FUNCTIONAL SAFETY CONCEPT GENERATION WITHIN THE PROCESS OF PRELIMINARY DESIGN OF AUTOMATED DRIVING FUNCTIONS AT THE EXAMPLE OF AN UNMANNED PROTECTIVE VEHICLE

Graubohm, Robert; Stolte, Torben; Bagschik, Gerrit; Steimle, Markus; Maurer, Markus

Technische Universität Braunschweig - Institute of Control Engineering

ABSTRACT

Structuring the early design phase of automotive systems is an important part of efficient and successful development processes. Today, safety considerations (e.g., the safety life cycle of ISO 26262) significantly affect the course of development. Preliminary designs are expressed in functional system architectures, which are required to form safety concepts. Thus, mapping tasks and work products to a reference process during early design stages is an important part of structuring the system development. This contribution describes the systematic creation and notation of the functional safety concept within the concept phase of development of an unmanned protective vehicle within the research project aFAS. Different stages of preliminary design and dependencies between them are displayed by the work products created and used. The full set of functional safety requirements and an excerpt of the safety argument structure of the SAE level 4 application are presented.

Keywords: Automated driving, Case study, Design practice, Requirements, Risk management

Contact:
Graubohm, Robert
Technische Universität Braunschweig
Institute of Control Engineering
Germany
graubohm@ifr.ing.tu-bs.de

Cite this article: Graubohm, R., Stolte, T., Bagschik, G., Steimle, M., Maurer, M. (2019) 'Functional Safety Concept Generation within the Process of Preliminary Design of Automated Driving Functions at the Example of an Unmanned Protective Vehicle', in *Proceedings of the 22nd International Conference on Engineering Design (ICED19),* Delft, The Netherlands, 5-8 August 2019. DOI:10.1017/dsi.2019.293

1 INTRODUCTION

The design of automated driving functions and driverless cars significantly increases the already high complexity of development activities for vehicle electronics. Additional requirements have to be considered for a systematic design of driverless systems, especially to incorporate several safety aspects when human drivers are not present as fallback for shortcomings of the technical system. Thus, safety considerations have significant impact on the outcome of design processes for automated driving functions, as the argument of safety on a vehicle level is a major concern during preliminary development.
In compliance with the standard ISO 26262 (International Organization for Standardization, 2016), the formation of a safety concept has to be divided into two individual parts, addressing different levels of abstraction, the functional safety concept and the technical safety concept. During functional safety conceptualization, functional safety requirements are derived from top-level safety goals of the system under development. Safety goals are generated as part of the work product of the hazard analysis and risk assessment task of ISO 26262, which also includes an assignment of automotive safety integrity levels (ASIL) to each goal that result from a risk classification. The functional safety concept is intended to describe safety strategies in order to achieve the safety goals. During the later steps of system design, the technical safety concept is defined; it outlines implementations of the functional concept and considers specific technology decisions or performance assumptions.
As presented in a previous work (Graubohm *et al.*, 2017), the early design phase of automated driving functions can be described through an iterative reference process, depicted in Figure 1b. The process defines two loops, i.e. a flexible inner loop representing the concept phase of development and an outer loop containing implementation and testing steps. In addition to generic milestones of advanced development, stages of the functional safety life cycle of ISO 26262 can be mapped to design phases without representing a strict sequence of individual process steps. Evidently, the process steps are performed simultaneously and iteratively especially as automotive systems design faces challenges of interdisciplinary development that can even be split between teams or companies.
Iterations of the functional concept, described by the inner loop, are the focus of this paper. Interdependent stages that can be distinguished during this concept phase are: the item definition, which specifies the system functionality, the hazard analysis and risk assessment, and the functional safety concept generation. A comprehensive and consistent functional safety concept is a prerequisite in order to develop system requirements and proceed into the technical design phase.
Due to its importance in the development process, the functional safety concept, describing risk mitigation strategies for identified hazards, is one of the main objectives within the concept phase. This contribution presents findings from the research project aFAS about safety concept generation and notation. Additionally, a systematic process structure for determining a sound set of safety requirements within the process of preliminary design of automated driving functions is discussed.
First, the project context and previous works are presented in the next section. Subsequently, Section 3 introduces related work on functional safety concept generation for vehicle systems. Lastly, the process of safety concept generation in the context of the research project aFAS is discussed in Section 4.

2 PROJECT CONTEXT

The goal of the successfully completed project aFAS was the development of a system for the unmanned operation of a protective vehicle on the hard shoulder of highways in Germany. The system allows for driverless low speed operation on hard shoulders only, following a leading vehicle within a defined distance. Stolte *et al.* (2015) describe the project concept in detail. The authors illustrate the system's intended functionality and present an early functional system architecture.
Additional contributions illustrate the process of the preliminary design while pursuing safety conceptualization; for example, Bagschik *et al.* (2016) describe a method to systematically identify system hazards for automated vehicles as demanded by ISO 26262 in the context of the hazard analysis and risk assessment (HARA). The authors evaluate their results in (Bagschik *et al.*, 2017) by applying Systems-Theoretic Process Analysis (STPA) to the vehicle concept. Subsequently, Stolte *et al.* (2017) introduce an approach to structure the HARA task of development of an automated driving function used in the aFAS project. The dependencies between identified individual process steps during the HARA task have been incorporated in the reference development process presented by Graubohm *et al.* (2017).

