived from complex sensors and processing algorithms” [3]. The SOTIF process focuses on hazards that do not exist because of failures, but instead because of insufficiency of specification, performance limitations, insufficient situational awareness, incorrect and inadequate Human-Machine Interface design, impact from active infrastructure and vehicle to vehicle communication, and external systems [3]. Note that attacks exploiting vehicle security vulnerabilities, and intentional actions that violate the system's intended use, like a substitute hand to fool an “hands-on wheel” detection safety measure, is out of the scope of SOTIF. Also, the standard is in its development stage, and a complete version is yet to be released to the public.

The SOTIF safety requirement elicitation process consists of five steps, as shown in Fig. 4. The first step, specification and design, is analogous to the item definition step from ISO 26262. This step consists of defining the operating environment like road surface and climatic conditions, the system's interactions with users and

traffic participants, and the system and its boundaries. The second step, SOTIF-related hazard identification, is analogous to the hazard analysis step from ISO 26262 but scoped to intended functionality rather than failure scenarios. The third step, SOTIF-related risk evaluation, is analogous to risk assessment from ISO 26262 and is based on three aspects: occurrence frequency of a given scenario, the severity of a triggering condition (same as in ISO 26262), and the effectiveness of measure taken for the safety of the intended functionality. The fourth step identifies insufficiencies of specification, performance limitations, and conditions that trigger the limitations that could initiate hazardous behavior. The final step is deriving safety requirements to avoid or prevent hazardous behavior.

Safety of Intended Functionality (SOTIF, ISO 21448) complements the ISO 26262 process for automated driving and include requirements relating to insufficiencies of specification, performance limitations, insufficient situational awareness, incorrect and inadequate Human-Machine Interface design, impact from active infrastructure and vehicle to vehicle communication, and external systems.

4.2. Analysis

We analyze the processes presented in the prior section based on their temporal adoption trend and context of usage. Based on this information and the comparison presented in the preceding section, we present research gaps and upcoming domain trends.

A process adoption's temporal trend is an indicator of its use. A positive trend points to tooling and community support. Both of these are essential for the application of the process in large-scale systems. The adoption of processes across years does not indicate any apparent overall patterns as shown in Fig. 5. However, the number of publications that mention the usage of ISO 26262's process peaked in 2019 with a substantial

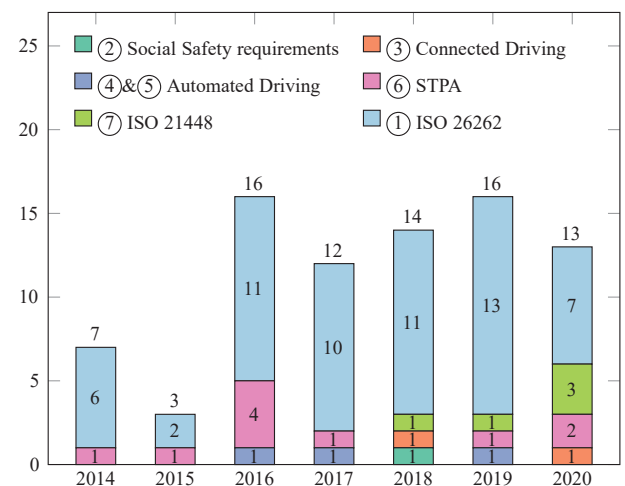


Figure 5. Number of primary studies that discuss safety requirement elicitation processes plotted across years.

decrease in 2020. We present three hypotheses for this decline: (1) The 2020 drop in ISO 26262 usage may reflect disruption from COVID-19, which slowed certification workflows, audits, and formal safety assessments across automotive development pipelines; (2) Some organizations may have shifted attention to rapid deployment of ADAS and automated driving features, emphasizing agile experimentation over strict standards compliance; (3) The rise of AI-centric components and novel architectures may have pushed researchers toward alternative frameworks or extensions (e.g., ISO 21448), temporarily reducing explicit ISO 26262 references.

The usage of the upcoming ISO 21448's process shows a steady increasing trend. The number of publications that report usage of STPA first peaked in 2016, followed by a downfall and a small increase again. Adopting the rest of the processes is reported primarily in the articles that describe them or in articles by the same authors. The only exception is one article by Stolte et al. [P66] which reports usage of Warg et al.'s [P77] process (described in ⑤). In summary, the application of processes proposed by industry-specific standards dominates across years, while the other processes proposed to extend or replace the standards do not show wide adoption except for STPA. Note that the adoption estimates are based on the primary studies and the real industry adoption might be different. Since industrial usage might not always be apparent from articles published, it will have to be substantiated via future research, for instance, using interviews or surveys.

High adoption of industry standard processes: ISO 26262's safety requirement elicitation process dominates in adoption across years while the adoption of ISO 21448's process shows a steady increase. Other processes proposed to extend or replace the ISO 26262's process do not show wide adoption with the exception of STPA.

The practicality and limitations of processes in different use-cases will only be known by the application of the process in those use-cases. Therefore, prior application contexts are important for researchers, practitioners, educators, and beginners to identify avenues for future research, the starting point for similar use-cases, and to act as a guide for the application of processes. For this, we first group the components and use cases where the processes have been applied into the following six categories based on existing classification schemes in literature [19,27].

1. *Vehicle-centric functional components* are the components necessary for the functioning of the vehicle. Examples are powertrain, battery management system, braking and steering system (including their safety systems such as anti-lock braking system), and fuel injection system.

2. *User-centric functional components*, which in our context is the Human-Machine Interface (HMI), for interacting with the vehicle.
3. *Advanced driver assistance systems* like adaptive cruise control, traffic jam assist, and lane management system, which can assist a human driver in a driving task but cannot accomplish a complete driving task on their own.
4. *Advanced active safety systems* like advanced emergency braking system, collision warning and avoidance systems, and maneuver assistance system that use multiple sensors and sensor fusion techniques to actively ensure the safety of traffic participants.
5. *Highly automated driving use-cases* where the vehicle is capable of handling a complete use-case without driver intervention like automated valet parking, automated shuttles that can operate without a human driver on specific routes, and completely automated driving that can drive ideally anywhere or at least in a geofenced area without the active intervention of a human driver.
6. *Connected driving use-cases* like platooning where multiple vehicles form a vehicle train with only the lead vehicle driven by a human and the rest autonomously following the vehicle in front.

The number of articles that report safety requirement elicitation in each of the above categories and the processes they use is plotted in Fig. 6. The ISO 26262's process is used in primary studies for every category except for User-centric functional components (HMI); STPA and ISO 21448 processes and the processes proposed for automated driving have been reported to be used in more complex use-cases (except in one study for battery management systems) and HMI. HMI is not seen traditionally as a safety-critical component; however, with the advent of advanced driver assistance systems, and highly automated and connected driving, HMI is becoming safety-critical.

Essential versus Advanced functions: The ISO 26262's process has shown to be usable for safety requirement elicitation of essential automotive functions that do not require complex situational awareness. STPA and ISO 21448's processes cumulatively dominate in the use-cases that need complex situational awareness.

Informed by the adoption, temporal trend, and comparison of processes, we point to the following three dimensions that need further exploration. One, components and use-cases to which the current processes can be applied, but have not been presented in the literature. Two, new contexts and emerging technologies like neural processing units and Machine Learning (ML) based software, which might require new processes for safety requirement elicitation. Three, the introduction

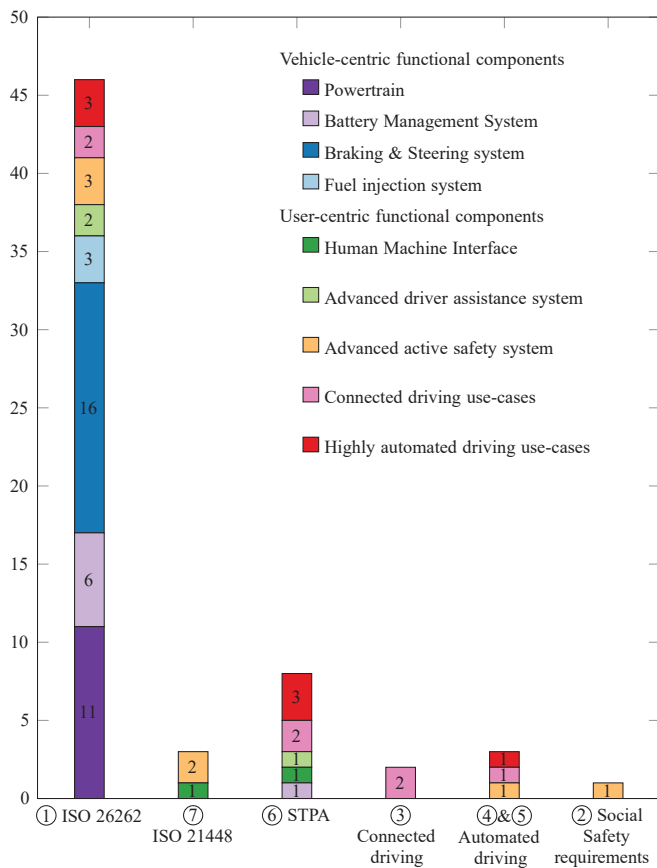


Figure 6. Number of primary studies presenting the usage of different safety requirement elicitation processes.

of new systems outside the vehicle like intelligent traffic infrastructure and use of the cloud for (assisting) automated driving. The scope and criticality of these external systems will have to be quantified to identify (1) whether they need a separate or integrated requirement elicitation and (2) whether the existing process can be used. We elaborate on each of these aspects in the rest of this section.

The literature lacks case studies on categories like advanced active safety systems like blind-spot detection and advanced driver assistance systems like adaptive cruise control, as evident from Fig. 5. These features have matured from research and development to production and are standard features in today's high-end cars. Upcoming technologies currently in research and development, like highly automated and connected driving, also lack case studies compared to other categories. The adoption of processes other than the industry-standard processes is still low. The lower adoption makes the iterative improvements and scope of their applicability harder to identify and hinders further research. The majority of existing case studies on advanced systems for automated and connected driving are rudimentary examples. The practicality of new processes presented within the scope of these advanced systems is yet needed to be shown in practice. To summarize, new processes proposed in primary studies

need more case studies in their respective context for a conclusive verdict on the feasibility of their application in real-world settings.

Case studies: There are few to no case studies that use requirement elicitation processes other than ISO 26262 or on advanced components and use-cases.

All the advanced driver-assist and safety features as well as automated and connected driving are enabled by special-purpose hardware and software that utilizes ML. Yet neither of the two standards ISO 26262 and ISO 21448 mentions [28] any requirements or processes regarding developing neural networks for usage in such systems. The basis and underlying model on which the requirement elicitation processes were built belonged to an era before ML-based software were mainstream. In ML-based systems, the system's behavior is dictated by the input data and not by human written logic. The newly proposed processes build on the basic safety requirement elicitation framework proposed by ISO 26262 and mainly focus on the increased complexity, non-existence of driver (controllability aspect), sufficient specification of (safety) requirements, and foreseeable misuses in the context of automated and connected driving, rather than on the above mentioned fundamental changes.

ML-based sub-systems: Whether the current processes are sufficient to elicit safety requirements for special purpose hardware and ML-based software is an open question.

Connected driving builds on collective traffic optimization by a set of vehicles communicating with each other and external entities (roadside infrastructure) using peer-to-peer networking or via the cloud. With the intelligent traffic infrastructure being a part of a driving task and the cloud acting as a data intermediary or a sensor, both of them become safety-critical components. However, the new methods proposed to elicit safety requirements for the connected driving context focus on the vehicles and do not consider the safety requirements for the infrastructure involved.

Smart infrastructure and intermediaries: How to elicit safety requirements for traffic infrastructure and communication intermediaries like the cloud in the context of connected driving is another open question.

The landscape shifts in the automotive industry with automated driving will also impact safety requirement elicitation. Like the smartphone replaced three separate devices for music, taking photos, and communication; automated driving bundles advanced tasks together. Therefore, many of the categories specified in Fig. 6 might be a single one in the future. This changes prior assumptions on driver fallback and turns many non-safety-critical systems into safety-critical. For example, maps, previously a non-safety-critical

part, used at human discretion, have an active role in automated driving and are sometimes considered as a sensor. Previously, the driver was assumed to be vigilant and ready all the time for fallback. Now, HMI can be used to decide on a driving task and for emergency takeover, making HMI a critical safety component. The impact of such changes on safety requirements and their elicitation is yet to be seen.

Blurring lines: No more separation of advanced driver assistance and safety systems; these all are bundled together in highly automated driving.

5. SAFETY REQUIREMENT ELICITATION TECHNIQUES (RQ2)

In this section we identify, review, taxonomize, and compare techniques (also referred to as methods [2,24,P20,P46,P78]) for safety requirement elicitation in the automotive domain. Techniques or methods refer to the alternative ways to conduct each high-level step [3,7,24,P40,P46,P59,P77] in safety requirement elicitation processes as presented in Section 4. For example, two widely used techniques to conduct the safety analysis step in the ISO 26262 process (the last step in the red highlighted part of Fig. 4) [2] are fault tree analysis [29] (FTA) and failure mode effect analysis [30] (FMEA).

We organize the rest of this section into two parts. Section 5.1 present a summary and taxonomies of techniques for safety requirement elicitation. Section 5.2 analyzes the techniques, their scope of use, the associated research gaps, and the upcoming domain trends.

5.1. Findings

There are 38 distinct safety requirement elicitation techniques discussed in the primary studies. Our taxonomy is inspired by stages in automotive product development and the reference product life cycle from industry standards [2,3]. In automotive product development, the norm is to design and evaluate at the system level, then subsystem level, followed by the design and development of the individual hardware and software components. We follow the same structure for creating our taxonomy. Our taxonomy is organized based on the level of application (system, software, and hardware), the usage context (general, automated driving, and connected driving), and the scope of application of the techniques, as shown in Tables 2 to 4. This allows easy identification of the choice of techniques by both researchers and practitioners. We organize the entire taxonomy of techniques based on the steps in safety requirement elicitation processes (since the techniques are alternate ways to conduct these steps).

