Systematic Design of Automated Driving Functions Considering Functional Safety Aspects

Robert Graubohm, Torben Stolte, Gerrit Bagschik, Andreas Reschka, and Markus Maurer
Institute of Control Engineering
Technische Universität Braunschweig
38106 Braunschweig, Germany
Email: {graubohm,stolte,bagschik,reschka,maurer}@ifr.ing.tu-bs.de

Abstract—**Structuring the early design phase of automotive systems is an important part of efficient and successful development processes. Reference models have to define stages to organize the collaboration of different engineering domains, whereas individual tasks often strongly influence each other. Early functional safety considerations, as required by ISO 26262, have significant impact on the structure of the development process. This contribution presents a procedure model which is based on a tried and proven design model for driver assistance systems. Multiple adaptions of the prior model are established, especially to reflect the functional safety life cycle. An additional layer is displayed adjoining the reference process to include supporting methods of modeling and model analysis. The proposed reference process strongly aligns with the flexible procedure model of VDI 2206, allowing for easier implementation in current automotive development processes.**

I. Introduction

Even in theory, development processes cannot be grasped as a strict sequence of individual process steps, since the different tasks influence each other recursively. The interaction between the steps of development can more easily be displayed in form of cycles. A reference process for the early design phase of driver assistance systems was developed during the research project “Automatic Emergency Braking” at Audi. It displays the iterative design loops required for such systems and was first introduced in 2002 [1].

Reference processes are important to manage the growing complexity of development activities for automated driving functions and driverless cars. In contrast to driver assistance systems, the systematic design of driverless systems has to consider additional requirements. This is especially true for safety aspects, as human drivers or supervisors might not be a fallback solution in all cases. Today, functional safety considerations can have significant impact on the outcome of design processes for automotive systems. Thus, functional specifications defined in the initial concept phase should already respect key requirements of the safety life cycle as defined by standard ISO 26262 [2]. The proof of functional safety has to be a major concern during preliminary development.

The ISO standard defines new requirements for the life cycle of safety-related systems in passenger cars that likely differ from the earlier used in-house standards and the generic product standard IEC 61508 [3]. Hence, reference processes for product development in the automotive industry have to be revised to reflect the adoption of the standard. In practice, the implementation of safety requirements in early development activities usually still lacks structured approaches. This is especially critical for the task of defining safety goals and deriving the functional safety concept within the concept phase, potentially supported by safety analysis steps, not further specified by the standard.

Leveson [4] argues that safety aspects have to be considered from the early concept formation stages of development in order to achieve cost-effective safety engineering. Thereby, all design decisions are guided by safety considerations. Sexton et al. state in [5] that concepts with poorly conceived safety requirements are likely to result in subsequent re-work and weak coordination with suppliers. Eventually, the developed product can actually be unsafe if missing safety aspects are not identified at later stages of the development process.

In order to reflect the current challenges of systematic design processes for automotive systems and the functional safety standard ISO 26262, the reference process described initially [1] is adapted and presented in a new version. A major modification is the introduction of tasks for defining safety concepts in the early stages of development, following the hazard analysis and risk assessment (HARA) described in ISO 26262. Thus, the new reference process incorporates feasibility and ease of validation of the functional safety concept, while inheriting the orientation towards customer benefit from the original design model.

II. Related Work

The application of the original systematic design model is described in detail by Rieken et al. in [6]. To elucidate the development of concepts and prototypes following the approach, the authors use the research project “Automatic Emergency Braking” as a concrete example. The underlying concept is a development in iterative loops, in which each iteration improves the functional definition of the system under development. Therefore, the main purpose of the loops is resolving basic design conflicts identified based on expert knowledge, but also adjusting non-realizable functional requirements. A distinctive feature of the model is the inner loop, describing an optional return to the initial stages based on an early evaluation of the functional definition and identified conflicts. This inner loop often does not require any realization in prototypes, but can be performed theoretically or supported by X-in-the-loop tools. Customer benefit is defined as the motivation for any later steps within the design process of assistance systems. Thus, functional definitions have to be based on objective or subjective driver needs.