3 RELATED WORK

This contribution investigates a structured approach for generating and documenting functional safety concepts on the basis of systematically derived abstract safety goals on a vehicle level. The externally visible behavior of the unmanned protective vehicle in the context of the safety conceptualization has first been examined by Bagschik *et al.* (2016). With regard to the definition used by Waymo (2017), the safety aspect directly addressed is the behavioral safety of the system under development. Within the early design phase, a top-down development of automated vehicles will likely focus on such safety goals describing external vehicle behavior. However, other safety aspects that will be addressed during system design specification, especially functional safety mechanisms, are included in the abstract consideration of vehicle behavior. Therefore, multiple standards, managing safety concerns within automotive development, can be simultaneously adopted, especially ISO 26262 and the upcoming ISO PAS 21448 "Safety of the intended functionality" (International Organization for Standardization, 2018).

Feth *et al.* (2018) discuss the current standard coverage defining safe behavior of automated vehicles focusing on behavioral planning functions. The authors argue that safe nominal behavior specification of level 3+ systems (SAE International, 2018) is currently not covered by standards and standard creation initiatives. They propose a multi-aspect safety engineering process, which defines different abstraction layers that influence a joint safety argument. Their approach determines sensor and algorithmic concepts before generating the functional safety concept and, thus, does not generate work products of the concept phase independent of technical implementation considerations, as performed in the aFAS project.

Johansson *et al.* (2017) discuss the iterative character of the concept phase comprising the work products of ISO 26262 in the context of the research project FUSE. The authors propose the need for additional steps and formal refinement verification when deriving safety requirements from safety goals. Abdulkhaleq *et al.* (2017) present an approach of using stages inferred from Systems-Theoretic Process Analysis after the definition of safety goals and before the specification of safety requirements. Nolte *et al.* (2017) discuss an approach for structuring the conceptualization of self-aware automated road vehicles based on investigations of skills and abilities. Based on the example of the aFAS project, it is illustrated how safety requirements can be systematically deduced from safety goals with the help of representations of the behavioral skills of the system under development.

Stolte *et al.* (2016) discuss functional safety mechanisms for actuation systems of automated vehicles as the basis of systematically deriving safety requirements and linking them with safety goals in the context of the aFAS project. As a series heavy commercial vehicle was used as the basis for the developed prototype, the systems theory-based approach presented uses concrete safety goals for functional components of the actuation system relying on extensive assumptions about the system structure.

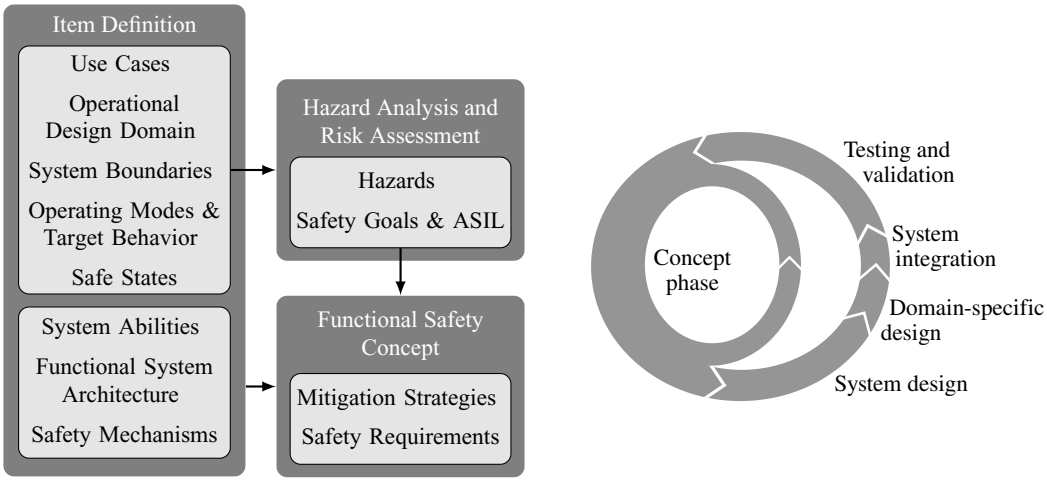
Several papers examine the safety concept design for driver assistance systems and automated vehicles with regard to functional strategies and effects on the functional architecture of the system under development, e.g., Hörwick and Siedersberger (2010); Binfet-Kull *et al.* (1998); Reschka (2016); Kocsis *et al.* (2017). These contributions commonly develop functional safety requirements; however, they do not comprise the results of the hazard analysis task. Nilsson *et al.* (2013) demonstrate the results of the process steps during concept phase of ISO 26262 for a vehicle platooning system. Safety requirements are directly derived from safety goals and allocated to a preliminary functional architecture. The authors, however, do not indicate a structured approach for deriving and documenting the safety requirements.