Level of Application	Usage Context	Technique	Process [Primary Studies]
	General	[1] Guide-word based brainstorming	ISO 21448 & STPA [P98]
		[2] Failure Mode and Effect Analysis (FMEA)	ISO 26262 [P84,P85]
		[3] Undesired Combination State Templates	No process specified [P1]
		[4] Hazard analysis using vehicle level simulator & item functional model	ISO 26262 & ISO 21448 [P62]
System & Software	Automated driving	[5] Situation/Scenario Analysis & Brainstorming	ISO 26262 [P96] ISO 21448 [P34]
		[6] Guide words based, HAZard and OPerability analysis (HAZOP)-inspired brainstorming	ISO 21448 [P34]
		[7] Iterative hazard analysis and function refinement	Process for automated driving [P77]
		[8] Shared and multi-level hazard analysis	ISO 26262 [P47]
Hardware specific	Connected driving	[9] Guide-word based brainstorming	Process for connected driving [P32] No process specified [P97]
	General	[10] Brainstorming	ISO 26262 [P68]
		[11] HAZOP	ISO 26262 [P15,P27]
		[12] FMEA	ISO 26262 [P68,P76]
	Automated driving	[13] HAZOP extension to automated driving	ISO 26262 [P5]
		[14] HAZOP based on sensor limitations to identify malfunctions	ISO 21448 [P42]

Table 2. Hazard analysis techniques from primary studies. All the above techniques are reported in the corresponding primary studies with the scope of identifying/deriving hazardous events or situations and thus deriving safety goals.

Level of Application	Scope	Technique	Process [Primary Studies]
System & Software	1 Identify/allocate Automotive Safety Integrity Level (ASIL) for systemwide safety goals	Usage of Controllability, Exposure, and Severity metrics from ISO 26262	ISO 26262 [P30,P32,P39, P41,P62,P72,P76,P82,P85, P96] STPA [P6,P40,P94]
		Augmenting the ISO 26262 metrics with plant and fault modeling	ISO 26262 [P84]
		Identifying severity ratings using simulation	No process specified [P17]
		Quantitative Risk Norm to replace ASIL ratings for automated & connected driving	ISO 26262 [P9,P78]
	2 ASIL decomposition	High to low ASIL decomposition according to ISO 26262 guidelines	ISO 26262 [P51]
		Merging ASIL allocation method from ISO 26262 with ASIL decomposition	ISO 26262 [P37]
	3 Optimal ASIL allocation out of possible allocation options	Genetic Algorithm with cost heuristics	ISO 26262 [P3]
		Tabu Search with cost heuristics	ISO 26262 [P3,P102]
		Penguin Search	No process specified [P93]
	4 Reducing ASIL allocation search space	Cut-set based reduction	ISO 26262 [P23]
Heuristic cost based reduction		ISO 26262 [P23]	
Hardware specific	5 Identify/allocate ASIL for functional component (hardware) specific safety goals	Ant colony optimization algorithm	No process specified [P24]
		Usage of Controllability, Exposure, and Severity metrics from ISO 26262	ISO 26262 [P15,P27,P35,P36, P38,P60,P63,P68,P69,P76]
	6 ASIL decomposition	Dependent Failure Analysis	ISO 26262 [P83]
	7 Optimal ASIL allocation	Genetic Algorithm with cost heuristics	ISO 26262 [P3]

Table 3. Risk assessment techniques from primary studies. Except for the quantitative risk norm (fourth row in the third column), the rest of the methods are used in general context. The quantitative risk norm is proposed and used specifically to replace the ASIL levels in the context of automated and connected driving.

To group techniques based on the safety requirement elicitation steps, we must adhere to the definitions of what each step is intended to achieve in the safety requirement elicitation processes. However, in the literature, there is little consensus on this subject. For example, Vilela et al. [7] use the term *safety analysis* to denote any technique used in safety requirement elicitation in the larger context of safety-critical systems; while Kolln et al. [P33], and Abdulkhaleq et al. [P89] use both the terms hazard analysis and safety analysis to compare the same set of techniques. Since this study focuses on the automotive domain, we follow the terminology from the industry standards ISO 26262 and ISO 21448. These standards have industry consensus and wide adoption (as is evident from the discussion in Section 4.2 above).

For consistency and brevity, we group techniques for similar steps of safety requirement elicitation processes (shown with the same color in Fig. 4) together and refer to each group with the terms (for steps) from the ISO 26262 process. However, in our taxonomy, we refer back to the original processes (refer to the fourth column of Tables 2 to 4 that shows our taxonomy). Note that the social safety requirement elicitation step [P20],

shown in the white box in Fig. 4, is not similar to any of the four steps from the ISO 26262 process. We did not find any technique for this step in primary studies including the original study itself [P20]. Therefore, we do not consider this step for our taxonomy. Also, our taxonomy does not have the first step of the ISO 26262 process (item definition) nor similar steps in other processes. This step (formally or informally) defines the system, its boundaries, the environment it operates in, the traffic participants it interacts with, and the stakeholders. Such a definition uses languages for modeling, which is a topic in itself for another study and beyond the scope of this work. Therefore, we group techniques based on their usage for each of the other three steps (and corresponding similar steps in other processes shown in Fig. 4).

We present the techniques in the following three parts (corresponding to the three steps in ISO 26262 process): **Hazard analysis**, **Risk assessment**, and **Safety analysis**. Tables 2 to 4 show our taxonomy, one for each of the three steps. The techniques are presented in the third column of each table. The primary studies that mention these techniques along with the corresponding process (identified from each primary

Level of Application	Usage Context	Technique	Process [Primary Studies]
System & Software	General	[1] Fault Tree Analysis (FTA)	No process specified [P10]
		[2] Dynamic fault trees	No process specified [P92]
		[3] Component integrated component fault trees	No process specified [P16]
		[4] Model Based Safety Analysis (MBSA)	ISO 26262 [P48,P84] No process specified [P53]
	Automated driving	[5] FTA	ISO 26262 [P58]
		[6] Environment fault tree	ISO 21448 [P34]
		[7] MBSA augmented with simulation	No process specified [P70]
	Connected driving	[8] FTA	Process for connected driving [P32,P86]
		[9] FTA with fault classification	ISO 26262 [P13]
Hardware specific	General	[10] FTA	ISO 26262 [P14,P15,P27,P35,P36,P38,P45,P48,P60,P82]
		[11] Common-cause fault analysis	ISO 26262 [P18,P27]
		[12] Failure Mode and Effect Analysis (FMEA)	ISO 26262 [P27,P35,P48] No process specified [P53]
		[13] Aging FMEA	ISO 26262 [P57]
		[14] Failure Mode Effect and Diagnostic Analysis (FMEDA)	ISO 26262 [P12,P28,P45,P50,P95]
		[15] FMEDA augmented with Simulation	ISO 26262 [P61]
		[16] Dependent failure analysis	ISO 26262 [P50]

Table 4. Safety analysis techniques from primary studies. All the above techniques are reported in the corresponding primary studies with the scope of identifying/deriving safety requirements from safety goals using architecture of the system or the specific component.

study) are presented in the fourth column. The first two columns present two dimensions of our taxonomy, and a third dimension is specified in the caption of each table. Note that we only considered explicitly mentioned techniques. For example, Wang et al. [P75] uses the method of brainstorming but does not mention it explicitly; thus, the study is not considered for the technique. Also, if a method is used for more than one step, it is presented in all steps.

Techniques: There are 38 distinct techniques used in primary studies for safety requirement elicitation. We group them into three categories: hazard analysis, risk assessment, and safety analysis. We taxonomize techniques in each category based on the application level, usage context, and scope, as shown in Tables 2 to 4.

5.1.1. Hazard Analysis

The objective of hazard analysis (and similar steps) is to identify (a) (minimal set of) hazardous events either caused by a system’s malfunctioning behavior or related to the system’s intended functionality, (b) unsafe control actions, (c) possible accidents, and (d) hazards that can cause the accidents. These can then be used to derive safety goals or to refine the system’s functionality (see Section 4.1 for more details). We

taxonomize hazard analysis techniques as shown in Table 2 and discuss each of the techniques starting with the simplest one.

Brainstorming ([5] and [10] in Table 2) is a technique to identify hazardous events and eventually safety goals for hardware, system, and software specific requirements [P34,P68,P96]. The idea is to first think of possible scenarios and situations that can lead to potential hazards; and then use these to identify safety goals to avoid harm in those hazardous situations.

Guide-word based brainstorming ([1] and [9] in Table 2) is a more structured, systematic form of brainstorming. It uses guide-words to explore the hazardous situation space [P32,P34,P96,P97,P98]. Guide-words are predefined words like *No* and *Late*, which, when combined with scenarios, can thus be used to identify potentially hazardous situations. This structured method is shown to be applied in general [P98] and in automated [P34,P96] and connected driving [P32,P97] contexts.

HAZard and OPerability analysis or *HAZOP* ([11] in Table 2) is the technique from which the usage of guide words stems. In its original form, HAZOP is a structured and systematic method with a specific documentation style. HAZOP also recommends a

specific team composition (to conduct the analysis) with certain roles inside the team [31]. HAZOP is reportedly used in its traditional form at the hardware level [P15,P27].

Three *extensions to HAZOP* ([6], [13], and [14] in Table 2) were proposed in the context of automated driving [P5,P34,P42]. Martin et al. [P42] showed that HAZOP, based on limitations of sensors like cameras and LiDARs, can be used to identify hazardous situations related to the safety of intended functionality ([14] in Table 2). Another extension of HAZOP uses a skill graph as a functional model of the system with scenarios for automated driving to find hazardous events [P5] ([13] in Table 2). Kramer et al. [P34] uses a HAZOP-inspired brainstorming approach using guide-words for identifying hazards in the context of automated driving ([5] in Table 2). They also use it in the context of safety of intended functionality, focusing on environment triggers that can cause hazards.

Failure Mode and Effect Analysis or FMEA ([2] and [12] in Table 2) is another traditional and systematic technique [30]. FMEA is a bottom-up method, starting from the failure of a component(s) and then identifying the potentially hazardous situations it can lead to. FMEA is reported to be used for hazard analysis at system, software, and hardware level [P68,P76,P84,P85].

Undesired combination state templates ([3] in Table 2) is a technique proposed by Aceituna et al. [P1] for identifying hazards which can be caused by a combination of system components' (and environmental) states. They argue that traditional hazard analysis techniques like FMEA focus on hazards relating to the state of (failure of) one component or event. The proposed method identifies hazards relating to multiple (failure) events while reducing the number of state permutations needed in combinatorial approaches. The technique uses templates to identify the combination of events/states (rather than a single event/state in FMEA), which can lead to a potential hazard. Thus it forms a complementary method to the traditional hazard analysis techniques.

Iterative hazard analysis and function refinement ([7] in Table 2) is a technique proposed by Warg et al. [P77] that can help reach completeness of safety goals for the completely automated driving functionality. They argue that in completely automated driving settings, the traditional methods used for hazard analysis are insufficient to ensure safety goals' completeness. They suggest that hazard analysis should have a broader scope to ensure that a vehicle's function fulfills its specifications for completely automated operation. Their technique uses an iterative procedure using trees of hazards and operational situations that can help reach a more complete and minimal set of safety goals than other techniques. They use hazard analysis as an aid rather than an

afterthought, when defining the scope of vehicular functions. On the contrary, other techniques define the functions before hazard analysis.

Shared and multi-level hazard analysis ([8] in Table 2) is a technique proposed based on the idea of shared responsibility in automated driving. The hazard analysis techniques discussed above take only the vehicle (and its driver) responsible for the potential hazards and associated safety goals. Monkhouse et al. [P47] suggest that automated driving comes with shared responsibility between multiple traffic participants to avoid hazardous situations. The study recommends performing hazard analysis considering the division of responsibilities, and handling hazard analysis at various levels, for instance, one level for each participant.

Hazard analysis using vehicle level simulator and item functional model ([4] in Table 2) is proposed to increase the accuracy and reliability of hazard analysis techniques. Most methods mentioned above (except FMEA) do not use a detailed system model for hazard analysis. Sini et al. [P62] and Tao et al. [P68] use simulators to model system and its environment (item functional model) to aid hazard analysis [P62,P68].

Hazard analysis techniques: There are 12 distinct techniques for hazard analysis and similar steps discussed across 17 primary studies. Brainstorming forms the basis for a majority ([1], [5], [6], [9], [10], [11], [13] and [14] in Table 2) of techniques. Some techniques ([3], [4], [7], [8], [13] and [14] in Table 2) are proposed by the primary studies while the rest of them use existing techniques in the automotive context. Most of the techniques are reported in the context of the safety requirement elicitation processes of industry standards ISO 26262 and ISO 21448.

5.1.2. Risk Assessment

Risk assessment intends to allocate scores for safety goals such that the score indicates the urgency and reliability level needed to address the safety goal. Table 3 shows a taxonomy of techniques for risk assessment derived from the primary studies. Unlike hazard assessment techniques, the risk assessment techniques have different scopes of application, as listed in the second column of Table 3. We elaborate on each group of techniques based on their scope of application.

Identification of ASILs ([1] and [5] in Table 3) is the problem of identifying the risk level of a safety goal. ASIL is the risk scoring scheme from the ISO 26262 standard (see Section 4.1 under ① for more details). The standard also provides a metric that combines the three individual ratings to identify the ASIL level.

These metrics are used by a majority of the studies [P6,P15,P27,P30,P32,P35,P36,P38,P39,P40,P41,P60,P62,P63,P68,P69,P72,P76,P82,P85,P94,P96] (first row of [1] and [5] in Table 3). These studies use the metrics

with the three assumed individual ratings derived from operational scenarios.

All the studies use the metrics for their case studies except Khastgir et al. [P30]. They explore how to improve inter-rater reliability of risk assessment while using the metrics in ISO 26262. They look at the two following settings: one, a rerun of the same techniques by different teams using the same data; two, with no restrictions on techniques and data (i.e. not necessarily the same methods and data) by different teams but with the same analysis scope and objectives [32]. They propose a rule set for risk assessment to improve the reliability of risk assessment (the severity and controllability ratings) in the automotive context. They conclude that subjective interpretation and resulting unreliability and variation could be reduced using an exhaustive and explanatory rule-set [P30].

Augmenting the ISO 26262 metrics with plant⁸ and fault modeling (second row of [1] in Table 3) is another method to reduce subjectivity of the ISO 26262 ASIL determination. The method stems from control theory and is proposed by Zhang et al. [P84]. They propose the use of mathematical modeling of the system and faults. Such modeling enables quantitative analysis via simulation. This can provide sound reasoning for exposure and controllability ratings, and evidence for the ratings can be provided by fault simulations.