An established example for a design reference process based on cycles is the "design methodology for mechatronic systems" defined by VDI 2206 [7]. The standard uses the V-model as cycle that requires multiple iterations until the development is completed. Gausemeier and Moehringer [8] introduced the procedure model of VDI 2206 in 2003, focusing on its flexibility and the integration of multiple engineering domains. The authors also introduce strategies to adapt the guideline for systematic design to individual development tasks in specific industries. Eigner et al. [9] propose a requirement, function, logical solution element, and physical element (RFLP) diagram as an extension of the V-model of VDI 2206 to include aspects of model-based product design.

Follmer et al. [10] derive an approach for the creation of mechatronic systems models based on the iterative character of VDI 2206, specifically displaying the challenges of the conceptual design phase. The extensive looping back to the initial task indicated by the process model largely corresponds with the reference process proposed in this paper. The authors additionally indicate, how the macro-cycle of VDI 2206 can be adapted to integrate different design stages.

Anzengruber et al. [11] propose a process model related to the approach of Follmer et al. that further considers the challenges of missing or incomplete information. Assumptions are discussed as a common aspect of early design processes that requires disclosure and documentation. To emphasize the possible iterations after reassessment of assumptions made, the process model displays a circular shape.

The functional safety aspects to be considered during system design are based on the functional safety standard ISO 26262 that addresses possible hazards caused by malfunctioning behavior of safety-related E/E systems [2]. The safety process described by the standard starts with determining necessary safety goals. This HARA task is split in different stages that allow for qualitative evaluation of the safety relevance and necessary risk reduction of different features. Stolte et al. [12] introduce an approach to structure the HARA task based on project experience in developing an automated unmanned protective vehicle. Since the vehicle will be operated without human supervision, early functional safety considerations are essential in their project context. Their work includes the results of applying the structured HARA process on the system under consideration.

Leveson [4] proposes a safety-guided design process in which hazard analyses widely support design decisions. The hazard analysis technique used is called STPA (System-Theoretic Process Analysis), and is based on the STAMP model of causation (System-Theoretic Accident Model and Processes). The approach does not require a completed system design, but process models based on the functional design. The author argues that a major mistake of system design processes is leaving the human operator out of the conceptual design stages. Accordingly, the proposed process model increases the design effort put into considerations of human error and preventing it.

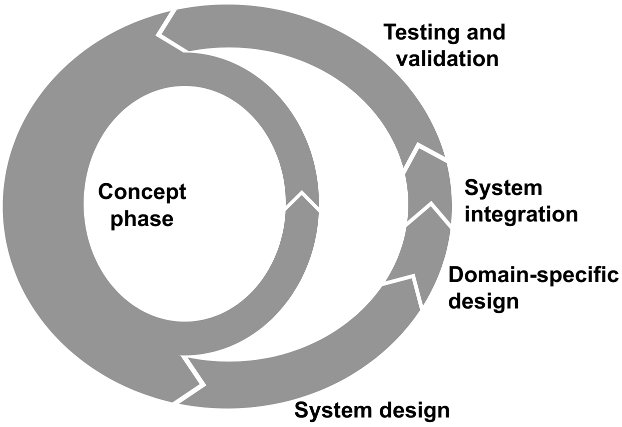

Fig. 1. Structure of the Design Model

Sexton et al. [5] describe a preliminary phase of safety engineering used in practice. The phases and iterative character of the informal process have similarities with the reference process described in this paper. It consists of cycles for early hazard analysis, early safety analysis, and early design decisions that provide input for the later formal development process. Thus, waiting time for conclusions during the main development can be avoided. Additionally, early activities of the development process can focus on safety goals that potentially will receive the highest ASIL rating or have significant impact on the system architecture.

III. Reference Model

A. Overview

Although current development processes in the automotive industry might largely correspond to an adaption of the V-model, early iterations in the concept and system design phase required in practice are not distinctively included in such visualization. Additionally, individual steps defined by models and standards are often outlined in impractical linear sequences within the top-down approach. Even if the sequence is supposed to be cycled through iteratively (cf. V-model as macro-cycle defined by VDI 2206 [7]), it does not match with the extensive looping back to the initial stage from various individual tasks of the development process.