The safety concept generation for vehicle subsystems in the context of ISO 26262 has been performed and presented in the context of multiple projects and industrial case studies; for example, Becker *et al.* (2017) discuss safety strategies and mechanisms in reaction to a specific ASIL-C-classified safety goal for a traffic jam pilot. The authors develop requirements for the electric power supply and communication system of safety-critical components and propose a technical architectural solution. Sexton *et al.* (2014) apply safety analysis techniques on a shift-by-wire system to derive requirements from potential safety goal violations. Krithivasan *et al.* (2015) systematically develop functional safety requirements from a set of safety goals for an electronic throttle controller using a process-modelling concept. Habli *et al.* (2010) describe the model-based design of a safety argument for an air suspension system comprising the functional safety concept. The safety concept notation used by the authors matches the approach used in the aFAS project (cf. Section 4.1). In contrast, some approaches use UML-based diagrams for development and documentation of safety requirements, e.g., Gillen *et al.* (2014); Beckers *et al.* (2014); Antonino and Trapp (2014).

It can be concluded that few of the published functional safety concepts deduce safety requirements based on the abstract description of desired vehicle behavior, as it was performed within the aFAS project. Additionally, a systematic process outline for safety requirement deduction and traceable documentation for a SAE level 3+ system is presented in this paper. The created functional safety concept of the unmanned protective vehicle is discussed in Section 4.2.

4 FUNCTIONAL SAFETY CONCEPT GENERATION

A process structure can be inferred from the experiences regarding functional safety concept generation in the research project aFAS. The safety requirement analysis depends on information of prior work products of the concept phase of ISO 26262. Key inputs of the design process are depicted in Figure 1a. Data generated and used within the item definition and HARA task is itemized and connected with subsequent steps using arrows. As discussed earlier, the functional safety concept is an important objective of the concept phase, depicted as an inner loop within the reference process shown in Figure 1b.



(a) Input of the Functional Safety Concept Design

(b) Structure of the Design Model (Graubohm *et al.*, 2017)

Figure 1. Functional safety concept design within the concept phase of development

Based on our observations in the research project, the item definition of ISO 26262 is a living document during the preliminary design stage. While the HARA task can be performed using an early item definition, lacking major concept design information, the safety concept generation requires comprehensive information on architectural assumptions. Furthermore, a consistent set of safety goals has to be available before a safety concept can be created, as safety concepts break down safety goals into requirements. Iterations in the form of item refinements, describing the adaptations of the item definition in response to design conflicts identified during the HARA task, have been described in previous work (Stolte *et al.*, 2017; Graubohm *et al.*, 2017).

The fundamental difference between safety goal definition and functional safety concept generation is the condition that safety requirements have to allow implementation. While safety goals are formulated abstractly, directly addressing the hazards identified, functional safety requirements are formed with respect to a preliminary functional system architecture, assigning formal requirements to functional elements of the system under development. Hence, the functional safety concept is the link between the functional concept and the technical design.

Mitigation strategies are deployed for breaking down safety goals into requirements. These strategies integrate information stemming from the item definition, i.e. system abilities and planned safety mechanisms strongly influence the outcome of safety requirement deduction. In order to document applied strategies and improve traceability within the work products of the concept phase, a graphical notation can be used, as discussed in the following section (cf. 4.1).

Each safety goal is broken down into one or many safety requirements, while one individual safety requirement can also realize multiple safety goals. The safety requirements and architectural elements assigned inherit the highest ASIL from the linked safety goals, unless the ASIL is decomposed,

reflecting that safety measures are split into redundant safety requirements, allocated to independent architectural elements.

4.1 Functional safety concept notation

The functional safety requirements deduced during safety concept creation are often presented in tabular form. This allows for easy documentation and adaptation of individual requirements. However, the traceability of considerations and decisions within the safety conceptualization is limited and changes likely result in inconsistencies. Using semi-formal notations to record functional safety concepts in graphical form enables illustration and documentation of links between safety goals, requirements, and applied strategies. Graphical safety argument structures also improve readability and avoid ambiguity.
The graphical representation applies argumentation structures typically used within safety cases. Thus, using graphical notations during safety concept creation generates preliminary safety arguments that can be extended and reassessed during the course of development. Eventually, the results of validation and verification activities can be included as evidence in the graphical safety argument (Bishop and Bloomfield, 1998; Kelly, 1998).
In the aFAS project, we used the Goal Structuring Notation (GSN) (SCSC Assurance Case Working Group, 2018) for graphical safety concept documentation. The basic elements defined within the semi-formal notation standard are shown in Figure 2. In general, statements are represented through rectangles and evidence is represented through circles in GSN. Solid arrows mark links in the context of an argument structure, in which strategies in the form of a parallelogram can also be included. Context information, assumptions, and justifications are represented through elliptical shapes and connected to other nodes of the argument structure through empty arrows.