Identify severity ratings using simulation (third row of [1] in Table 3), the usage of formal models and physics based simulations for risk assessment. This contrasts with the abovementioned studies, where severity level is computed based on various assumptions. Duracz et al. propose a method that allows computing severity levels for specific operational scenarios with accurate bounds on all the modeled parameters like the pre-collision and post-collision velocities, which contribute to a hazardous event [P17].

Quantitative Risk Norm or QRN to replace ASIL ratings for automated and connected driving (fourth row of [1] in Table 3) is a risk assessment scoring system proposed by Warg et al. [P78]. They suggest that the automated driving systems' safe behavior results from a combination of tactical and operational decisions. Therefore, safety guarantees can be achieved by adjusting the proactive decision-making, in addition to addressing random and systematic failures. These two kinds of failures are independent of the traffic situations and are the only kinds of failures the ASIL ratings takes into account [P78]. QRN is proposed to substitute the fixed risk assessment criteria of ISO 26262. Warg et al. [P78] suggests to define what is

regarded 'sufficiently safe' at design time. This definition is to be used to identify discrete risk levels called consequence classes. Each consequence class receives a total norm frequency informing how often, at most, this kind of consequence is allowed to occur. The consequence classes along with their norm frequency is QRNs. QRNs can be used to classify incidents into a set of incident types. Now each safety goal will be associated with one incident type. Warg et al. [P78] demonstrate the applicability of QRN for automated driving while Bergenhem et al. [P9] show its applicability for connected driving.

ASIL decomposition ([2] and [6] in Table 3) is the process of decomposing a higher ASIL rating of a functional component by implementing the functional component with redundancy. Here, each redundant component will have a lower ASIL rating than the original functional component, while combined, the functionality they achieve will still have a higher ASIL rating. The idea is that redundant components with individually higher probability of failure will have a lower overall failure rate. Readers can refer to Park et al. [P51] (first row in [2] Table 3) for an example implementation of the guideline.

Merging ASIL allocation method from ISO 26262 with ASIL decomposition (second row of in [2] Table 3) is proposed by Lidström et al. [P37]. They argue that the allocation and decomposition of ASILs should not be separate as specified in ISO 26262 and instead should be merged into one. They point out that separating the two processes applies only to systems with a specific kind of redundancy where two or more safety mechanisms check some state and take action sequentially. Such separation is not applicable in cases of redundancy where only one of the redundant components is operating and the other is on standby. They propose a method to combine the allocation and decomposition of ASILs. They apply it in the context of an actuation system for automated driving.

Dependent Failure Analysis or DFA ([6] in Table 3) is a part of the ASIL decomposition where a higher ASIL rating is split to lower ASILs among a set of components. DFA [33] is performed to ensure that a single root cause cannot lead to the failure of all the lower ASIL components: whether the ASIL rating, when split into multiple components, does not lead to dependent failures among the components. Young et al. [P83] propose a new scoring system for root causes of dependent failures. This scoring system can be used to compare failures' root causes, which can aid ASIL decomposition. They claim that their scoring system is more exhaustive

⁸ Plant (in control theory) refers to a machine or system. Plant modeling refers to specifying the system as a relation between output and input signals. Plant and fault modeling refers to modeling both the system and probable faults.

and compelling than that of the predecessor of the ISO 26262 standard, IEC 61508.

Optimal ASIL allocation ([3] and [7] in Table 3) problem arises when there are multiple ways to allocate ASIL ratings to individual components which together perform a function (forming a functional component). According to Azevedo et al., the ASIL allocation problem is a complex optimization problem with a vast search space of possible ASIL allocations to individual components [P3]. They present a genetic algorithm and tabu search algorithm with cost heuristics to find a strategy that minimizes the total cost of development and production while meeting the desired ASIL level with the least effort [P3]. Following Azevedo et al.'s work, Sorokos et al. [P102] also showed the application of tabu search to ASIL, allocation in the context of a braking system. Another work in the direction of optimal ASIL allocation is using the penguin search algorithm by Gheraibia et al. [P93]. They claim that the penguin search algorithm can produce optimal or near-optimal results within the least amount of time and resources for the computation. Detailing these search algorithms is beyond the scope of this article.

Reducing ASIL allocation search space ([4] in Table 3) is important since, in any practical case, the search space for finding an optimal ASIL allocation that meets the safety and cost requirements has a huge solution space due to the combinatorial nature of the problem [P23]. Searching through this space may become impracticable in large and complex systems [P23]. Therefore Gheraibia et al. [P23] propose two solutions that can be sequentially performed to reduce the solution space: (1) Cut-set based reduction where cut sets⁹ with different orders are formed as trees with their roots and nodes as the cut sets and leaves as basic events. The idea is to limit the possible ASIL range for a basic event (leaf node) and thus reduce the search space by reducing the possible ASIL allocations; (2) Heuristic cost-based reduction¹⁰ which reduces solution space by grouping the ASIL allocations to equivalence classes and creating a priority list of the allocations in each equivalence class. Gheraibia et al. [P24] further builds on their earlier work [P23] and adds an ant colony optimization algorithm for further solution space reduction.

Note that techniques like FMEA and its augmentation [P11] are used to assess whether a component or system adheres to a specific ASIL level (*ASIL evaluation*). This is out of our scope since it does not belong to eliciting safety requirements but instead assesses the fulfillment of safety requirements.

Risk assessment techniques: There are thirteen distinct techniques for risk assessment and similar steps discussed across 34 primary studies. These are techniques to (1) identify/allocate risk scores to safety goals; (2) decompose risk scores to multiple components; (3) identify optimal allocation of risk scores; or (4) reduce risk score allocation space. Most studies discuss or use techniques belonging to the first category. The only process specified for risk assessment in all the primary studies is ISO 26262's process.

5.1.3. Safety Analysis

Safety analysis is the process of deriving functional safety requirements from safety goals and allocating them to the individual components, system, software, or hardware architecture¹¹. A taxonomy of techniques used for safety analysis in the primary studies is presented in Table 4. Now we summarize each method in the order of predominance of usage and simplicity.

Fault Tree Analysis or FTA ([1], [5], [8] and [10] in Table 4) is a top-down, tree based, safety analysis technique that starts from a safety goal and leads to safety requirements and their allocation to architecture components [29]. The safety goal (or a potential hazard) is taken as the root node or top event of a tree made of logic gates as intermediate nodes. The safety requirements form the leaf nodes of the tree. The tree is constructed top-down from the root to the leafs. The fault tree can be qualitative (without any labels on edges connecting the nodes) or quantitative (with the edges labelled with failure probabilities). FTA has been applied for all levels and all usage contexts that we considered in this article [P10,P14,P15,P27,P32,P35,P36,P38,P45,P48,P58,P60,P82,P86].

FTA with fault classification ([9] in Table 4) is proposed by Dajsuren et al. [P13] for identifying the relative contributions of different groups of faults (fault classes) to the safety goals. They use fault classification – a key-value structure indicating the frequency of different faults – rather than failure probabilities to label the fault tree starting with the leaf nodes. They use this method to identify the percentage of total potential failures caused by vehicle-to-vehicle communication faults in connected driving.

Dynamic Fault Trees or DFTs ([2] in Table 4) are proposed by Ghadhab et al. [P92] to augment fault trees for faithful representation of vehicle system model. They suggest that the traditional fault trees are not sufficiently expressive for faithful representation of vehicle system models. DFTs extend fault trees with the following four specific gates: *sequence-enforcers*,

⁹ "A cut-set is a minimal combination of failures of components, which, if they occur in conjunction, lead to a hazard" and fault tree analysis is used to find cut sets [P23].

¹⁰ "Cost heuristics are functions that determine the cost of associating the ASILs to each component of the system" [P23].

¹¹ In some processes, the intermediate safety goal step is skipped, and safety requirements are directly derived from hazardous events.

for restricting sequence between children of a node; *priority-and*, for indicating priority between children of a node; *spare-gates*, for supporting reduced or zero failure rate; and *functional dependencies* supporting modeling feedback loops and triggers. They show the applicability of DFTs in the case study of a vehicle guidance system.

Environment Fault Tree or EFT ([6] in Table 4) proposed by Kramer et al. [P34] extends fault trees to specify environmental conditions using special gates. In EFT, environmental conditions are modeled as leaf nodes that trigger higher-level faults. EFTs classify the causes for deviation from correct behavior to (random) hardware faults, (systemic) design faults in hardware or software, (systemic) specification faults either due to incorrect assumptions or lacking a structural approach. This method is specified in the context of safety of intended functionality in automated driving.

Common Cause Fault analysis or CCF ([11] in Table 4) is a safety analysis technique that uses fault trees to identify faults caused by the same set of causes or conditions. Such common cause faults can be fatal in case of redundancy, especially in cases where a higher risk level is addressed by using redundant components rated with lower risk levels. Here a common cause fault can lead to the failure of all redundant units at once, potentially leading to a sub-system or system-wide failure. Frigerio et al. [P18] suggest that such faults should be avoided across individual components contributing to redundancy. An application of CCF is presented by Huang et al. [P27] in the context of the steer-by-wire system's hardware.

Failure Mode and Effect Analysis or FMEA ([12] in Table 4), in contrast to FTA, is a bottom up safety analysis technique [30]. The analysis starts with the possible malfunction or failure of individual components. It works backward to identify the effects of the failure in the system and which safety goals they (failure of a component) violate. The potential failure modes are typically derived from experience with similar products and processes. In our primary studies, FMEA is reported in the contexts of the hardware part of steer-by-wire system [P27], brake-by-wire system [P35], and part of ignition system [P53]. Further optimizations for streamlining FMEA are proposed in [P48].

Aging FMEA ([13] in Table 4) tailor fits FMEA to focus on aging effects for circuits in automotive. Aging FMEA proposed by Scharfenberg et al. [P57] analyze the electrical properties' change due to aging and identify aging-dependent critical hardware components that can lead to a potential hazard or safety goal violation. The method is an adaptation of FMEA assisted with simulation. They show the feasibility of the method using a fuel injection system case study.

Failure Mode Effects and Diagnostic Analysis or FMEDA ([14] in Table 4) builds on FMEA [34] with adding three aspects to each failure mode that affects safety goals: (1) failure rate or the rate at which the component experiences faults; (2) whether there is a safety mechanism to detect the failure mode or probability to detect internal failures; and (3) the effectiveness of the safety mechanism at detecting faults. The end product of this analysis consists of the hardware parts associated with each failure or safety goal and different hardware metrics that show the level of safety readiness. In primary studies, FMEDA has been applied in the contexts of hardware of anti-lock braking system [P45,P50], system-on-chip [P12], FPGA [P28], and powertrain electronics [P95].

FMEDA augmented with simulation ([15] in Table 4) is presented by Sini et al. [P61] to help designers, especially in cases where the system's behavior is highly coupled with the vehicle's behavior. They simulate the system/component and generate possible failures or misbehaviors using fault injection and then propagate these misbehaviors to the vehicle level using a vehicle dynamics simulator. They use it for failure effect classification by taking the predicted effects on dynamics and drivability of the vehicle.

Component Integrated Component Fault Trees or C²FTs ([3] in Table 4) are proposed as a combination of FTA and FMEA [35]. The resulting tree structure's root nodes represent safety goal violations or hazards of a system, leaf nodes represent basic failure modes, and the intermediate nodes present the relation between failure modes and hazards with Boolean gates. Domis et al. [P16] use C²FT in the context of product lines.

Dependent Failure Analysis or DFA ([16] in Table 4) focus on safety goal violation due to possible common cause(s) and cascading failures between elements [33]. DFA aims to identify the common causes that can violate required independence or freedom from interference between elements and, in turn, causes a safety goal violation. Nardi et al. [P50] mentions the usage of this method in the case study of an anti-lock braking system.

Model based safety analysis or MBSA ([4] and [7] in Table 4) is an umbrella term that is used to denote any safety analysis that uses a (formal) system model created ideally using a model-based development process, extended with a fault model [36]. Using a system model in the safety analysis can minimize subjectivity and be more complete, consistent, and error-free than using an informal system model or no model. The underlying safety analysis technique(s) can be any of the above-discussed techniques. MBSA, in conjunction with FTA and FMEA, is reported in primary studies [P48,P53,P84]. In addition, a study by Tlig et al. [P70]

extends MBSA with simulation for safety analysis of automated driving systems.

Safety analysis techniques: There are 13 distinct techniques for safety analysis and similar steps discussed across 28 primary studies. These techniques build on two base techniques: (1) the top-down Fault-Tree Analysis or FTA; and (2) the bottom-up Failure Mode and Effect Analysis or FMEA. FMEA and its extensions are predominantly reported in hardware-specific contexts, while FTA and its extensions dominate usage in systems and software. While ISO 26262's process dominates the underlying process for which these techniques are used, a good number of primary studies (5 out of 28) do not specify any process.

5.2. Analysis

We analyze the techniques presented in the prior section regarding their scope and context of usage. Based on this information and the comparison presented in the preceding section, we present research gaps and upcoming domain trends.

Each step in safety requirement elicitation can be conducted using multiple kinds of techniques. Especially for beginners, it is important to understand which techniques can be employed in a given context; for educators, which techniques to teach. Our study can aid in these directions. We find that no one technique fits all levels of an application or all use-cases for any step in the safety requirement elicitation. For any real-life use case, we believe it is best to use a combination of techniques to identify safety requirements. Each technique has its strengths and drawbacks. For instance, FTA can easily be applied for the safety analysis at system, software, and hardware levels; however, it might not be able to find dependent failures. To the best of our knowledge, no cheat sheet lists the strengths and drawbacks of individual techniques. Our taxonomy is a mere first step in this direction. However, an in-depth comparison of the techniques for their use in the automotive context is out of the scope of this study and is an essential future research direction.

No silver bullets: No one technique fits all application contexts; it is best to use a combination of techniques to identify safety requirements.

The repeatability of safety requirement elicitation techniques is a key factor in ensuring safety from a safety engineering and requirements engineering perspective. For instance, one element in the safety certification in almost all domains is based on an assessment by an independent team by repeating or assessing the safety cases. Such activities require objective safety requirement elicitation. The primary studies show that most methods rely on expert knowledge, rendering them subjective. Surprisingly there is little effort to quantify the subjectivity. We found only one study

on the subjectivity of a technique, which focused on a specific risk-assessment technique [P30]. Even though methods like model-based safety analysis are proposed to increase reliability and repeatability of the safety analysis, (1) their adoption rate is low (only one of the primary studies uses model-based safety analysis in their case study), and (2) there are fewer such methods for hazard analysis and risk assessment.