Adaptions of the V-model for the automotive domain are usually focused on software-based systems and do not visualize iterations [13], [14]. In this context, a complete set of system requirements and the generation of test cases for later integration and validation is anticipated. Hence, these development models cannot be directly applied to describe the multi-disciplinary design of the whole system, which requires a higher level of flexibility especially while finding concepts.

The VDI 2206 suggests an adaption of its generic macrocycle to reflect the individual tasks needed for specific projects and integrates elements for these adaptations [8]. The reference process proposed in this paper and depicted in Fig. 1 can be seen as such an adaption. The breakdown into the main phases of system design, domain-specific design, and system integration has been adopted, while the V-shape was omitted to visualize the structure of the approach, comprising an inner and an outer cycle. The iterative character of the reference model still corresponds with the idea of VDI 2206 that multiple iterations mark different degrees of maturity of the product. Thus, a first complete iteration does not have to produce a finished product, but can come up with a detailed specification of functionality or elements that contribute a partial solution to the problem [8]. Such results can also be described as concept studies or early prototypes.

However, the guideline does not cover the earlier concept phase extensively outlined in the process model described in this paper. This stage is of large importance for the development of systems for automatic driving, especially in view of the functional safety standard, since it defines functional requirements for the subsequent highly complex cross-domain system design. Thereby, most tasks listed in the reference process are part of the left wing of the V-model, while the stages of integration and tests are not broken down further.

As already described, resolving design conflicts is the main purpose of multiple iterations within the design model. Iterations during system design can additionally be caused by new technological information being obtainable. Automotive development especially for automated driving heavily relies on assumptions about innovative technology, probably available on the market when the feature is introduced in series production. Thus, technical specifications of sensors and other parts might not be accessible during early development procedures. With new information, the applicability of assumptions made and technical feasibility have to be reassessed. Adaptions of the product require running through the development process again, which is best visualized in cycles.

In prior versions of the reference model, the definition of the safety concept used to be a late task of the outer cycle. In compliance with the standard ISO 26262, this stage has to be separated in two individual parts, the functional safety concept and the technical safety concept. The functional safety concept consists of functional safety requirements that describe a functionality in order to achieve safety goals. Whereas the technical safety concept outlines the implementation of functions in hardware and software. Additional changes are discussed later (cf. III-E). The specification of a functional safety concept in early development stages is one of the most important additions of ISO 26262 with respect to other approaches. The establishment of a safety life cycle can reflect the domain-specific high degree of innovation in development projects for which there is a lack of standardized solutions.

Both safety concepts are based on the previously performed HARA, in which hazards are identified and safety goals are formulated for each hazardous scenario. Additionally, an Automotive Safety Integrity Level (ASIL) is assigned with each safety goal. The structure for including these stages in the reference model is derived from [12].

Due to their influence on design decisions, functional safety requirements have to be obtainable early in the development process. If functional safety requirements are defined too late, the system design has to be revised. Especially the system architecture and technical requirements for hardware and software implementation can be affected. However, those requirements are also supposed to effectively define a complete safety concept derived from previously defined safety goals. Therefore, defining safety goals has to be an initial task of the concept phase. The individual tasks within the proposed reference model are depicted in Fig. 2.

B. *Concept Phase*

The preliminary requirement description is the starting point of development process. It is an abstract idea of functional requirements reflecting customer needs or requirements derived from use-cases. Thus, the whole design process is driven by an identified customer benefit, transferred into recorded ideas and use cases. The overall goal of the concept phase is a specification of the functional concept of the system, based on these requirements. In order to achieve this goal, while minding multiple aspects, especially those related to functional safety, the concept phase strongly requires cross-domain collaboration.

In accordance with the functional safety standard ISO 26262, a following early task of the development process is the item definition, serving as input for the whole subsequent functional safety consideration. Moreover, the item definition is an essential aspect of the concept phase, since it specifies a functional description that defines the goal of the development process. Especially when considering automated driving, the item definition has to cover the complete functionality of the vehicle to allow considering its functional safety. In complex systems, this allows for later consideration of interactions among components for safety validation. Leveson [4] argues that hazardous system states can otherwise occur whilst all items satisfy their individual requirements.