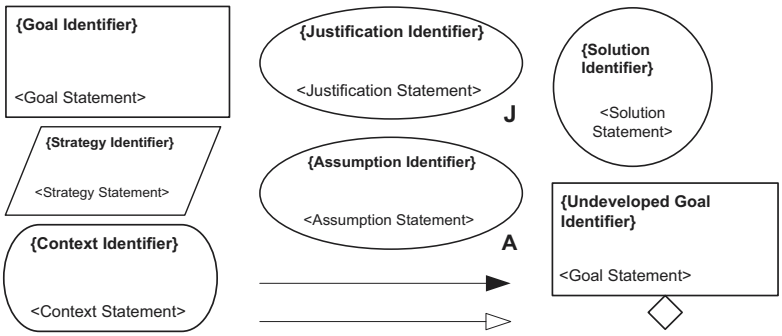
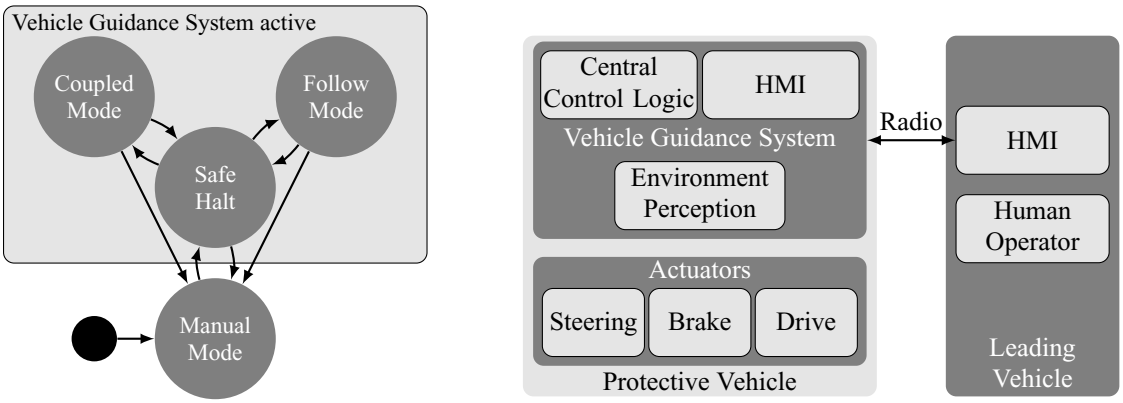


Figure 2. Elements of the goal structuring notation (SCSC Assurance Case Working Group, 2018)

The pattern of safety arguments in GSN focusses on breaking down top-level goals into multiple sub-goals. Hence, in the context of a functional safety concept, the notation can be used for breaking down safety goals into safety requirements. In later stages of development, the notation can also be employed for linking technical requirements with functional requirements.

4.2 Functional safety concept of the aFAS project

As discussed above, the results of the HARA task of the system under development are a required input of the functional safety concept generation. The hazard analysis process centrally relies on the definition of operating modes and target behavior within the item definition. The operating modes specified in the aFAS vehicle guidance system are shown in Figure 3a.
Process and results of the HARA for the operation of an unmanned protective vehicle without human supervision are presented by Stolte *et al.* (2017). The safety goals and the classification assigned are listed in Table 1. As the hazard analysis was performed in the context of the vehicle guidance system, the majority of safety goals defined is only applicable during specific operating modes.
Additional required input from the context of the item definition was presented in other previous contributions. Illustrating the systematic deduction of safety requirements from safety goals, Nolte *et al.* (2017) provide an example of the graphical system ability representation. These skill graphs are used



(a) Operating Modes (Stolte *et al.*, 2015) (b) Functional Components

Figure 3. Modes of operation and functional components of the aFAS system

Table 1. Safety goals and ASIL classification in aFAS project following Stolte et al. (2017)

ID	Safety Goal	ASIL
SG01	Unintended and not permitted operating mode change must be prevented	B
SG02	Intended and permitted operating mode change to Safe Halt must be ensured	B
SG03	Steering actuation beyond specification must be prevented	D
SG04	Unintended anti-lock brake actuation must be prevented	C
SG05	Unintended acceleration must be prevented	QM
SG06	Detection of driver intervention must be ensured	QM
SG07	Display of actual operating mode in HMI must be ensured	B
SG08	Unintended vehicle movement must be prevented	B
SG09	Deceleration to standstill must be ensured	B
SG10	Leaving tolerance ranges must trigger operating mode change to Safe Halt	QM
SG11	Maximum vehicle speed specified must not be exceeded	B
SG12	Overrunning hard shoulder markings must be prevented	B
SG13	Detection of and reaction to (deceleration to standstill) relevant obstacles must be ensured	QM
SG14	Identification of leading vehicle must be ensured	QM
SG15	Detection of missing leading vehicle and operating mode change to Safe Halt must be ensured	QM
SG16	Anti-lock functionality must be ensured	D
SG17	Unintended steering actuation must be prevented	D

to break down the external behavior into functional categories as an input for deriving strategies to obtain and assign functional safety requirements. Skill graphs represent a system architecture within a capability viewpoint (Bagschik *et al.*, 2018). Thus, the functional system architecture as an alternative viewpoint on the system shares the same functional components. A thorough introduction to the functional system architecture, including the information flow between components, can be found in Stolte *et al.* (2015). Components considered during safety concept creation are depicted in Figure 3b.

The functional components addressed to fulfill all safety goals are split between the protective vehicle and the leading vehicle, which are connected through a radio link. Requirements are derived for human-machine interfaces in both vehicles and the wireless connection. Additionally, the human operator manually driving the protective vehicle to the job site and changing into the leading vehicle is included in the safety concept. The components of the protective vehicle include the actuator subsystems as well as HMI, control logic, and environment perception of the vehicle guidance system.

Characteristical safety goals within the aFAS project result from the target behavior of the automated protective vehicle to maintain a safe distance to the left lane marking at all times. Hazards of high severity and low controllability result from potentially entering the adjacent traffic lane, in which flowing traffic with high differential speed is expected. Thus, Safety Goal 3, which is used to argue the ASIL level of Safety Goal 12, is a key element of the safety concept. Figure 4 shows the excerpt of the functional safety concept addressing Safety Goal 3, it serves as an example for split argument structures. Different strategies were identified to prevent steering actuation beyond specification. Requirements can result from both strategies independently, while also a joint requirement assigned to the brake system was created.