Repeatability: Most methods rely on expert knowledge rendering them subjective and thus hampering repeatability. We emphasize the need for standardized, tool-supported techniques to reduce subjectivity.

Informed by our taxonomy of techniques presented in the prior section, we foresee four aspects that need further exploration: (1) comparison among techniques; (2) completeness and coverage of safety requirements; (3) lack of techniques to support steps of newer processes; and (4) whether the current techniques are a match for the new application contexts arising along with the automated and connected driving. We elaborate on each of these aspects below.

Comparison among techniques is necessary to identify the most suited techniques for use by both practitioners and researchers. There is little empirical evidence on which method to choose among the available options. Current studies only compare the techniques FTA, FMEA, and STPA, where STPA is considered as a technique rather than a process [P33,P89]. Existing studies argue that STPA is better than FTA and FMEA. However, no studies specify the scope of the techniques which could allow practitioners to make an informed decision on which technique to choose for a specific use case. Also, most of the studies that compare the methods are on toy case studies, which might not represent methods' real-world efficacy.

Comparison: There is a lack of studies that systematically compare the requirement elicitation techniques.

Ensuring the completeness and coverage of safety requirements is essential for the rest of the development process. Failing to ensure this can lead to high costs, impact the timeline of product development, and potentially catastrophic consequences during operation [37,38]. However, we did not find any studies that look in this direction for any of the specified techniques.

Completeness & coverage: Completeness and coverage of safety requirements, especially in the context of automated and connected driving, are seldom explored.

Any process for safety requirements is ineffective unless there are systematic techniques to support or perform the individual steps in the process. Even though the steps in newer processes like STPA are similar to the

steps from more established processes like the one from ISO 26262, the way to conduct them and their intended outcomes are either different or have different scopes. Thus the techniques to conduct the steps in traditional techniques do not apply to the newer processes, and we did not find any other systematic techniques in the primary studies to conduct the individual steps. For example, no systematic method to perform the individual steps of STPA is used in any of the primary studies that apply STPA [P27,P40,P42,P87,P91,P98]. Rather these studies use informal guidance and previous examples to conduct STPA. The only exception is a technique for hazard analysis, namely iterative hazard analysis ([7] in Table 2), which is specified to conduct a step similar to hazard analysis in a new process for automated driving ([5] in Fig. 4).

New processes versus old techniques: The newer processes, especially based on fundamentally different approaches, lack systematic techniques to support their steps.

One primary enabler for current innovations in automated and connected driving is the use of ML-based sub-systems, especially for perception and planning [19]. Most of the techniques mentioned in this section were developed in and for an era prior to the development of these technologies. The special-purpose hardware like Neural Processing Units uses a different style of instruction execution than traditional processing units [39]. The applicability and adequacy of current techniques, which might be built on the assumptions for traditional general-purpose hardware, need further studies. It is also yet to be seen whether the current techniques can be applied in the context of safety requirements for developing neural networks, which are increasingly used in perception and planning subsystems of automated driving stacks.

ML-based systems: The adequacy of current techniques to elicit requirements for special purpose hardware and ML-based software is yet to be seen.

6. IMPLICATIONS

We presented a taxonomy and comparison between different processes. One use-case of this work is as a cheat sheet or guidebook for practitioners and educators. This work outlines what exists in the peer-reviewed literature in almost every technical dimension of automotive safety requirement elicitation.

This study has broad implications from research to practice. We present the implications in the rest of this section in the following five parts:

- *current state* of safety requirement elicitation;
- a trend of creating *islands of knowledge*;
- the *changing landscape* of the automotive domain;

- the lessons that can be learned and reused *beyond automotive software engineering*; and
- *education*.

6.1. Current State

We discuss two aspects of the current state of safety requirement elicitation research: *maturity* of the research field and *transparency & replicability* of the primary studies.

Maturity: The safety requirement elicitation for older technologies has matured while the newer concepts need further research. Four ways to empirically measure the maturity of a research area are (1) author divergence [40], where a diverse set of authors indicate a mature research field; (2) prevalence of case studies [41] where the bulk of case studies point to maturity; (3) relation between academic work and what is applied in the field [40,42] where more evidences of industry/practitioner participation form an indicator of maturity; and (4) convergence of best practices [42] where a majority of studies showing adaptation of a set of similar practices indicate maturity. Based on these four parameters, we classify the safety requirement elicitation into two contexts: for traditional components and the newer age concepts and components.

We define traditional components as the components in production for more than a decade. Examples are the steering system and most items belonging to vehicle-centric functional components as shown in Fig. 6. We define newer age concepts as those that have not entered or are currently entering the production stage and components that enable the implementation of the concepts. Example concepts are highly automated driving and example components are ML-based perception systems that enable highly automated driving. The safety requirement elicitation relating to the former context (traditional components) is more mature than the latter based on the above mentioned four metrics. The evidences are high author divergence, a wide range of case studies, and increased industry participation (based on author affiliation). For the fourth metric, the convergence of best practices, we have two angles: processes and techniques. In the context of processes, we can see convergence to ISO 26262. In the context of techniques, we can see convergence to brain-storming and related techniques for hazard analysis, usage of metrics from ISO 26262 for risk assessment, and FTA and FMEA-related techniques for safety analysis.

Transparency & replicability: A majority of the primary studies do not specify details on techniques that the studies employ, hampering transparency and replicability. In the case of hazard analysis, many studies do not specify which technique they use for hazard

analysis; instead, they directly present the results of hazard analysis. For risk assessment, the assumptions on coming up with a specific value for exposure, controllability, and severity are often not specified. For safety analysis, the intermediate results are often not presented, making it hard to understand and replicate the final result. For future studies, we recommend reporting the techniques, intermediate results from these techniques, associated assumptions, and their scope.

6.2. Islands of Knowledge

From our 102 primary studies, we noticed a systematic trend of creating islands of knowledge inside companies where the detailed knowledge on safety requirement elicitation stays inside the companies and are not available via peer reviewed publications. We present two related aspects below.

Sharing specifications, intermediate results, and related data of research: Continuing our prior discussion on *transparency & replicability*, the majority of the studies, except for a few (e.g., [P32]), do not share the details on case studies. For example, an operational design domain (ODD) definition is essential for making an informed judgment on any result of hazard analysis of a system. However, most studies do not provide details but only discuss the final result. The assumptions (e.g., exclude snowing conditions) during the process and the intermediate steps (e.g., fault trees; hazardous events) are essential to judge the results produced in the articles and, most importantly, to build on for future studies. In its current format, this “*unknown details*” makes it difficult for newer researchers and other related disciplinarians to enter this field. The sharing of related data on research should be the norm as in other software engineering fields like mining software repositories.

Sharing real-case studies: Given the existence of myriad vehicle types with various capabilities, it is safe to assume that considerable safety requirement elicitation has been performed for their development. Yet, to our knowledge, no real-world, industry-scale case studies have been published on this topic in peer-reviewed literature. So far, publications in collaboration with industries either use toy case studies (e.g., [P1]) or very high-level abstractions (e.g., [P86]) hampering any real-world reproducibility. The publication of real-world case studies can help researchers and the automotive community to identify current issues facing the industry and contribute to rectifying and proposing methods and techniques, rather than creating islands of knowledge inside companies. This can reduce the work to re-invent the knowledge and benefit the companies to get better talent and suggestions from academia. Additionally, with the higher reliance on software and related components for automated and

connected driving, openness to independent safety verification/certification (in contrast to self-certification) should be made a norm.

6.3. Changing Landscape

Is safety requirement elicitation catching up? The last decade marks arguably the most significant paradigm shift in the automotive industry since its inception. Four dimensions of this shift are the transition from internal combustion to electrification, automated and connected driving, ongoing shift to open source software development, and start-ups entering the field and finding success bringing disruptive ideas and new business models. This means profound changes in almost all dimensions of automotive software and the electronics that run them. Whether the safety requirements elicitation is catching up is still an open question. There is relatively more research on transition to electrification (especially on battery and power-train) as evident from Fig. 6. The open-sourcing trend is still unfolding [19] and its safety requirement elicitation side might be too early to research. Automated and connected driving is achieved by combining special purpose hardware, ML-based software, and traditional software to make them work seamlessly. We discuss three dimensions of this topic further: (a) functional safety; (b) safety of intended functionality in the context of ML-based components; and (c) connected driving-specific issues. All the above aspects are particularly challenging to safety certification bodies across the globe.

Another paradigm change happening in automotive industry is over-the-air-updates (OTA). Through OTA new features are introduced and bug-fixes for existing features are performed. When safety-critical functionalities are either introduced or updated via OTA, how to evaluate implications on safety requirements and safety analysis is unclear. The current methodologies does not consider such updates.

ML-based components & functional safety. Both software and hardware components specific to ML (and mainly neural networks) function fundamentally different from traditional components. For example, the software components are built from data rather than human logic. The hardware components are based on multi-threaded execution, parallelism, and many levels of optimizations compared to non-parallel execution units otherwise used. Given the ML-based components are now becoming a part of safety-critical applications, we need (functional) safety requirement elicitation methods that take the peculiar nature of these components into account, which is not the case currently. This might need thinking with a different perspective altogether than the traditional kinds.

When we look at the case studies (on functional safety), the vast majority use traditional processes and techniques. Even though newer methods and techniques for automated and connected driving are proposed, there is little evidence for their applicability and suitability in the real world. Also, the sufficiency of current processes and techniques to address ML-based systems is another daunting question for industries and safety certification bodies. Multiple processes and techniques might be applicable to ML-based systems. While our study presents a comparison among processes, no study on in-depth comparison of techniques, in the context of the automotive domain. To summarize, there are many potential directions for research in the ML-based component's context, including case studies on newer processes and techniques and in-depth comparison among existing techniques for their suitability, sufficiency, and scope.

ML-based components & safety of intended functionality. Safety of intended functionality, especially in the context of removing the human operator fallback, is out of the scope of traditional processes and techniques. Even though methods like STPA is developed to cover some aspects, its real-world adaption is low, and so far, the scope of STPA is at the system level. The standard, ISO 21448, is proposed to tackle the safety of intended functionality. It is still in its beginning stage and gives only conceptual directions than concrete guidelines. Safety of intended functionality in both hardware and software levels still needs processes and techniques that can be applied to special purpose hardware like neural processing units. The processes and techniques could be entirely new, extension of current ones, or studies show that existing techniques are applicable in such settings.

Formal modeling and verification for functional safety and safety of intended functionality. While formal modeling and verification is a mature field which can be used to demonstrate and ensure safety guarantees, only a small fraction of the primary studies [P17,P48, P53,P70,P84] at least mentions some form of modeling or verification being employed. From both a functional safety and safety of intended functionality perspective, there is research and practice gap for a more comprehensive treatment. This could be formal modeling of (parts) of the system combined with model checking and conformance testing. We believe that limitations and feasibility of application of such formal methods to completely automated driving in real-life settings need to be explored further.

Connected driving specific issues. There can be three kinds of communications connected driving: vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-road users (V2R). The first two kinds are more established than the third kind. As we mentioned in Section 4, there is a lack of methods that integrates V2I along with the traditional automotive safety requirement elicitation. There are at least two challenges here, (1) safety requirement elicitation for communication intermediaries like cloud for connected driving¹² and (2) requirements spanning across multiple vendors (e.g., the manufacturers for smart traffic infrastructure and vehicles might be different). Further research is needed in these two directions.

While vulnerable road users form about a third of fatalities in road accidents in the USA¹³, safety requirement elicitation for vehicle-to-road user communication is not mentioned in any of the primary studies. It is still an open question how to complement the information on road users (cyclists and pedestrians) beyond vehicle sensors (like camera and LiDAR) and remove their blind spots. Safety requirement elicitation regarding the same is also in its nascent stages and needs further research.

6.4. Multi-Disciplinarity: Beyond Automotive Software Engineering

This article explored the technical dimension of safety requirement elicitation. However, there are other dimensions, e.g. combining safety requirement elicitation with aspects like security, tool support, and the human and social factors of safety requirement elicitation. These directions are yet to be explored.

While this article considered a system and software view of safety requirement elicitation, the area is primarily multi-disciplinary, as shown in Fig. 3c. Also, there are similar domains like advanced robotics (e.g., robots from Bostodynamics)¹⁴, which are multi-disciplinary, with similar challenges in perception systems and unsupervised deployment (in the future). It might be interesting to see how these domains compare and what can be learned from each discipline.

6.5. Education

The next generation of engineers who will have to build more of these new systems is being educated today. In the context of software engineering, most

¹² Connected driving refers to a set of vehicles and traffic infrastructure communicate various parameters to optimize the collective traffic behavior. This communication is often achieved by using intermediaries such as cloud.

¹³ <https://crashstats.nhtsa.dot.gov/Api/Public/Publication/813178>

¹⁴ <https://www.bostodynamics.com>

curricula do not focus on safety, let alone the safety of the newer types of systems. Since software systems are becoming more safety-critical, this trend needs to change, and safety has to be incorporated as a topic. We believe it is equally important to educate on the caveats and limitations of current techniques since it is crucial to understand the scope of existing processes and techniques for their correct usage in real-life. Also, in typical software engineering curricula, a systems view is seldom included but is crucial in the context of safety requirements. We strongly encourage including this in the curricula for educating future software engineers.

From a practitioner's perspective, it might be difficult to have a definitive idea on which processes and techniques to use in different contexts, especially for ML-based systems. While this article can be used as a cheat-sheet, there is still room for an in-depth comparison of the techniques. Some directions are: (a) the scope and possible application contexts of each technique; and (b) objective criteria on when to and when not to choose a technique.

7. THREATS TO VALIDITY

This section presents the threats inherent in our study despite our best attempts at mitigating them during design, implementation and interpretation. Below we use the framework by Cook and Campbell [43] to discuss the threats to validity.