The ideas and use cases are utilized as an overview of functions for the formal item definition. Additional information like preliminary assumptions of the system architecture or potential misuses will also be used at this point, particularly requiring expert knowledge and experience. In this context, the main inner iteration of the reference process is labeled “item refinement”, expressing an adaption of the item description in reaction to conflicts emerged at any state of the concept phase or system design. Hence, the refinement can have a direct impact on the proposed functionality.

The following HARA is based on the item definition. The iterative character of the tasks, described by Stolte et al. [12], can best be displayed as a loop inside the proposed process. An initial rating of possible malfunctions of the defined items will be performed, followed by a description of hazards caused by

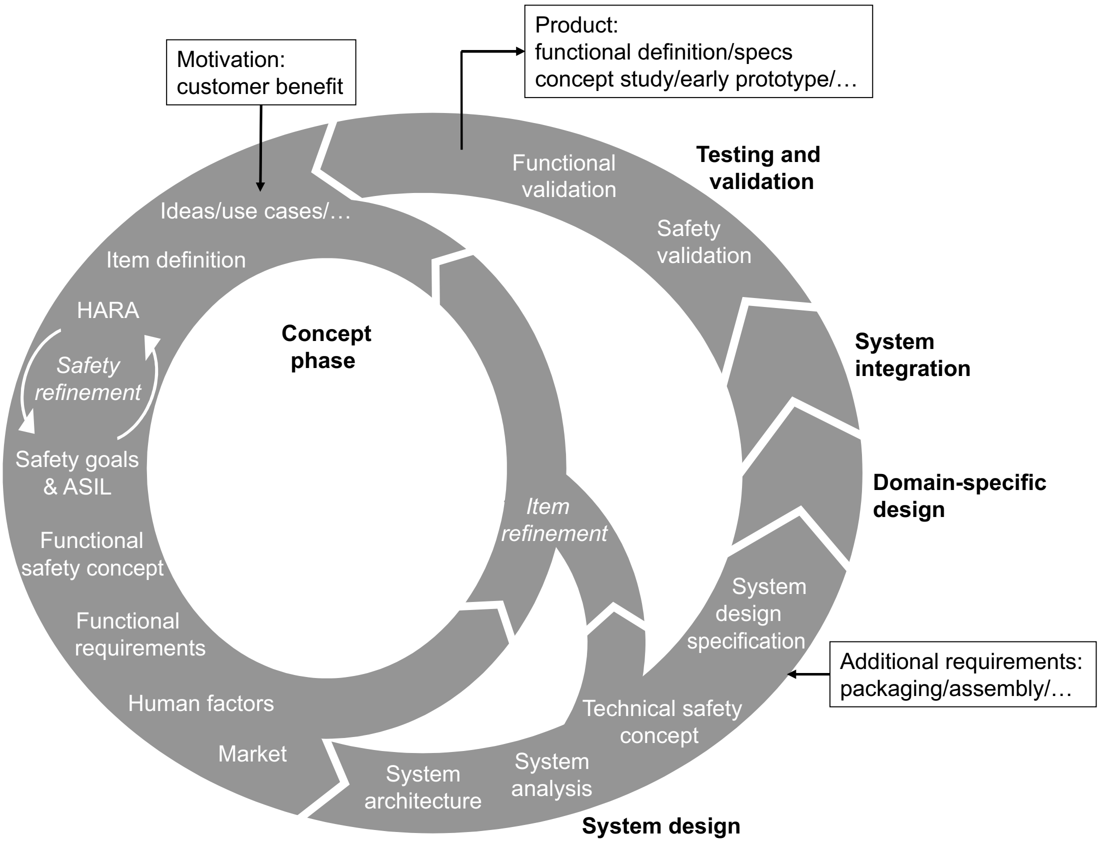

Fig. 2. Systematic Design Model for Automated Driving Functions

this malfunctioning behavior. Hazardous scenarios will then be derived, based on a consideration of possible driving situations and environment aspects.