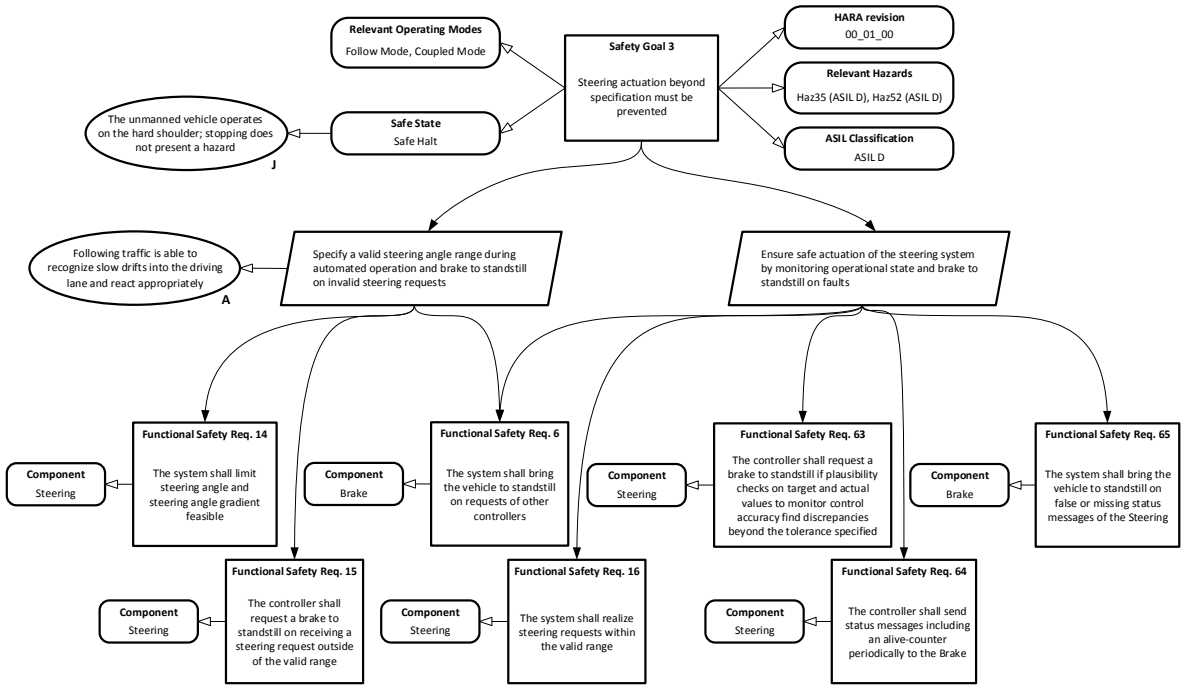


Figure 4. Excerpt of the functional safety concept addressing safety goal 3

The graphical structure allows for linking various information of the HARA results to the safety goal. Functional safety requirements are connected to the safety goal through a strategy node, forming an argument structure also including assumptions and justifications. In the context of the GSN standard, functional safety requirements during the concept phase of development might also be represented through undeveloped goal identifiers (cf. Figure 2), imparting that evidence is not yet linked to the statements made (Kelly *et al*., 1997).

Also in cases of safety goals being applicable in both, manual and automated operation, different paths within the argument structure were developed. An example is Safety Goal 1, aiming to prevent unintended and not permitted operating mode changes. During manual operation, the hazards are mitigated by using a main switch as part of the HMI in the protective vehicle to disconnect the vehicle guidance system from any power supply. The switch is secured against accidental switch-on and the strategy justified by required safety training of the human operator. In contrast, during the automated operation, the main switch cannot be part of the strategy to prevent false mode changes. Thus, a permanent monitoring of system states within the central controller logic was designed.

A detailed listing of all functional safety requirements, the assigned components and the highest associated ASIL classification can be found in the Appendix.

5 CONCLUSION

The systematic process structure for determining safety requirements in the concept phase of development was discussed in this contribution. Additionally, findings about safety concept generation and notation from the research project aFAS were presented, including an excerpt of the safety argument structure and the full set of safety requirements of the SAE level 4 application. The graphical form used for the documentation improves tractability of requirements and readability of argument structures; however, the semi-formal notation does not guarantee the validity of the safety argument. As GSN elements contain free-text statements, a thorough validation of the functional safety concept has to be performed before proceeding with further steps of system design.

The safety concept presented has proven itself in practice during the development of the protective vehicle guidance system, demonstrated in public traffic at the end of the project. In the future, the discussion of a structured extension of the safety arguments towards automotive safety cases will be continued. Lastly, novel insights will be obtained in the safety concept generation for driverless vehicles for inner-city traffic in the research project UNICARagil (cf. Woopen *et al*., 2018). The applicability of

the presented approach will be evaluated in the context of the different operational design domain and larger number of functional components.

REFERENCES

Abdulkhaleq, A., Wagner, S., Lammering, D., Boehmert, H. and Blueher, P. (2017), "Using STPA in Compliance with ISO 26262 for Developing a Safe Architecture for Fully Automated Vehicles", In: Dencker, P., Klenk, H., Keller, H. B. and Plödereder, E. (Ed.), *Automotive - Safety & Security 2017*, Gesellschaft für Informatik, Bonn, Germany, pp. 149–162.