Construct validity: For a systematic literature review to be useful, the articles analyzed should be representative, presenting an overview. To identify representative scientific articles, we employed multiple methods, including:

1. the PICO method (see [Section 2.2](#)) to create the search string;
2. both forward and backward snowballing on the primary studies to improve the coverage of relevant research articles and to make the process as insensitive to the choice of the search string and databases as possible;
3. documentation of our search process, inclusion-exclusion criteria and information extracted from the selected articles for transparency and replicability of our research; and
4. independently assessing the intermediate steps as authors and resolving disagreements with discussions. Still, we might have missed relevant articles, for instance, non-peer-reviewed articles.

Conclusion validity: In comprehending the scientific literature for presenting insights, we foresee two threats: one, characteristics of the available literature, and two,

researcher bias in interpretation. For the first part, we have limited control over the availability of scientific literature. For instance, we observed that case studies on real-life vehicles could have added deeper insights for investigation. Unfortunately, such studies are limited. To mitigate researcher bias in interpretation, we followed the definitions from the literature and did not make assumptions or choices if the text was not clear. Also, we explicitly defined the criteria we followed to ensure objectivity.

Internal validity: As indicated above, our findings are susceptible to publication bias since we only analyze published scientific literature. Our choices ensure that our analysis rests on systematic scientific findings but implies that non-peer-reviewed articles (e.g., negative results) are systematically removed. It is possible that a study including other sources of information can present a different picture than the one depicted here.

External validity: The representativeness of our study hinges on the domains we considered for our analysis and the representativeness of the studies within these domains. We search for relevant articles on a broader range: using multiple databases and applying techniques such as snowballing. But our investigation is also limited by our choices to study articles written in English, non-grey literature, and published in reputed venues. All of the above factors influence our findings' generalizability and define the scope within which our results apply.

8. RELATED WORK

We classify the secondary studies that cover safety requirements during product development into three categories: (i) studies applicable to multiple domains; (ii) studies on safety assurance; and (iii) studies that focus on the automotive domain. Since our scope is limited to safety, we do not discuss secondary studies on the intersection of safety and security. This section discusses relevant secondary studies and excludes primary studies as this article is a secondary study.

8.1. Cross Domain Studies

Pereira et al. conducted an SLR on requirements to be considered and on requirement engineering practices a challenges in developing embedded systems [6]. They summarize open issues that can be potential research directions, which include: “Requirements Specification for automotive system”; “Improve the development process for ensure functional safety requirements”; “Handling of non-functional requirements such as ..., safety, ...”; “Specification of safety requirements”; and “Analysis of hazard and threats, ..., and safety”.

Martins et al. present an SLR on approaches to elicit, model, specify and validate safety requirements in the context of safety-critical systems and usage of these approaches in industrial settings [5]. This work forms a precursor to our study, as detailed in [Section 2.2](#).

Vilela et al. performed an SLR to explore methods to improve the integration between RE and safety engineering [7]. They identified techniques and tools used for hazard analysis and safety analysis (to be) used by requirement engineering and safety engineering teams. They also generated a taxonomy of these techniques along with a separate taxonomy of the safety information used or generated by these techniques. Vilela et al. also performed a systematic mapping study on approaches to improve the integration of specification, analysis, and exchanging information on all artifacts involved in the requirements engineering process among stakeholders [44]. Most of the approaches found by this study are domain-independent (78%), while 5% of them are specific to the automotive domain. The study also found that over 76% of the approaches do not follow any safety standard. These studies are complementary to our focus.

Bozhinoski et al. [8] presents a systematic mapping study on managing safety in mobile robotic systems from a software engineering perspective. Their primary studies on safety management in the context of self-driving cars conclude that *“self-driving vehicles lack a standardized platform, processes, and tools for designing and analyzing safety approaches”* [8]. However, they did not consider safety standards from the automotive domain.

Another direction pursued in literature is functional safety in product line engineering. Baumgart et al. conducted a systematic mapping study to summarize topics covered and evaluation approaches used in the literature on the functional safety of product lines [9]. Gadelha Queiroz et al. performed an SLR for identifying approaches, methods, and methodologies from the intersection of the product line engineering and model-driven engineering for safety-critical systems [45]. We consider this direction of research out of scope for this work.

8.2. On Safety Assurance

Safety assurance is about providing evidence that safety is ensured. Safety requirements are a part of safety assurance, and in this SLR, we focus on eliciting functional safety requirements. Nair et al. conducted an SLR towards establishing evidence for system safety [46]. They focused on three aspects: the information that constitutes evidence; structuring of evidence; and evidence assessment. There are also

model-based methods based on goal structured notation and conceptual models for establishing evidence for system safety [47,48,49].

Bolbot et al. examined different sources of complexity introduced to cyber-physical systems and explained different methods for safety assurance in those contexts [50]. This work does not specify methods used in the automotive domain nor uses any systematic method to identify the different techniques in the literature for safety assurance.

Glairscher et al. performed a rigorous literature survey on design and argument patterns for the assurance of system safety [51]. They primarily focus on reusable design patterns and categorize them into software, electrical/electronic, and mechanical hardware.

Ingbergsson et al. [52] conducted a systematic mapping study on (coding) practices in developing safety-critical software for field robots. Field robots are machinery for outdoor tasks like agriculture. They concluded that most approaches propose solutions to attain safety, focus on behavior modeling, and do not stress reliable software development e.g. involving formal verification. Half of the literature they considered uses non-standardized methods to develop software. They also note an increase in safety-related issues with the introduction of computer vision.

In this work, we concentrate on approaches for generating safety requirements rather than safety assurance. However, conclusions from these studies, for example, the nascence of technologies like computer vision which does not follow traditional development methods, equally, apply in the context of our work.

8.3. On Safety in the Automotive Domain

Some secondary studies from the last decade discuss safety and are specific to the automotive domain. A few studies ([53,54]) outline safety-related methods across the entire product life cycle, while others focus on a specific stage of product development [55], a specific technology [56] or a specific use-case [57]. In addition to the secondary studies, there is a proliferation of experience reports [58,59]. We do not cover experience reports in our related work since they form a different class of studies than secondary studies.

Studies by Kannan et al. and Gosavi et al. consider the entire product life cycle [53,54]. Kannan et al. [53] present a gap analysis between the objectives of the ISO 26262 standard and safety-related techniques to achieve these objectives. They conclude that there is a need for tooling for conducting HARA, combining sub-phases of product development, integration among the product development phases of design, requirement

management, and validation and verification. They also find a lack of methods for ASIL decomposition for large-scale systems.

Gosavi et al. [54] summarize four primary studies from the product development phase at the system, hardware, and software levels covered by parts 4, 5, and 6 of ISO 26262. They noted the lack of a standard and inadequacy of ISO 26262 to address functional safety in the development of autonomous and semi-autonomous vehicles.

Gheraibia et al. [55] reviewed different approaches for the specific sub-phase of product development, ASIL allocation. ASIL allocation methods find optimal allocations of ASILs (QM, A, B, C, D, with QM being negligible risk and D being highest risk) to system architecture components such that safety requirements are guaranteed to be met at the lowest possible cost. They classify approaches for ASIL allocation into two categories – exact and optimization approaches – and present the pros and cons of each method.

Borg et al. present a short review of validation and verification (V&V) methods for the safety of the specific technology, machine learning and deep learning methods, to be used in the automotive domain [56]. They classify support for V&V of machine learning and deep learning-based systems as formal methods, control theory, probabilistic methods, process guidelines and simulated test cases. They conclude that the V&V methods for machine learning and deep learning lag compared to other areas. Also, those V&V methods suggested by ISO 26262 do not apply to developing components that use machine learning and deep learning methods. They stress the need for a new standard for them.

Axelsson [57] presented an SLR and a gap analysis on safety in the specific use-case of platooning. Platooning is a coordinated movement of vehicles as a train with minimal distance between vehicles in the pack. Specifically, they focus on safety analysis methods, hazards and failures, and solutions to improve safety for platooning. The authors also note a lack of studies from commercial settings and current research primarily from research prototypes or technology demonstrators.

Even though many of these studies overlap with our work, we did not find any systematic study on eliciting safety requirements for the automotive domain.

9. CONCLUSIONS

This work characterizes safety requirement elicitation in the automotive domain and presents a comprehensive overview of the pre-GPT era landscape through a systematic literature review. This article is a first step

in the direction of summarizing, taxonomizing and comparing processes and techniques for safety requirement elicitation from the automotive domain.

We identified nine safety requirement elicitation processes and 38 distinct techniques. Out of the nine processes, we observed that the process outlined in the ISO 26262 standard forms the basis for requirements elicitation in the automotive industry. Other processes have been proposed to complement, extend or replace the process outlined in the standard. This article offers an overview, comparison and taxonomy of such processes and corresponding techniques for safety requirement elicitation in the automotive domain. Based on this information, temporal adoption trend, usage context and scope, we presented research gaps and discussed current domain trends.

We empirically showed the immaturity of the safety requirement elicitation concerning newer concepts and components like automated and connected driving. For instance, the majority of processes and techniques for safety requirement elicitation were proposed more than two decades ago. At the same time, the upcoming perception and decision systems for automated driving rely on ML-based components whose feasibility of usage in real-world scenarios (e.g., neural networks) was demonstrated only a decade ago. The applicability and scope of the processes and techniques to these new-age components is still an open question. Another example is the lack of studies on safety requirements regarding traffic infrastructure and communication with vulnerable road users, which are critical to accomplishing connected driving. Other dimensions, e.g. combining safety requirement elicitation with aspects like security, tool support, and the human and social factors of safety requirement elicitation, are yet to be explored.

We emphasize the importance of safety requirement elicitation of software and related systems and show the importance of a systems and multi-disciplinary perspective. This work opens up many future avenues for research and provide a concise and comprehensive guide to practitioners and educators.

Conflict of Interest

The authors declare that they have no conflicts of interest. Note that because the third and fourth authors of this article are Editors-in-Chief of the journal, the peer review process has been managed without any involvement from these Editors-in-Chief.

Data Availability

This article is self-contained and any further data that support the findings of this study are available on request.

Funding

This work is part of the i-CAVE research programme (14897 P14–18) funded by the NWO (Netherlands Organisation for Scientific Research).

Authors' Contribution

S. Kochanthara contributed to study conceptualization, study design, study implementation and writing of the manuscript. L. Cleophas, Y. Dajsuren and M. van den Brand supervised the study and contributed to the writing (reviewing & editing) of the manuscript.

REFERENCES

- [1] I. Solaiman, Z. Talat, W. Agnew, L. Ahmad, D. Baker, S.L. Blodgett, et al. Evaluating the Social Impact of Generative AI Systems in Systems and Society. arXiv preprint arXiv:2306.05949, 2023.
- [2] ISO. BS ISO 26262-10:2018. Road Vehicles. Functional Safety - Guidelines on ISO 26262. Geneva, Switzerland: BSI, 2018.
- [3] ISO. ISO/PAS 21448:2022. Road Vehicles — Safety of the Intended Functionality. Geneva, Switzerland: International Organization for Standardization (ISO), 2022.
- [4] K. Czarnecki. Automated Driving System (ADS) High-Level Quality Requirements Analysis. Driving Behavior Comfort. Waterloo Intelligent Systems Engineering (WISE) Lab Report, University of Waterloo, Waterloo, Canada, 2018.
- [5] L.E.G. Martins, T. Gorschek. Requirements Engineering for Safety-Critical Systems: A Systematic Literature Review. *Information and Software Technology*, 2016, 75: 71–89.
- [6] T. Pereira, D. Albuquerque, A. Sousa, F.M. Alencar, J. Castro. Retrospective and Trends in Requirements Engineering for Embedded Systems: A Systematic Literature Review. *Proceedings of the CIBSE Conference*. Buenos Aires, Argentina: CIBSE, #SLR, IEEE, 2017, pp. 427–440.
- [7] J. Vilela, J. Castro, L.E.G. Martins, T. Gorschek. Integration Between Requirements Engineering and Safety Analysis: A Systematic Literature Review. *Journal of Systems and Software*, 2017, 125: 68–92.
- [8] D. Bozhinoski, D. Di Ruscio, I. Malavolta, P. Pelliccione, I. Crnkovic. Safety for Mobile Robotic Systems: A Systematic Mapping Study from a Software Engineering Perspective. *Journal of Systems and Software*, 2019, 151: 150–179.
- [9] S. Baumgart, J. Fröberg. Functional Safety in Product Lines—A Systematic Mapping Study. *Proceedings of the 2016 42nd Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*. Limassol, Cyprus: IEEE, 2016, pp. 313–322.
- [10] B. Kitchenham, S. Charters. Guidelines for Performing Systematic Literature Reviews in Software Engineering. EBSE Technical Report, Keele University, Keele, UK, 2007.
- [11] P. Garner, S. Hopewell, J. Chandler, H. MacLehose, E.A. Akl, J. Beyene, et al. When and How to Update Systematic Reviews: Consensus and Checklist. *BMJ*, 2016, 354: i3507.
- [12] M. Petticrew, H. Roberts. *Systematic Reviews in the Social Sciences: A Practical Guide*. Hoboken, NJ, USA: Wiley, 2008, p. 354.
- [13] K. Petersen, S. Vakkalanka, L. Kuzniarz. Guidelines for Conducting Systematic Mapping Studies in Software Engineering: An Update. *Information and Software Technology*, 2015, 64: 1–18.
- [14] S. Tiwari, A. Gupta. A Systematic Literature Review of use Case Specifications Research. *Information and Software Technology*, 2015, 67: 128–158.
- [15] R. Wieringa, N. Maiden, N. Mead, C. Rolland. Requirements Engineering Paper Classification and Evaluation Criteria: A Proposal and a Discussion. *Requirements Engineering*, 2006, 11: 102–107.
- [16] E. Mendes, C. Wohlin, K. Felizardo, M. Kalinowski. When to Update Systematic Literature Reviews in Software Engineering. *Journal of Systems and Software*, 2020, 167: 110607.
- [17] V. Garousi, J.M. Fernandes. Highly-Cited Papers in Software Engineering: The Top-100. *Information and Software Technology*, 2016, 71: 108–128.
- [18] L. Bornmann. How are Excellent (Highly Cited) Papers Defined in Bibliometrics? A Quantitative Analysis of the Literature. *Research Evaluation*, 2014, 23(2): 166–173.
- [19] S. Kochanthara, Y. Dajsuren, L. Cleophas, M. van den Brand. Painting the Landscape of Automotive Software in GitHub. *Proceedings of the 19th International Conference on Mining Software Repositories (MSR '22)*. New York, NY, USA : ACM, 2022, pp. 215–226.
- [20] C. Wohlin. Guidelines for Snowballing in Systematic Literature Studies and a Replication in Software Engineering. *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering (EASE '14)*. New York, NY, USA : ACM, 2014, pp. 1–10.
- [21] J. Cohen. Weighted Kappa: Nominal Scale Agreement Provision for Scaled Disagreement or Partial Credit. *Psychological Bulletin*, 1968, 70(4): 213–220.
- [22] J. Cohen. A Coefficient of Agreement for Nominal Scales. *Educational and Psychological Measurement*, 1960, 20(1): 37–46.