The next task shown in the cycle is the specification of safety goals and ASILs. The ASIL rating is defined in ISO 26262, assessing severity, exposure, and controllability for each failure mode. Safety goals of an item are not supposed to define technological solutions, but functional objectives. After safety goals are identified based on all hazardous scenarios, countermeasures in form of functional safety requirements can be specified. The requirements are derived from the safety goals, since they define a concept of function that satisfies the goals. The functional safety concept, outlined as the next stage within the proposed development cycle, is composed of all safety requirements specified, based on the findings of the HARA.

At this point, two different types of refinement in form of iterations are possible. Based on safety considerations, an item refinement is likely needed to narrow the functional range, in order to effect feasible safety requirements. Alternatively, the safety refinement describes alterations of the described malfunctions and hazards, specifically affecting the set of hazardous scenarios. Thus, the functional range is not affected by the safety refinement; it aims at achieving completeness of the HARA and the functional safety concept [12].

As described, the HARA stage ends with the definition of safety goals from which the functional safety concept is inferred. Since the following tasks rely on the specification of functional requirements, the safety concept has to allow implementation, while safety goals addressing hazardous scenarios can be abstract. Hence, ISO 26262 handles functional safety requirements as links between the concept phase and the product development. However, the allocation of safety requirements to architectural elements, as defined by the standard, requires the assumption of a preliminary functional system architecture within the concept phase that later has to be reassessed.

It can be stated that requirements about the functional safety of an item are a key part of the concept phase. The steps within the HARA should also be well documented since ISO 26262 requires detailed traceability between all main steps of the safety development (e.g. hazards, safety goals, requirements and design decisions). Traceability is also important for a later validation of the defined safety goals. The documentation is of additional importance to the iterative design process, since it can assure reusability of parts of the decisions made in previous HARA phases after altering the item definition.

As ISO 26262 only addresses hazards caused by malfunctions, the complete set of functional requirements might actually consist of additional safety requirements that are not part of the functional safety concept. Nevertheless, safety requirements related to the implementation will most likely be specified with the technical requirements later on.

The next proposed step within in the concept phase is the revised description of functionality specified in functional requirements. For this, safety requirements are combined with other requirements derived from the current item definition. Based on these requirements, additional human factors can be incorporated, evaluating whether the currently considered functionalities and limitations can be designed user-transparent. This can include a reassessment of the assumptions about controllability from the HARA phase. A final task within the specification of a functional concept is the consideration of marketing aspects, focusing on the characterization of market chances and a potential target price. Any of these latter steps of the concept phase can lead to an item refinement, if any kind of conflict occurs.

C. System Design

If a functional concept is found at the end of the concept phase that does not require any other refinement, the system design can be conducted to create a technical solution concept. The first step outlined is a specification of the functional system architecture. For this, all specified functional requirements have to be considered, as well as the preliminary assumptions of the architecture within the concept phase, especially the HARA stage.

Based on the architectural outline, a system analysis can be performed to produce a technical safety concept based on the safety goals defined earlier. This phase mainly addresses system failures caused by hardware and software faults, usually supported by analysis techniques like fault tree analysis (FTA) and failure modes and effects analysis (FMEA). Potential conflicts within the system analysis require the option of an adaption of system architecture assumptions. Larger problems in matters of technical feasibility will additionally require an item refinement, triggering a new iteration to modify the functional concept. An early consideration of technical safety requirements in development processes is important to reflect the significant impact on the outcome of the system design.

After a technical safety concept is found, the system design can be specified, incorporating safety requirements and architectural decisions, as well as additional system requirements like packaging. These requirements for software and hardware design form a solution concept, which is realized within the following domain-specific design phase. Design, implementation and integration of hardware and software can be seen as individual development processes, not detailed at this point.

Subsequently, the results of domain-specific design processes are integrated to an overall system. The integration process is checked on the basis of the specified functional concept and the technical requirements. Further verification is carried out within the next phase of testing and validation, which is the final phase of the development cycle. The task of safety validation includes verification of functional and technical safety requirements, but also describes the validation of an overall functional safety independently of specified requirements. Lastly, the functional validation allows contrasting the functionality of the product of the development process with the original ideas or use cases derived from customer demand. Large discrepancies can already lead to another iteration at this point.