Antonino, P. O. and Trapp, M. (2014), "Improving Consistency Checks between Safety Concepts and View Based Architecture Design", *Probabilistic Safety Assessment and Management PSAM 12*, Honolulu, HI, USA, International Association for Probabilistic Safety Assessment and Management.

Bagschik, G., Nolte, M., Ernst, S. and Maurer, M. (2018), "A System's Perspective Towards an Architecture Framework for Safe Automated Vehicles", *IEEE 21st International Conference on Intelligent Transportation Systems*, Maui, HI, USA, IEEE, pp. 2438–2445. https://doi.org/10.1109/itsc.2018.8569398

Bagschik, G., Reschka, A., Stolte, T. and Maurer, M. (2016), "Identification of Potential Hazardous Events for an Unmanned Protective Vehicle", *IEEE Intelligent Vehicles Symposium*, Gothenburg, Sweden, IEEE, pp. 691–697. https://doi.org/10.1109/ivs.2016.7535462

Bagschik, G., Stolte, T. and Maurer, M. (2017), "Safety Analysis Based on Systems Theory Applied to an Unmanned Protective Vehicle", *Procedia Engineering*, Vol. 179, pp. 61–71. https://doi.org/10.1016/j.proeng.2017.03.096

Becker, J., Helmle, M. and Pink, O. (2017), "System Architecture and Safety Requirements for Automated Driving", In: Watzenig, D. and Horn, M. (Ed.), *Automated Driving*, Springer International Publishing, Cham, Switzerland, pp. 265–283. https://doi.org/10.1007/978-3-319-31895-0_11

Beckers, K., Côté, I., Frese, T., Hatebur, D. and Heisel, M. (2014), "Systematic Derivation of Functional Safety Requirements for Automotive Systems", In: Bondavalli, A. and Di Giandomenico, F. (Ed.), *Computer Safety, Reliability, and Security*, Vol. 8666, Springer International Publishing, Cham, Switzerland, pp. 65–80. https://doi.org/10.1007/978-3-319-10506-2_5

Binfet-Kull, M., Heitmann, P. and Ameling, C. (1998), "System Safety for an Autonomous Driving Vehicle", *IEEE International Conference on Intelligent Vehicles*, Stuttgart, Germany, IEEE, pp. 469–474.

Bishop, P. and Bloomfield, R. (1998), "A Methodology for Safety Case Development", In: Redmill, F. and Anderson, T. (Ed.), *Industrial Perspectives of Safety-critical Systems*, Springer London, England, pp. 194–203. https://doi.org/10.1007/978-1-4471-1534-2_14

Feth, P., Adler, R., Fukuda, T., Ishigooka, T., Otsuka, S., Schneider, D., Uecker, D. and Yoshimura, K. (2018), "Multi-aspect Safety Engineering for Highly Automated Driving: Looking Beyond Functional Safety and Established Standards and Methodologies", In: Gallina, B., Skavhaug, A. and Bitsch, F. (Ed.), *Computer Safety, Reliability, and Security. Lecture Notes in Computer Science*, Vol. 11088, Springer International Publishing, Cham, Switzerland, pp. 59–72. https://doi.org/10.1007/978-3-319-99130-6_5

Gillen, C., Hesse, L. and Lammermann, M. (2014), "The Efficient Safety Concept of the SpeedE Steer-By-Wire System", *23rd Aachen Colloquium Automobile and Engine Technology*, Aachen, Germany, pp. 379–387.

Graubohm, R., Stolte, T., Bagschik, G., Reschka, A. and Maurer, M. (2017), "Systematic Design of Automated Driving Functions Considering Functional Safety Aspects", *8. Tagung Fahrerassistenz*, Munich, Germany, Chair of Automotive Technology with TÜV SÜD Academy.

SCSC Assurance Case Working Group (2018), *GSN Community Standard*, Version 2, SCSC.

Habli, I., Ibarra, I., Rivett, R. S. and Kelly, T. (2010), "Model-Based Assurance for Justifying Automotive Functional Safety", *SAE World Congress & Exhibition*, Detroit, MI, USA, SAE International. https://doi.org/10.4271/2010-01-0209

Hörwick, M. and Siedersberger, K.-H. (2010), "Strategy and Architecture of a Safety Concept for Fully Automatic and Autonomous Driving Assistance Systems", *IEEE Intelligent Vehicles Symposium*, La Jolla, CA, USA, IEEE, pp. 955–960. https://doi.org/10.1109/ivs.2010.5548115

International Organization for Standardization (2016), *ISO/DIS 26262: Road vehicles : Functional safety*, ISO, Geneva, Switzerland.

International Organization for Standardization (2018), *ISO/PRF PAS 21448: Road vehicles : Safety of the intended functionality*, ISO, Geneva, Switzerland.