- [23] J.R. Landis, G.G. Koch. The Measurement of Observer Agreement for Categorical Data. *Biometrics*, 1977, 33(1): 159–174.
- [24] N.G. Leveson, J.P. Thomas. *STPA Handbook*. Cambridge, MA, USA: MIT, 2018, pp. 1–188.
- [25] IEC. IEC Functional Safety and IEC 61508. Standard, International Electrotechnical Commission. Geneva, Switzerland: IEC, 2010.
- [26] S. Baumgart, J. Fröberg, S. Punnekkat. Analyzing Hazards in System-of-Systems: Described in a Quarry Site Automation Context. *Proceedings of the 2017 Annual IEEE International Systems Conference (SysCon)*. Montreal, QC, Canada: IEEE, 2017, pp. 1–8.
- [27] M. Broy, I.H. Kruger, A. Pretschner, C. Salzmann. Engineering Automotive Software. *Proceedings of the IEEE*, 2007, 95(2): 356–373.
- [28] E. Gracic, F. Svensson, J. Ehrich, O. Beck, M. Jansen. Concept for Safety-Related Development of Deep Neural Networks in the Automotive. *Proceedings of the 2020 Fourth International Conference on Multimedia Computing, Networking and Applications (MCNA)*. Valencia, Spain: IEEE, 2020, pp. 10–15.
- [29] W.S. Lee, D.L. Grosh, F.A. Tillman, C.H. Lie. Fault Tree Analysis, Methods, and Applications—A Review. *IEEE Transactions on Reliability*, 1985, 34(3): 194–203.
- [30] D.H. Stamatis. *Failure Mode and Effect Analysis: FMEA From Theory to Execution*. Milwaukee, WI, USA: ASQ Quality Press, 2003, p. 455.
- [31] T.A. Kletz. Hazop—Past and Future. *Reliability Engineering and System Safety*, 1997, 55(3): 263–266.
- [32] T. Aven, B. Heide. Reliability and Validity of Risk Analysis. *Reliability Engineering and System Safety*, 2009, 94(11): 1862–1868.
- [33] B.D. Johnston. A Structured Procedure for Dependent Failure Analysis (DFA). *Reliability Engineering*, 1987, 19(2): 125–136.
- [34] W.M. Goble, A.C. Brombacher. Using a Failure Modes, Effects and Diagnostic Analysis (FMEDA) to Measure Diagnostic Coverage in Programmable Electronic Systems. *Reliability Engineering and System Safety*, 1999, 66(2): 145–148.
- [35] D. Domis. *Integrating Fault Tree Analysis and Component-Oriented Model-Based Design of Embedded Systems*. München, Germany: Verlag Dr. Hut, 2012.
- [36] A. Joshi, M. Whalen, M.P. Heimdahl, S.P. Miller. *Model-Based Safety Analysis: Final Report*. Technical Report. Minneapolis, MN, USA: University of Minnesota, 2005.
- [37] M. Wilikens, M. Masera, D. Vallerio. Integration of Safety Requirements in the Initial Phases of the Project Lifecycle of Hardware/Software Systems. In: P. Daniel (Eds.), *Safe Comp 97*. London: Springer, 1997, pp. 83–97.
- [38] A. Saeed, R. de Lemos, T. Anderson. On the Safety Analysis of Requirements Specifications for Safety-Critical Software. *ISA Transactions*, 1995, 34(3): 283–295.
- [39] Y. Chen, Y. Xie, L. Song, F. Chen, T. Tang. A Survey of Accelerator Architectures for Deep Neural Networks. *Engineering*, 2020, 6(3): 264–274.
- [40] M.J. Maloni, C.R. Carter, A.S. Carr. Assessing Logistics Maturation Through Author Concentration. *International Journal of Physical Distribution and Logistics Management*, 2009, 39(3): 250–268.
- [41] M.J. Cheon, V. Groven, R. Sabherwal. The Evolution of Empirical Research in IS: A Study in IS Maturity. *Information and Management*, 1993, 24(3): 107–119.
- [42] A. Neely. The Evolution of Performance Measurement Research: Developments in the Last Decade and a Research Agenda for the Next. *International Journal of Operations and Production Management*, 2005, 25(12): 1264–1277.
- [43] C. Wohlin, P. Runeson, M. Höst, M.C. Ohlsson, B. Regnell, A. Wesslén. *Experimentation in Software Engineering*. Berlin, Heidelberg: Springer, 2012.
- [44] J. Vilela, J. Castro, L.E.G. Martins, T. Gorschek, C. Almendra. Requirements Communication in Safety-Critical Systems. *Proceedings of the 22nd Workshop on Requirements Engineering (WER2019)*. Brazil, 2019.
- [45] P.G.G. Queiroz, R.T.V. Braga. Development of Critical Embedded Systems Using Model-Driven and Product Lines Techniques: A Systematic Review. *Proceedings of the 2014 Eighth Brazilian Symposium on Software Components, Architectures and Reuse*. Maceió, Brazil: IEEE, 2014, pp. 74–83.
- [46] S. Nair, J.L. de La Vara, M. Sabetzadeh, L. Briand. An Extended Systematic Literature Review on Provision of Evidence for Safety Certification. *Information and Software Technology*, 2014, 56(7): 689–717.
- [47] R.K. Panesar-Walawege, M. Sabetzadeh, L. Briand, T. Coq. Characterizing the Chain of Evidence for Software Safety Cases: A Conceptual Model Based on the IEC 61508 Standard. *Proceedings of the 2010 Third International Conference on Software Testing, Verification and Validation*. Paris, France: IEEE, 2010, pp. 335–344.
- [48] J.L. de la Vara, R.K. Panesar-Walawege. SafetyMet: A Metamodel for Safety Standards. In: A. Moreira, B. Schätz, J. Gray, A. Vallecillo, P. Clarke (Eds.), *Proceedings of the 16th International Conference on Model-Driven Engineering Languages and*

- Systems. MODELS 2013. Lecture Notes in Computer Science, Vol. 8107. Berlin, Heidelberg: Springer, 2013, pp. 69–86.
- [49] J.L. de la Vara, A. Ruiz, K. Attwood, H. Espinoza, R.K. Panesar-Walawege, A. López, et al. Model-Based Specification of Safety Compliance Needs for Critical Systems: A Holistic Generic Metamodel. *Information and Software Technology*, 2016, 72: 16–30.
- [50] V. Bolbot, G. Theotokatos, L.M. Bujorianu, E. Boulougouris, D. Vassalos. Vulnerabilities and Safety Assurance Methods in Cyber-Physical Systems: A Comprehensive Review. *Reliability Engineering and System Safety*, 2019, 182: 179–193.
- [51] M. Gleirscher, S. Kugele. Assurance of System Safety: A Survey of Design and Argument Patterns. arXiv preprint arXiv:1902.05537, 2019.
- [52] J.T.M. Ingibergsson, U.P. Schultz, M. Kuhrmann. On the use of Safety Certification Practices in Autonomous Field Robot Software Development: A Systematic Mapping Study. In: P. Abrahamsson, L. Corral, M. Oivo, B. Russo (Eds.), *Proceedings of the 16th International Conference on Product-Focused Software Process Improvement. PROFES 2015. Lecture Notes in Computer Science*, Vol. 9459. Cham, Switzerland: Springer, 2015, pp. 335–352.
- [53] S.M. Kannan, Y. Dajsuren, Y. Luo, I. Barosan. Analysis of ISO 26262 Compliant Techniques for the Automotive Domain. *Proceedings of the International Workshop on Modelling in Automotive Software Engineering (MASE) co-located with 2015 ACM/IEEE 18th International Conference on Model Driven Engineering Languages and Systems (MODELS)*. Ottawa, Canada: ACM/IEEE, 2015, pp. 33–42.
- [54] M.A. Gosavi, B.B. Rhoades, J.M. Conrad. Application of Functional Safety in Autonomous Vehicles Using ISO 26262 Standard: A Survey. *Proceedings of the SoutheastCon 2018*. St. Petersburg, FL, USA: IEEE, 2018, pp. 1–6.
- [55] Y. Gheraibia, S. Kabir, K. Djafri, H. Krimou. An Overview of the Approaches for Automotive Safety Integrity Levels Allocation. *Journal of Failure Analysis and Prevention*, 2018, 18: 707–720.
- [56] M. Borg, C. Englund, K. Wnuk, B. Duran, C. Levandowski, S. Gao, et al. Safely Entering the Deep: A Review of Verification and Validation for Machine Learning and a Challenge Elicitation in the Automotive Industry. *Journal of Automotive Software Engineering*, 2019, 1(1): 1–19.
- [57] J. Axelsson. Safety in Vehicle Platooning: A Systematic Literature Review. *IEEE Transactions on Intelligent Transportation Systems*, 2017, 18(5): 1033–1045.
- [58] G. Xie, Y. Li, Y. Han, Y. Xie, G. Zeng, R. Li. Recent Advances and Future Trends for Automotive Functional Safety Design Methodologies. *IEEE Transactions on Industrial Informatics*, 2020, 16(9): 5629–5642.
- [59] A. Nardi, S. Camdzic, A. Armato, F. Lertora. Design-for-Safety for Automotive IC Design: Challenges and Opportunities. *Proceedings of the 2019 IEEE Custom Integrated Circuits Conference (CICC)*. Austin, TX, USA: IEEE, 2019, pp. 1–8.

PRIMARY STUDIES

- [P1] D. Aceituna, K. Madala, H. Do. Deriving Functional Safety Requirements Using Undesired Combination State Templates. *Proceedings of the 2018 4th International Workshop on Requirements Engineering for Self-Adaptive, Collaborative, and Cyber Physical Systems (RESACS)*, Banff, AB, Canada: IEEE, 2018, pp. 1–8.
- [P2] T. Aoki, K. Traichaiyaporn, Y. Chiba, M. Matsubara, M. Nishi, F. Narisawa. Modeling Safety Requirements of ISO26262 Using Goal Trees and Patterns. In: C. Artho, P. Ölveczky (Eds.), *Formal Techniques for Safety-Critical Systems. 4th International Workshop, FTSCS 2015. Communications in Computer and Information Science*, Vol. 596. Cham, Switzerland: Springer, 2016, pp. 206–221.
- [P3] L.S. Azevedo, D. Parker, Y. Papadopoulos, M. Walker, I. Sorokos, R.E. Araujo. Exploring the Impact of Different Cost Heuristics in the Allocation of Safety Integrity Levels. In: F. Ortmeier, A. Rauzy (Eds.), *Model-Based Safety and Assessment. 4th International Symposium, IMBSA 2014. Lecture Notes in Computer Science*, Vol. 8822. Cham, Switzerland: Springer, 2014, pp. 70–81.
- [P4] L.d.S. Azevedo, D. Parker, M. Walker, Y. Papadopoulos, R.E. Araujo. Assisted Assignment of Automotive Safety Requirements. *IEEE Software*, 2014, 31(1): 62–68.
- [P5] G. Bagschik, A. Reschka, T. Stolte, M. Maurer. Identification of Potential Hazardous Events for an Unmanned Protective Vehicle. *Proceedings of the 2016 IEEE Intelligent Vehicles Symposium (IV)*. Gothenburg, Sweden: IEEE, 2016, pp. 691–697.
- [P6] G. Bagschik, T. Stolte, M. Maurer. Safety Analysis Based on Systems Theory Applied to an Unmanned Protective Vehicle. *Procedia Engineering*, 2017, 179: 61–71.
- [P7] K. Beckers, I. Côté, T. Frese, D. Hatebur, M. Heisel. Systematic Derivation of Functional Safety Requirements for Automotive Systems. In: A. Bondavalli, F. Di Giandomenico (Eds.), *Computer*