D. Model Support

In order to support managing the complexity and heterogeneity of multi-domain design tasks the macro-cycle of VDI 2206 distinctively displays the use of methods of modeling and model analysis trough all stages of development [8]. The work of Eigner et al. [9] can be used as an indicator for the support individually required in different stages of the reference development process. The work illustrates how early design models and simulation models can support the different stages of the cross-domain collaboration during system design and integration.

Functional models are used to identify a suitable functional solution in the early design phase. Hence, they describe systems solely with respect to their desired functionality and not to their technical implementation. That allows for later consideration of various technical solution using the same functional description. Thus, after the first iterations, the functional model can be a stable element of the development process.

In early iterations, the domain-specific design might even be accomplished on the model level only. Thereby, the product of such development cycles would be a detailed simulation model that has been virtually tested, and no physical product would be developed.

Fig. 3 shows the addition of modeling and simulation support through the different stages. Early models can already be used in the first tasks of the development process, e.g. to simulate functionality and support the functional concept identification. Though not mandated, safety analyses might also be used during HARA to derive a complete set of effective functional safety requirements [2]. Using system models and advanced analysis techniques might be advantageous when design specifications are still mostly unclear or multiple approaches have to be analyzed and compared before detailing the functional requirements [5]. Model support in finding and defining malfunctions can ultimately lead to more sophisticated safety goals.

However, using deductive techniques like fault trees might require system architecture views that are usually not detailed at this early stage of development. One approach is the creation of preliminary fault trees for critical safety goals that describe only basic functional dependencies (cf. STPA control diagrams [4]). Those can be detailed and updated after details of the technical implementation are specified. Thereby, the same but extended fault tree can again be used while creating a technical safety concept.

As described earlier, modeling and model analysis are important components of the system design, realization, and integration. Models will help identifying design challenges early and deciding on required item refinements. In the stage of system integration, Hardware-in-the-loop methods can be

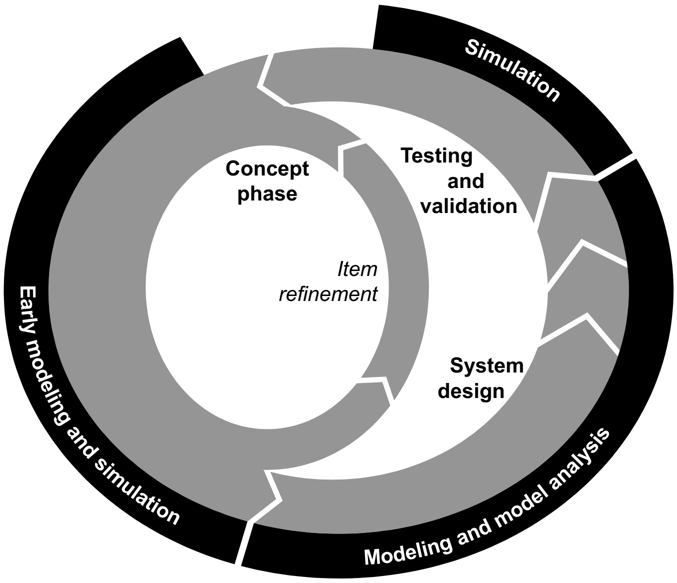

Fig. 3. Model Support in the Different Stages of Systematic Design

used to support the task. These allow for the analysis of a combination of real and virtual components.

Finally, sophisticated simulation allow parts of the testing and validation to be done virtually. Safety analysis techniques might also be used for verification of safety requirements.

E. Discussion of Additional Changes

The main additions to the development model in contrast to earlier versions, especially the adaption to the functional safety standard, have been discussed earlier. Smaller changes will be commented in this section.

In an earlier version, checking the technical feasibility of a vague functional concept was a first step for specifying functional requirements. Due to the fact of feasibility being an aspect in multiple stages of development, this task is not listed individually in the development cycle presented. Based on individual experience, feasibility will be regarded by using cross-domain expert knowledge to find a functional safety concept and to specify the functional requirements. In a similar manner, technical feasibility of agreed functional concept will again be checked when specifying technical requirements within the system design phase.

Furthermore, in contrast to prior process models, system design aspects characteristic for automotive systems, particularly packaging, do not appear as individual tasks. They are now described as additional requirements to be considered in the specification of the system design.