Johansson, R., Nilsson, J., Bergenhem, C., Behere, S., Tryggvesson, J., Ursing, S., Söderberg, A., Törngren, M. and Warg, F. (2017), "Functional Safety and Evolvable Architectures for Autonomy", In: Watzenig, D. and Horn, M. (Ed.), *Automated Driving*, Springer International Publishing, Cham, Switzerland, pp. 547–560. https://doi.org/10.1007/978-3-319-31895-0_25

Kelly, T. P. (1998), *Arguing Safety: A Systematic Approach to Managing Safety Cases*, PhD Thesis, University of York, England.
Kelly, T. P., Bate, I. J., McDermid, J. A. and Burns, A. (1997), "Building a Preliminary Safety Case: An Example From Aerospace", *Proceedings of the Australian Workshop on Industrial Experience with Safety Critical Systems and Software*, Sydney, Australia, Australian Computer Society.
Kocsis, M., Susmann, N., Buyer, J. and Zollner, R. (2017), "Safety Concept for Autonomous Vehicles that Operate in Pedestrian Areas", *IEEE/SICE International Symposium on System Integration*, Taipei, Taiwan, IEEE, pp. 841–846. https://doi.org/10.1109/sii.2017.8279327
Krithivasan, G., Taylor, W. and Nelson, J. (2015), "Developing Functional Safety Requirements using Process Model Variables", *SAE World Congress & Exhibition*, Detroit, MI, USA, SAE International. https://doi.org/10.4271/2015-01-0275
Nilsson, J., Bergenhem, C., Jacobson, J., Johansson, R. and Vinter, J. (2013), "Functional Safety for Cooperative Systems", *SAE World Congress & Exhibition*, Detroit, MI, USA, SAE International. https://doi.org/10.4271/2013-01-0197
Nolte, M., Bagschik, G., Jatzkowski, I., Stolte, T., Reschka, A. and Maurer, M. (2017), "Towards a Skill- And Ability-Based Development Process for Self-Aware Automated Road Vehicles", *IEEE 20th International Conference on Intelligent Transportation Systems*, Yokohama, Japan, IEEE. https://doi.org/10.1109/itsc.2017.8317814
Reschka, A. (2016), "Safety Concept for Autonomous Vehicles", In: Maurer, M., Gerdes, J. C., Lenz, B. and Winner, H. (Ed.), *Autonomous Driving*, Springer Berlin Heidelberg, Germany, pp. 473–496. https://doi.org/10.1007/978-3-662-48847-8_23
SAE International (2018), *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*, SAE. https://doi.org/10.4271/j3016_201806
Sexton, D., Priore, A. and Botham, J. (2014), "Effective Functional Safety Concept Generation in the Context of ISO 26262", *SAE International Journal of Passenger Cars - Electronic and Electrical Systems*, Vol. 7 No.1, pp. 95–102. https://doi.org/10.4271/2014-01-0207
Stolte, T., Bagschik, G. and Maurer, M. (2016), "Safety Goals and Functional Safety Requirements for Actuation Systems of Automated Vehicles", *IEEE 19th International Conference on Intelligent Transportation Systems*, Rio de Janeiro, Brazil. IEEE, pp. 2191–2198. https://doi.org/10.1109/itsc.2016.7795910
Stolte, T., Bagschik, G., Reschka, A. and Maurer, M. (2017), "Hazard Analysis and Risk Assessment for an Automated Unmanned Protective Vehicle", *IEEE Intelligent Vehicles Symposium*, Redondo Beach, CA, USA, IEEE, pp. 1848–1855. https://doi.org/10.1109/ivs.2017.7995974
Stolte, T., Reschka, A., Bagschik, G. and Maurer, M. (2015), "Towards Automated Driving: Unmanned Protective Vehicle for Highway Hard Shoulder Road Works", *IEEE 18th International Conference on Intelligent Transportation Systems*, Las Palmas de Gran Canaria, Spain, IEEE, pp. 672–677. https://doi.org/10.1109/itsc.2015.115
Waymo (2017), *Waymo Safety Report: On the Road to Fully Self-Driving*, Waymo, Mountain View, CA, USA.
Woopen, T., Lampe, B., Böddeker, T., Eckstein, L., Kampmann, A., Alrifaee, B., Kowalewski, S., Moormann, D., Stolte, T., Jatzkowski, I., Maurer, M., Möstl, M., Ernst, R., Ackermann, S., Amersbach, C., Leinen, S., Winner, H., Püllen, D., Katzenbeisser, S., Becker, M., Stiller, C., Furmans, K., Bengler, K., Diermeyer, F., Lienkamp, M., Keilhoff, D., Reuss, H.-C., Buchholz, M., Dietmayer, K., Lategahn, H., Siepenkötter, N., Elbs, M., v. Hinüber, E., Dupuis, M. and Hecker, C. (2018), "UNICARagil - Disruptive Modular Architectures for Agile, Automated Vehicle Concepts", *27th Aachen Colloquium Automobile and Engine Technology*, Aachen, Germany. https://doi.org/10.18154/RWTH-2018-229909

ACKNOWLEDGMENTS

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). The project consortium consists of MAN (consortium leader), ZF TRW, WABCO, Bosch Automotive Steering, Technische Universität Braunschweig, Hochschule Karlsruhe, Hessen Mobil - Road and Traffic Management, and BASt - Federal Highway Research Institute.
We would like to thank Andreas Reschka for his contributions to the development of the functional safety concept in the aFAS project during his time at the institute.

APPENDIX

Table A1 displays the functional safety requirements developed in the project aFAS. Several IDs were discarded while the ID numbering was not adjusted, in order to preserve traceability between different functional safety concept versions. Safety goals are referenced using the IDs introduced in Table 1.