- Safety, Reliability, and Security. 33rd International Conference, SAFECOMP 2014. Lecture Notes in Computer Science, Vol. 8666. Cham, Switzerland: Springer, 2014, pp. 65–80.
- [P8] K. Beckers, I. Côté, T. Frese, D. Hatebur, M. Heisel. A Structured and Systematic Model-Based Development Method for Automotive Systems, Considering the OEM/Supplier Interface. Reliability Engineering and System Safety, 2017, 158: 172–184.
- [P9] C. Bergenhem, M. Majdandzic, S. Ursing. Concepts and Risk Analysis for a Cooperative and Automated Highway Platooning System. In: S. Bernardi, V. Vittorini, F. Flammini, R. Nardone, S. Marrone, R. Adler, et al (Eds.), Dependable Computing - EDCC 2020 Workshops. EDCC 2020. Communications in Computer and Information Science, Vol. 1279. Cham, Switzerland: Springer, 2020, pp. 200–213.
- [P10] L. Bressan, A.L. de Oliveira, F. Campos. An Approach to Support Variant Management on Safety Analysis Using CHESSE Error Models. Proceedings of the 2020 16th European Dependable Computing Conference (EDCC). Munich, Germany: IEEE, 2020, pp. 135–142.
- [P11] C.-C. Chiu, K.-S. Lin. A New Design Review Method for Functional Safety of Automotive Electrical Systems. 2018 VII International Conference on Network, Communication and Computing, ICNCC 2018. New York, NY, USA: ACM, 2018, pp. 318–326.
- [P12] S. Chonnad, R. Iacob, V. Litovtchenko. A Quantitative Approach to SoC Functional Safety Analysis. Proceedings of the 2018 31st IEEE International System-on-Chip Conference (SOCC). Arlington, VA, USA: IEEE, 2018, pp. 197–202.
- [P13] Y. Dajsuren, G. Loupias. Safety Analysis Method for Cooperative Driving Systems. Proceedings of the 2019 IEEE International Conference on Software Architecture (ICSA). Hamburg, Germany: IEEE, 2019, pp. 181–190.
- [P14] N. Das, W. Taylor. Quantified Fault Tree Techniques for Calculating Hardware Fault Metrics According to ISO 26262. Proceedings of the 2016 IEEE Symposium on Product Compliance Engineering (ISPC). Anaheim, CA, USA: IEEE, 2016, pp. 1–8.
- [P15] V. Dhaked, V. Gupta, J. Harmalkar. Application of Concept Phase to Design an Electric Powertrain in Compliance with ISO 26262. Proceedings of the 2019 IEEE 5th International Conference for Convergence in Technology (I2CT). Bombay, India: IEEE, 2019, pp. 1–5.
- [P16] D. Domis, R. Adler, M. Becker. Integrating Variability and Safety Analysis Models Using Commercial UML-Based Tools. Proceedings of the 19th International Conference on Software Product Line, SPLC 2015. New York, NY, USA: ACM, 2015, pp. 225–234.
- [P17] A. Duracz, A. Aljarboub, F.A. Bartha, J. Masood, R. Philippsen, H. Eriksson, et al. Advanced Hazard Analysis and Risk Assessment in the ISO 26262 Functional Safety Standard Using Rigorous Simulation. In: R. Chamberlain, M. Edin Grimheden, W. Taha (Eds.), Cyber Physical Systems. Model-Based Design. CyPhy WESE 2019. Lecture Notes in Computer Science, Vol. 11971. Cham, Switzerland: Springer, 2020, pp. 108–126.
- [P18] A. Frigerio, B. Vermeulen, K. Goossens. A Generic Method for a Bottom-Up ASIL Decomposition. In: B. Gallina, A. Skavhaug, F. Bitsch (Eds.), Computer Safety, Reliability, and Security. SAFECOMP 2018. Lecture Notes in Computer Science, Vol. 11093. Cham, Switzerland: Springer, 2018, pp. 12–26.
- [P19] A. Frigerio, B. Vermeulen, K. Goossens. Component-Level ASIL Decomposition for Automotive Architectures. Proceedings of the 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops, DSN-W 2019. Portland, OR, USA: IEEE, 2019, pp. 62–69.
- [P20] M. Gharib, P. Lollini, M. Botta, E. Amparore, S. Donatelli, A. Bondavalli. On the Safety of Automotive Systems Incorporating Machine Learning Based Components: A Position Paper. Proceedings of the 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops, DSN-W 2018. Luxembourg, Luxembourg: IEEE, 2018, pp. 271–274.
- [P21] M. Gharib, P. Lollini, A. Ceccarelli, A. Bondavalli. Dealing with Functional Safety Requirements for Automotive Systems: A Cyber-Physical-Social Approach. In: G. D'Agostino, A. Scala (Eds.), Critical Information Infrastructures Security. CRITIS 2017. Lecture Notes in Computer Science, Vol. 10707. Cham, Switzerland: Springer, 2018, pp. 194–206.
- [P22] M. Gharib, P. Lollini, A. Ceccarelli, A. Bondavalli. Engineering Functional Safety Requirements for Automotive Systems: A Cyber-Physical-Social Approach. Proceedings of the IEEE International Symposium on High Assurance Systems Engineering (HASE). Hangzhou, China: IEEE, 2019, pp. 74–81.
- [P23] Y. Gheraibia, K. Djafri, H. Krimou. Reduction of Solution Space in the Automotive Safety Integrity Levels Allocation Problem. In: S. Chikhi, A. Amine, A. Chaoui, M. Kholadi, D. Saidouni (Eds.), Modelling and Implementation of Complex Systems. Lecture Notes in Networks and Systems, Vol. 1. Cham, Switzerland: Springer, 2016, pp. 67–76.

- [P24] Y. Gheraibia, K. Djafri, H. Krimou. Ant Colony Algorithm for Automotive Safety Integrity Level Allocation. *Applied Intelligence*, 2018, 48: 555–569.
- [P25] G. Griessnig, A. Schnellbach. Development of the 2nd Edition of the ISO 26262. In: J. Stolf, S. Stolf, R. O'Connor, R. Messnarz (Eds.), *Systems, Software and Services Process Improvement. EuroSPI 2017. Communications in Computer and Information Science*, Vol. 748. Cham, Switzerland: Springer, 2017, pp. 535–546.
- [P26] M. Großmann, M. Hirz, J. Fabian. Efficient Application of Multi-Core Processors as Substitute of the E-Gas (Etc) Monitoring Concept. *Proceedings of the 2016 SAI Computing Conference (SAI)*. London, UK: IEEE, 2016, pp. 913–918.
- [P27] C. Huang, L. Li. Architectural Design and Analysis of a Steer-by-Wire System in View of Functional Safety Concept. *Reliability Engineering and System Safety*, 2020, 198:106822.
- [P28] B.P. Jeppesen, M. Rajamani, K.M. Smith. Enhancing Functional Safety in FPGA-Based Motor Drives. *The Journal of Engineering*, 2019, 2019(17): 4580–4584.
- [P29] M. Kaessmeyer, D.S.V. Moncada, M. Schurius. Evaluation of a Systematic Approach in Variant Management for Safety-Critical Systems Development. *Proceedings of the IEEE/IFIP 13th International Conference on Embedded and Ubiquitous Computing, EUC 2015*. Porto, Portugal: IEEE, 2015, pp. 35–43.
- [P30] S. Khastgir, S. Birrell, G. Dhadyalla, H. Sivencrona, P. Jennings. Towards Increased Reliability by Objectification of Hazard Analysis and Risk Assessment (HARA) of Automated Automotive Systems. *Safety Science*, 2017, 99: 166–177.
- [P31] S. Klaasse, G. Kwintenberg, I. Barosan. Development of a Functional Safety Software Layer for the Control of an Electric In-Wheel Motor Based Powertrain. *Proceedings of the 2018 IEEE 15th International Conference on Software Architecture Companion (ICSA-C)*. Seattle, WA, USA: IEEE, 2018, pp. 144–147.
- [P32] S. Kochanthara, N. Rood, L. Cleophas, Y. Dajsuren, M.V. Den Brand. Semi-Automatic Architectural Suggestions for the Functional Safety of Cooperative Driving Systems. *Proceedings of the 2020 IEEE International Conference on Software Architecture Companion (ICSA-C)*. Salvador, Brazil: IEEE, 2020, pp. 55–58.
- [P33] G.C. Kolln, M. Klicker, S. Schmidt. Comparison of Hazard Analysis Methods with Regard to the Series Development of Autonomous Vehicles. *Proceedings of the 2019 IEEE Intelligent Transportation Systems Conference (ITSC)*. Auckland, New Zealand: IEEE, 2019, pp. 2969–2975.
- [P34] B. Kramer, C. Neurohr, M. Büker, E. Böde, M. Fränzle, W. Damm. Identification and Quantification of Hazardous Scenarios for Automated Driving. In: M. Zeller, K. Höfig (Eds.), *Model-Based Safety and Assessment. IMBSA 2020. Lecture Notes in Computer Science*, Vol. 12297. Cham, Switzerland: Springer, 2020, pp. 163–178.
- [P35] K.-L. Leu, H. Huang, Y.-Y. Chen, L.-R. Huang, K.-M. Ji. An Intelligent Brake-by-Wire System Design and Analysis in Accordance with ISO-26262 Functional Safety Standard. *Proceedings of the 2015 International Conference on Connected Vehicles and Expo (ICCVE)*. Shenzhen, China: IEEE, 2015, pp. 150–156.
- [P36] H.-P. Li, Y.-w. Li. The Research of Electric Vehicle's MCU System Based on ISO26262. *Proceedings of the 2017 2nd Asia-Pacific Conference on Intelligent Robot Systems (ACIRS)*. Wuhan, China: IEEE, 2017, pp. 336–340.
- [P37] C. Lidström, C. Bondesson, M. Nyberg, J. Westman. Improved Pattern for ISO 26262 ASIL Decomposition with Dependent Requirements. *Proceedings of the 2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C)*. Sofia, Bulgaria: IEEE, 2019, pp. 28–35.
- [P38] B. Liu, Y. Li. Research on Vehicle Control Unit Based on Functional Safety. *Proceedings of the 2017 2nd Asia-Pacific Conference on Intelligent Robot Systems (ACIRS)*. Wuhan, China: IEEE, 2017, pp. 160–164.
- [P39] R. Mader, H. Martin, R. Obendrauf, P. Prinz, B. Winkler, G. Griesnig. A Framework for Model-Based Safety Requirements Round-Trip Engineering. *Proceedings of the 10th IET System Safety and Cyber-Security Conference 2015*. Bristol, UK: IEEE, 2015, pp. 1–6.
- [P40] A. Mallya, V. Pantelic, M. Adedjouma, M. Lawford, A. Wassing. Using STPA in an ISO 26262 Compliant Process. In: A. Skavhaug, J. Guiochet, F. Bitsch (Eds.), *Computer Safety, Reliability, and Security. SAFECOMP 2016. Lecture Notes in Computer Science*, Vol. 9922. Cham, Switzerland: Springer, 2016, pp. 117–129.
- [P41] D. Marcos, J. Perez, P. Zubizarreta, M. Garmendia, I.P. de Arenaza, J. Crego, et al. A Safety Concept for an Automotive Lithium-Based Battery Management System. *Proceedings of the 2019 Electric Vehicles International Conference (EV)*. Bucharest, Romania: IEEE, 2019, pp. 1–6.
- [P42] H. Martin, B. Winkler, S. Grubmüller, D. Watzenig. Identification of Performance Limitations of Sensing Technologies for Automated Driving.

- Proceedings of the 2019 IEEE International Conference on Connected Vehicles and Expo (ICCVE). Graz, Austria: IEEE, 2019, pp. 1–6.
- [P43] L.E.G. Martins, T. Gorschek. Requirements Engineering for Safety-Critical Systems: An Interview Study with Industry Practitioners. *IEEE Transactions on Software Engineering*, 2020, 46(4): 346–361.
- [P44] P. Mauborgne, S. Deniaud, É. Levrat, É. Bonjour, J.-P. Micaelli, D. Loise. The Determination of Functional Safety Concept Coupled with the Definition of Logical Architecture: A Framework of Analysis from the Automotive Industry. *IFAC-PapersOnLine*, 2017, 50(1): 7278–7283.
- [P45] R. Messnarz, H. Sporer. Functional Safety Case with FTA and FMEDA Consistency Approach. In: X. Larrucea, I. Santamaria, R. O'Connor, R. Messnarz (Eds.), *Systems, Software and Services Process Improvement. EuroSPI 2018. Communications in Computer and Information Science*, Vol. 896. Cham, Switzerland: Springer, 2018, pp. 387–397.
- [P46] H.E. Monkhouse, I. Habli, J. McDermid. An Enhanced Vehicle Control Model for Assessing Highly Automated Driving Safety. *Reliability Engineering and System Safety*, 2020, 202: 107061.
- [P47] H. Monkhouse, I. Habli, J. McDermid, S. Khastgir, G. Dhadyalla. Why Functional Safety Experts Worry About Automotive Systems Having Increasing Autonomy. *Proceedings of the 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*. San Francisco, CA, USA: IEEE, 2017, pp. 1–6.
- [P48] P. Munk, A. Abele, E. Thaden, A. Nordmann, R. Amarnath, M. Schweizer, et al. INVITED: Semi-Automatic Safety Analysis and Optimization. *Proceedings of the 2018 55th ACM/ESDA/IEEE Design Automation Conference (DAC)*. San Francisco, CA, USA: IEEE, 2018, pp. 1–6.
- [P49] P. Nag, U. Ghanekar, J. Harmalkar. A Novel Multi-Core Approach for Functional Safety Compliance of Automotive Electronic Control Unit According to ISO 26262. *Proceedings of the 2019 IEEE 5th International Conference for Convergence in Technology (I2CT)*. Bombay, India: IEEE, 2019, pp. 1–5.
- [P50] A. Nardi, A. Armato. Functional Safety Methodologies for Automotive Applications. *Proceedings of the 2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. Irvine, CA, USA: IEEE, 2017, pp. 970–975.
- [P51] M. Park, H.C. Koag, H.-S. Ahn. Functional Safety Improvement of Electric Power Steering System by Using Electronic Stability Control System. *Proceedings of the IEEE 27th International Symposium on Industrial Electronics (ISIE)*. Cairns, QLD, Australia: IEEE, 2018, pp. 230–234.
- [P52] Q. Rao, J. Frtunikj. Deep Learning for Self-Driving Cars: Chances and Challenges. *Proceedings of the 1st International Workshop on Software Engineering for AI in Autonomous Systems. SEFAIS 2018*. New York, NY, USA: ACM, 2018, pp. 35–38.
- [P53] L. Rogovchenko-Buffoni, A. Tundis, M.Z. Hossain, M. Nyberg, P. Fritzson. An Integrated Toolchain for Model Based Functional Safety Analysis. *Journal of Computational Science*, 2014, 5(3): 408–414.
- [P54] A. Ruiz, A. Melzi, T. Kelly. Systematic Application of ISO 26262 on a SEooC: Support by Applying a Systematic Reuse Approach. *Proceedings of the Design, Automation and Test in Europe Conference (DATE)*. Grenoble, France: IEEE, 2015, pp. 393–396.
- [P55] R.R. Sabbella, M. Arunachalam. Functional Safety Development of Motor Control Unit for Electric Vehicles. *Proceedings of the 2019 IEEE Transportation Electrification Conference (ITEC-India)*. Bengaluru, India: IEEE, 2019, pp. 1–6.
- [P56] A. Salikiryaki, I. Petrova, S. Baumgart. Graphical Approach for Modeling of Safety and Variability in Product Lines. *Proceedings of the 41st Euromicro Conference on Software Engineering and Advanced Applications, SEAA 2015*. Madeira, Portugal: IEEE, 2015, pp. 410–417.
- [P57] G. Scharfenberg, L. Elis, G. Hofmann. New Design Methodology – Using VHDL-AMS Models to Consider Aging Effects in Automotive Mechatronic Circuits for Safety Relevant Functions. *Proceedings of the 2019 International Conference on Applied Electronics (AE)*. Pilsen, Czech Republic: IEEE, 2019, pp. 1–5.
- [P58] T. Schmid, S. Schraufstetter, S. Wagner. An Approach for Structuring a Highly Automated Driving Multiple Channel Vehicle System for Safety Analysis. *Proceedings of the 2018 3rd International Conference on System Reliability and Safety (ICSRS)*. Barcelona, Spain: IEEE, 2018, pp. 362–367.
- [P59] V. Schönemann, H. Winner, T. Glock, S. Otten, E. Sax, B. Boeddeker, et al. Scenario-Based Functional Safety for Automated Driving on the Example of Valet Parking. In: K. Arai, S. Kapoor, R. Bhatia (Eds.), *Advances in Information and Communication Networks. FICC 2018. Advances in Intelligent Systems and Computing*, Vol. 886. Cham, Switzerland: Springer, 2019, pp. 53–64.
- [P60] M.N. Shankar Kumar, K. Balakrishnan. Functional Safety Development of Battery Management System for Electric Vehicles. *Proceedings of*