IV. Conclusion

In order to integrate the early safety life cycle of ISO 26262 into a reference process for the early design phase of driver assistance systems, a new design model is proposed in this contribution. Multiple adaptions of the prior version of the cycle model are implemented, while the original structure of the model, compromising of an inner cycle and an outer cycle, was preserved. The model arranges tasks of the concept phase and system design of automotive systems to illustrate dependencies. The individual steps are explained in detail in their respective section. An additional layer signifies how methods of modeling and model analysis can be used in different stages of the development process.

In the future, the discussion of modeling support and simulation in the early development process, can be continued considering scenario-based approaches. Also, multiple extensions of the proposed model are feasible. Additional layers can include aspects not yet covered by the design model (e.g. automotive security requirements in different stages of development). Lastly, applications of the reference process in industrial case studies will allow a qualitative evaluation of the adaptions made.

Acknowledgment

This paper incorporates results of the research project aFAS. The project aFAS is partially funded by the German Federal Ministry of Economics and Technology (BMWi).

References

[1] M. Maurer and K.-F. Wörsdörfer, "Unfallschwereminderung durch Fahrerassistenzsysteme mit maschineller Wahrnehmung – Potentiale und Risiken," presented at the Seminar Fahrerassistenzsysteme und aktive Sicherheit, Essen, Germany, 2002.

[2] *Road vehicles – Functional safety*, Int. Org. for Standardization (ISO) Standard 26262:2011.

[3] *Functional safety of electrical/electronic/programmable electronic safety-related systems*, Int. Electrotechnical Commission (IEC) Standard 61508:2010.

[4] N. Leveson, *Engineering a safer world: systems thinking applied to safety.* Cambridge, MA, USA: MIT Press, 2011.

[5] D. Sexton, A. Priore, and J. Botham, "Effective functional safety concept generation in the context of ISO 26262," in *SAE Int. J. of Passenger Cars - Electron. and Elect. Syst.*, vol. 7, no. 1, pp. 95–102, May, 2014.

[6] J. Rieken, A. Reschka, and M. Maurer, "Development process of forward collision prevention systems," in *Handbook of Driver Assistance Systems*, H. Winner, S. Hakuli, F. Lotz, and C. Singer, Eds. Cham, Switzerland: Springer Int., 2016, pp. 1177–1206.

[7] *Design methodology for mechatronic systems*, Verein Deutscher Ingenieure (VDI) Standard 2206, 2004.

[8] J. Gausemeier and S. Moehringer, "New guideline VDI 2206 – a flexible procedure model for the design of mechatronic systems," presented at the 14th Int. Conf. Eng. Design, Stockholm, Sweden, 2003.

[9] M. Eigner, T. Gilz, and R. Zafirov, "Proposal for functional product description as part of a PLM solution in interdisciplinary product development," in *Proc. Int. Design Conf.*, 2012, pp. 1667–1676.

[10] M. Follmer, P. Hehenberger, S. Punz, R. Rosen and K. Zeman, "Approach for the creation of mechatronic system models," presented at the 18th Int. Conf. Eng. Design, Lyngby/Copenhagen, Denmark, 2011.

[11] K. Anzengruber, P. Hehenberger, S. Boschert, R. Rosen and K. Zeman, "Development and usage of a mechatronic design process model with focus on assumptions," in *Proc. Int. Workshop Integrated Design Eng.*, 2014, pp. 37–47.

[12] T. Stolte, G. Bagschik, A. Reschka, and M. Maurer, "Hazard analysis and risk assessment for an automated unmanned protective vehicle," in *2017 IEEE Intelligent Vehicles Symp.*, to be published.

[13] K. D. Mueller-Glaser, C. Reichmann, M. Kuehl, and S. Benz, "Quality assurance and certification of software modules in safety critical automotive electronic control units using a CASE-tool integration platform," in *Automotive Software – Connected Services in Mobile Networks*, M. Broy, I. H. Krüger, and M. Meisinger, Eds. Berlin, Germany: Springer, 2006, pp. 15–30.

[14] J. Schäuffele and T. Zurawka, *Automotive software engineering: principles, processes, methods, and tools.* Warrendale, PA, USA: SAE Int., 2005.