Table A1. Functional safety requirements of the aFAS project

ID	Component	Functional Safety Requirement	ASIL	Safety Goal
FSR01	HMI	The system shall contain a main switch disconnecting the vehicle guidance system from any power supply	D	SG01 SG04 SG05 SG17
FSR02	HMI	The main switch shall be secured against accidental switch-on	D	SG01 SG04 SG05 SG17
FSR03	Steering	The controller shall request a brake to standstill on missing operating mode status messages	B	SG01
FSR04	Control Logic	The controller shall send operating mode status periodically	B	SG01 SG02
FSR05	Steering	The controller shall request a brake to standstill on detecting discrepancies in the operating mode over a period greater than the tolerance specified while monitoring the state machine of the vehicle guidance system	B	SG01 SG02
FSR06	Brake	The system shall bring the vehicle to standstill on requests of other controllers	D	SG01 SG02 SG03 SG12
FSR13	Steering	The force applied to the steering wheel shall be limited to allow driver override	D	SG17
FSR14	Steering	The system shall limit steering angle and steering angle gradient feasible	D	SG03
FSR15	Steering	The controller shall request a brake to standstill on receiving a steering request outside of the valid range	D	SG03
FSR16	Steering	The system shall realize steering requests within the valid range	D	SG03
FSR19	Brake	The system shall not perform brake actuation on false requests of other controllers in Manual Mode	C	SG04
FSR23	Brake	The system shall bring the vehicle to standstill on detection of internal faults	QM	SG04
FSR24	Brake	The controller shall notify other controllers of internal faults detected	QM	SG04
FSR25	Control Logic	The system shall perform a mode change into Safe Halt on notifications of faults of the Brake	QM	SG04
FSR29	Brake	The system shall contain a safety monitor to ensure changing into Manual Mode on driver intervention	QM	SG06
FSR30	Steering	The system shall detect human intervention on the steering wheel and communicate intervention to other controllers	QM	SG06
FSR31	Brake	The system shall detect human intervention on the brake pedal and communicate intervention to other controllers	QM	SG06
FSR32	Drive	The system shall detect human intervention on the accelerator pedal and communicate intervention to other controllers	QM	SG06
FSR34	HMI	The controller shall acknowledge receipt of messages of the Control Logic	B	SG07
FSR35	HMI	The system shall display error states	B	SG07
FSR36	HMI	The system shall read out the operating mode indicator and perform a plausibility check on target and indicated values	B	SG07
FSR37	Radio	The link shall support an end-to-end protection mechanism and include an alive-counter	B	SG07
FSR38	Control Logic	The controller shall acknowledge receipt of messages of the HMI	B	SG07
FSR39	Control Logic	The system shall remain in Coupled Mode on detecting faults in sending operating mode status	B	SG07
FSR40	Control Logic	The system shall perform a mode change into Safe Halt on detecting faults in sending operating mode status in Follow Mode	B	SG07
FSR42	Brake	The system shall hold the vehicle at standstill in Safe Halt mode	B	SG08
FSR43	Control Logic	The controller shall continuously send the Safe Halt condition to the Brake	B	SG08
FSR45	Control Logic	The controller shall communicate the operating mode change into Safe Halt to the Brake	B	SG09
FSR46	Brake	The system shall bring the vehicle to standstill on mode change into Safe Halt	B	SG09
FSR47	Environment Perception	The system shall determine the lateral and longitudinal distance of the leading vehicle with sufficient precision and communicate the result to other controllers	QM	SG10
FSR48	Control Logic	The system shall perform a mode change into Safe Halt on one or both distance values of the leading vehicle exceeding their tolerance band	QM	SG10
FSR49	Brake	The system shall determine the vehicle speed with sufficient precision	B	SG11
FSR50	Brake	The system shall bring the vehicle to standstill on detection of vehicle speed exceeding the limit specified	B	SG11
FSR52	Steering	The controller shall request a brake to standstill on falling below the minimum distance to the left lane marking specified	B	SG12
FSR54	Environment Perception	The system shall determine the relative distance of the vehicle to the left lane marking and communicate the result to other controllers	B	SG12
FSR57	Control Logic	The system shall perform a mode change into Safe Halt on falling below the minimum distance to detected obstacles specified	QM	SG13
FSR58	Environment Perception	The system shall detect relevant obstacles and communicate their relative position to other controllers	QM	SG13
FSR59	Human Operator	Operating instructions on initializing automated operation shall be prepared on the basis of the item definitions	QM	SG14
FSR60	Environment Perception	The controller shall notify other controllers of a missing leading vehicle	QM	SG14 SG15
FSR61	Control Logic	The system shall perform a mode change into Safe Halt on notifications of a missing leading vehicle	QM	SG14 SG15
FSR62	Brake	The system shall ensure anti-lock functionality according to the specifications	D	SG16
FSR63	Steering	The controller shall request a brake to standstill if plausibility checks on target and actual values to monitor control accuracy find discrepancies beyond the tolerance specified	D	SG03
FSR64	Steering	The controller shall send status messages including an alive-counter periodically to the Brake	D	SG03
FSR65	Brake	The system shall bring the vehicle to standstill on false or missing status messages of the Steering	D	SG03
FSR66	Human Operator	Operating instructions shall state that an obstacle has to be removed before starting automated operation	QM	SG13
FSR67	Control Logic	The controller shall communicate the operating mode change into Manual Mode to the Brake	C	SG04