- the 2019 IEEE Transportation Electrification Conference (ITEC-India). Bengaluru, India: IEEE, 2019, pp. 1–6.
- [P61] J. Sini, M. D'Auria, M. Violante. Towards Vehicle-Level Simulator Aided Failure Mode, Effect, and Diagnostic Analysis of Automotive Power Electronics Items. Proceedings of the 2020 IEEE Latin-American Test Symposium (LATS). Maceio, Brazil: IEEE, 2020, pp. 1–6.
- [P62] J. Sini, M. Violante. A Simulation-Based Methodology for Aiding Advanced Driver Assistance Systems Hazard Analysis and Risk Assessment. *Microelectronics Reliability*, 2020, 109: 113661.
- [P63] J. Sini, M. Violante, R. Dessi. ISO26262-Compliant Development of a High Dependable Automotive Powertrain Item. In: W. Zamboni, G. Petrone (Eds.), *ELECTRIMACS 2019. Lecture Notes in Electrical Engineering*, Vol. 615. Cham, Switzerland: Springer, 2020, pp. 315–326.
- [P64] M. Skoglund, H. Svensson, H. Eriksson, T. Arts, R. Johansson, A. Gerdes. Checking Verification Compliance of Technical Safety Requirements on the AUTOSAR Platform Using Annotated Semi-Formal Executable Models. In: A. Bondavalli, A. Ceccarelli, F. Ortmeier (Eds.), *Computer Safety, Reliability, and Security. SAFECOMP 2014. Lecture Notes in Computer Science*, Vol. 8696. Cham, Switzerland: Springer, 2014, pp. 19–26.
- [P65] T. Stolte, G. Bagschik, M. Maurer. Safety Goals and Functional Safety Requirements for Actuation Systems of Automated Vehicles. Proceedings of the IEEE 19th International Conference on Intelligent Transportation Systems (ITSC). Rio de Janeiro, Brazil: IEEE, 2016, pp. 2191–2198.
- [P66] T. Stolte, G. Bagschik, A. Reschka, M. Maurer. Hazard Analysis and Risk Assessment for an Automated Unmanned Protective Vehicle. Proceedings of the IEEE Intelligent Vehicles Symposium (IV). Los Angeles, CA, USA: IEEE, 2017, pp. 1848–1855.
- [P67] R. Tan. A Safety Concept for Camera Based ADAS Based on Multicore MCU. Proceedings of the 2014 IEEE International Conference on Vehicular Electronics and Safety (ICVES). Hyderabad, India: IEEE, 2014, pp. 1–6.
- [P68] C. Tao. Functional Safety Concept Design of Hybrid Electric Vehicle Following ISO 26262. Proceedings of the IEEE Conference and Expo Transportation Electrification Asia-Pacific (ITEC Asia-Pacific). Beijing, China: IEEE, 2014, pp. 1–6.
- [P69] S.S. Tikar. Compliance of ISO 26262 Safety Standard for Lithium Ion Battery and Its Battery Management System in Hybrid Electric Vehicle. Proceedings of the 2017 IEEE Transportation Electrification Conference (ITEC-India). Pune, India: IEEE, 2017, pp. 1–5.
- [P70] M. Tlig, M. Machin, R. Kerneis, E. Arbaretier, L. Zhao, F. Meurville, et al. Autonomous Driving System: Model Based Safety Analysis. Proceedings of the 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W). Luxembourg, Luxembourg: IEEE, 2018, pp. 2–5.
- [P71] R.F.B. Trindade, L. Bulwahn, C. Ainhauser. Automatically Generated Safety Mechanisms from Semi-Formal Software Safety Requirements. In: A. Bondavalli, F. Di Giandomenico (Eds.), *Computer Safety, Reliability, and Security. SAFECOMP 2014. Lecture Notes in Computer Science*, Vol. 8666. Cham, Switzerland: Springer, 2014, pp. 278–293.
- [P72] E. van Nunen, F. Esposto, A.K. Saberi, J.-P. Paardekooper. Evaluation of Safety Indicators for Truck Platooning. Proceedings of the IEEE Intelligent Vehicles Symposium (IV). Los Angeles, CA, USA: IEEE, 2017, pp. 1013–1018.
- [P73] Y. Wang, D. Graziotin, S. Kriso, S. Wagner. Communication Channels in Safety Analysis: An Industrial Exploratory Case Study. *Journal of Systems and Software*, 2019, 153: 135–151.
- [P74] W. Yang, L. Yanwen, L. Chunshu, W. Xiyang. Analysis and Application of Functional Safety Based on Modified FMEA Method. Proceedings of the 2017 2nd Asia-Pacific Conference on Intelligent Robot Systems (ACIRS). Wuhan, China: IEEE, 2017, pp. 98–103.
- [P75] Y. Wang, S. Wagner. On Groupthink in Safety Analysis: An Industrial Case Study. Proceedings of the 40th International Conference on Software Engineering in Practice. ICSE-SEIP '18. New York, NY, USA: ACM, 2018, pp. 266–275.
- [P76] Y.-C. Wang, C.-S. Lee, P.-C. Kuo, Y.-L. Lin. Overcurrent Protection Design, Failure Mode and Effect Analysis of an Electric Vehicle Inverter. Proceedings of the IEEE International Conference on Industrial Technology (ICIT). Taipei, Taiwan: IEEE, 2016, pp. 1287–1292.
- [P77] F. Warg, M. Gassilewski, J. Tryggvesson, V. Izosimov, A. Werneman, R. Johansson. Defining Autonomous Functions Using Iterative Hazard Analysis and Requirements Refinement. In: A. Skavhaug, J. Guiochet, E. Schoitsch, F. Bitsch (Eds.), *Computer Safety, Reliability, and Security. SAFECOMP 2016. Lecture Notes in Computer Science*, Vol. 9923. Cham, Switzerland: Springer, 2016, pp. 286–297.
- [P78] F. Warg, M. Skoglund, A. Thorsen, R. Johansson, M. Brannstrom, M. Gyllenhammar, et al. The Quantitative Risk Norm - A Proposed Tailoring of HARA for ADS. Proceedings of the 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W). Valencia, Spain: IEEE, 2020, pp. 86–93.

- [P79] R. Weissnegger, M. Schuß, C. Kreiner, M. Pistauer, K. Römer, C. Steger. Seamless Integrated Simulation in Design and Verification Flow for Safety-Critical Systems. In: A. Skavhaug, J. Guiochet, E. Schoitsch, F. Bitsch (Eds.), *Computer Safety, Reliability, and Security. SAFECOMP 2016. Lecture Notes in Computer Science*, Vol. 9923. Cham, Switzerland: Springer, 2016, pp. 359–370.
- [P80] J. Westman, M. Nyberg. Providing Tool Support for Specifying Safety-Critical Systems by Enforcing Syntactic Contract Conditions. *Requirements Engineering*, 2019, 24: 231–256.
- [P81] F. Wotawa, B. Peischl, F. Klück, M. Nica. *Quality Assurance Methodologies for Automated Driving. Elektrotechnik und Informationstechnik*, 2018, 135: 322–327.
- [P82] Z. Wu, X. Su, Y. Zhu, Luke. Functional Safety System Design on EPS. In: *Proceedings of SAE-China Congress 2016: Selected Papers. SAE-China 2016. Lecture Notes in Electrical Engineering*, Vol. 418. Singapore: Springer, 2017, pp. 647–664.
- [P83] A. Young, A. Walker. Qualifying Dependent Failure Analysis Within ISO26262: Applicability to Semiconductors. In: X. Larrucea, I. Santamaria, R. O'Connor, R. Messnarz (Eds.), *Systems, Software and Services Process Improvement. EuroSPI 2018. Communications in Computer and Information Science*, Vol. 896. Cham, Switzerland: Springer, 2018, pp. 331–340.
- [P84] J. Zhang, G. Rizzoni, A. Cordoba-Arenas, A. Amodio, B. Aksun-Guvenc. Model-Based Diagnosis and Fault Tolerant Control for Ensuring Torque Functional Safety of Pedal-by-Wire Systems. *Control Engineering Practice*, 2017, 61: 255–269.
- [P85] Z. Yaling, G. Jing, S. Hanwen. The Functional Safety Analysis and Design of Dual-Motor Hybrid Bus Clutch System. *Proceedings of the 2018 IEEE International Conference of Safety Produce Informatization (IICSPI)*. Chongqing, China: IEEE, 2018, pp. 299–304.
- [P86] A.K. Saberi, E. Barbier, F. Benders, M. van den Brand. On Functional Safety Methods: A System of Systems Approach. *Proceedings of the Annual IEEE International Systems Conference (SysCon)*. Vancouver, BC, Canada: IEEE, 2018, pp. 1–6.
- [P87] A. Abdulkhaleq, S. Wagner. A Software Safety Verification Method Based on System-Theoretic Process Analysis. In: A. Bondavalli, A. Ceccarelli, F. Ortmeier (Eds.), *Computer Safety, Reliability, and Security. SAFECOMP 2014. Lecture Notes in Computer Science*, Vol. 8696. Cham, Switzerland: Springer, 2014, pp. 401–412.
- [P88] A. Abdulkhaleq, S. Wagner, N. Leveson. A Comprehensive Safety Engineering Approach for Software-Intensive Systems Based on STPA. *Procedia Engineering*, 2015, 128: 2–11.
- [P89] A. Abdulkhaleq, S. Wagner. A Controlled Experiment for the Empirical Evaluation of Safety Analysis Techniques for Safety-Critical Software. *Proceedings of the 19th International Conference on Evaluation and Assessment in Software Engineering. EASE '15*. New York, NY, USA: ACM, 2015, pp. 1–10.
- [P90] A. Abdulkhaleq, D. Lammering, S. Wagner, J. Röder, N. Balbierer, L. Ramsauer, et al. A Systematic Approach Based on STPA for Developing a Dependable Architecture for Fully Automated Driving Vehicles. *Procedia Engineering*, 2017, 179: 41–51.
- [P91] A. Abdulkhaleq, M. Baumeister, H. Böhmert, S. Wagner. Missing No Interaction—Using STPA for Identifying Hazardous Interactions of Automated Driving Systems. *International Journal of Safety Science*, 2018, 2(1): 115–124.
- [P92] M. Ghadhab, S. Junges, J.-P. Katoen, M. Kuntz, M. Volk. Model-Based Safety Analysis for Vehicle Guidance Systems. In: S. Tonetta, E. Schoitsch, F. Bitsch (Eds.), *Proceedings of the 36th International Conference on Computer Safety, Reliability, and Security. SAFECOMP 2017. Lecture Notes in Computer Science*, Vol. 10488. Cham, Switzerland: Springer, 2017, pp. 3–19.
- [P93] Y. Gheraibia, A. Moussaoui, L.S. Azevedo, D. Parker, Y. Papadopoulos, M. Walker. Can Aquatic Flightless Birds Allocate Automotive Safety Requirements? *Proceedings of the 2015 IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS)*. Cairo, Egypt: IEEE, 2015, pp. 1–6.
- [P94] J. Oscarsson, M. Stolz-Sundnes, N. Mohan, V. Izosimov. Applying Systems-Theoretic Process Analysis in the Context of Cooperative Driving. *Proceedings of the 2016 11th IEEE Symposium on Industrial Embedded Systems (SIES)*. Krakow, Poland: IEEE, 2016, pp. 1–5.
- [P95] J. Sini, M. Violante. An Automatic Approach to Perform FMEDA Safety Assessment on Hardware Designs. *Proceedings of the 2018 IEEE 24th International Symposium on On-Line Testing and Robust System Design (IOLTS)*. Platja d'Aro, Spain: IEEE, 2018, pp. 49–52.
- [P96] M. Adedjouma, G. Pedroza, B. Bannour. Representative Safety Assessment of Autonomous Vehicle for Public Transportation. *Proceedings of the 2018 IEEE 21st International Symposium on Real-Time Distributed Computing (ISORC)*. Singapore: IEEE, 2018, pp. 124–129.
- [P97] S. Baumgart, J. Fröberg, S. Punnekkat. A Process to Support Safety Analysis for a System-of-Systems. *Proceedings of the 2020 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*. Coimbra, Portugal: IEEE, 2020, pp. 61–66.

- [P98] J. Chen, S. Wang, T. Zhou, L. Xiong, X. Xing. Study on Safety Analysis Method for Take-Over System of Autonomous Vehicles. Proceedings of the IEEE Intelligent Vehicles Symposium (IV). Las Vegas, NV, USA: IEEE, 2020, pp. 1972–1977.
- [P99] A. Di Sandro, S. Kokaly, R. Salay, M. Chechik. Querying Automotive System Models and Safety Artifacts: Tool Support and Case Study. Journal of Automotive Software Engineering, 2020, 1(1): 34–50.
- [P100] N. Grabbe, A. Kellnberger, B. Aydin, K. Bengler. Safety of Automated Driving: The Need for a Systems Approach and Application of the Functional Resonance Analysis Method. Safety Science, 2020, 126: 104665.
- [P101] G. Koelln, M. Klicker, S. Schmidt. Comparison of the Results of the System Theoretic Process Analysis for a Vehicle SAE Level Four and Five. Proceedings of the 2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC). Rhodes, Greece: IEEE, 2020, pp. 1–6.
- [P102] I. Sorokos, L.P. Azevedo, Y. Papadopoulos, M. Walker, D.J. Parker. Comparing Automatic Allocation of Safety Integrity Levels in the Aerospace and Automotive Domains. IFAC-PapersOnLine, 2016, 49(3): 184–190.