Approach to Maintain a Safe State of an Automated Vehicle in Case of Unsafe Desired Behavior

Christoph Popp* , Stefan Ackermann* , Hermann Winner*

Abstract: For automated driving, higher levels of automation pose new challenges in terms of safety. In this paper, we develop a generic behavior safety framework that maintains a safe vehicle state even in case of system failures. It is applicable to different configurations of automated driving system architectures. We verify the designed generic behavior safety framework by applying it to two different architectures from both projects PRORETA 5 and UNICAR*agil*. The previously defined safety requirements are met with both applications, which indicates that the developed generic safety framework is also valid for other configurations of automated driving systems.

Keywords: automated driving, minimal risk condition, safety, vehicle behavior

1 Introduction

Providing safety for automated vehicles remains an unsolved challenge for stakeholders of automated driving. In operation, an automated vehicle shall provide safe behavior at all times. Unsafe desired behavior led to fatal accidents in the past. For example, there were accidents involving vehicles from Tesla in 2016 [1] and Uber in 2018 [2]. The published accident reports reveal that both accidents were caused by faults in the processing sequence between environment perception and desired behavior planning combined with failed vehicle behavior monitoring by the safety driver. These vehicles were not in SAE level 4 operation mode.

Those fatal accidents prove that the state of the art automated driving functions (perception, interpretation and behavior planning) do not yet have the necessary capabilities to generate safe vehicle behavior at any given time. We propose our Behavior Safety Framework (BSF). It is a necessary component to aim to keep automated vehicles in a safe state for state of the art automated vehicles. In this paper, we present the state of the art for safeguarding the desired behavior of automated vehicles and elaborate the lack of a BSF providing safe vehicle behavior in all driving situations. We further identify the requirements for such a safety framework and design a generic modular architecture. We verify this architecture in a formal way and also by applying the generic architecture to two specialized applications within different automated driving system (ADS) configurations. We conclude that our generic architecture meets our set of requirements and that the verification, both formally and by applying it to two example applications, indicate that the generic architecture is valid for other ADS configurations as well.

*Institute of Automotive Engineering (FZD) at Technical University of Darmstadt, 64287 Darmstadt (e-mail: *firstname.lastname*@tu-darmstadt.de).

2 Methodology

The purpose of this paper is to provide a functional safety assessment of the desired behavior of an automated vehicle equipped with a level 4 ADS according to SAE J3016 [3] and to generate a safe desired behavior if needed. We begin with a survey of the state of the art for safeguarding the desired behavior of a highly automated vehicle in Section 3. By comparing the state of the art with our problem statement, we conclude that it does not provide a generic modular architecture of a BSF. This conclusion motivates the development of such a framework in Section 4. In Section 4.1 and 4.2, we provide definitions and derive the requirements for a modular BSF, based on which we design a generic architecture for the BSF in Section 4.3. The verification of our architecture is done using two approaches in Section 5. For the first approach, we formally compare the capabilities of our BSF with the requirements. For the second approach, we apply our generic architecture to two applications with different ADS configurations and verify that the requirements are met even with different ADS configurations. Finally, we review our results and give an outlook on future research in Section 6.

3 State of the Art

The literature overview contains several approaches for safeguarding automated vehicles. Some of these are briefly presented below.

Shalev-Shwartz et al. [4], Nistér et al. [5], and based on these, de Iaco et al. [6] provide formal behavioral descriptions that prevent collisions between road users. If all road users adhere to mathematically defined safety distances in the longitudinal and lateral directions as well as other behavioral guidelines and react appropriately in dangerous situations, no collisions can occur. Other behavioral guidelines are among others to "not cut-in recklessly", that "right-of-way is given, not taken" in cooperative situations and to "be careful of areas with limited visibility" [4].

Molina et al. [7] present an architecture approach for vehicle behavior safeguarding where the outputs from the behavior planning modules are not tested directly, but indirectly by monitoring the vehicle behavior. The monitoring system is equipped with environmental perception separated from the primary environment perception and intervenes when criticalities are detected. It then overrides the controller output of the primary system and specifies a risk-minimizing vehicle behavior corresponding to the situation.

Stolte et al. [8] develop an ADS for an unmanned protective vehicle for the highway hard shoulder. In the event of component or system failures, or if the defined system limit is exceeded, the vehicle brakes to standstill. The vehicle estimates its own perception quality and uses sensor redundancies to ensure the required safety.

Pek et al. [9] present a safety layer that can be used for existing motion planners. During the operation of the automated vehicle, all legally possible movements of other road users are predicted and the safety of the current traffic situation is thus assessed in real time. In case of identified unsafeties, a combination of reachability analysis and convex optimization is used to determine drivable fail-safe emergency trajectories that end in a safe area with vehicle standstill. Similarly, the concept of Stahl et al. [10] checks the results of specific modules whose functional safety can only be insufficiently proved. In case of unsafety, a previously defined emergency braking trajectory is used.

Further approaches for emergency trajectories are presented, among others, by Funke et al. [11], Hilgert et al. [12] and Mehmed et al. [13]. For emergency maneuvers, Reschka [14] considers three options: Decelerating with constant steering angle, decelerating along the last calculated path, or stopping at a suitable place, for example on the roadside. Ackermann and Winner [15] present another option for an emergency maneuver: The behavior planner searches for safe stop locations and plans a minimal risk maneuver as described in ISO/TR 4804 [16] and ISO/DIS 21448 [17] to these locations. The purpose of this is to reach the minimal risk condition for each emergency situation.

In summary, literature contains many different approaches to increase safety of automated vehicles. We listed formal behavior rule definitions and various concepts to ensure the safety of the whole ADS. Still, the state of the art does not provide a generic architecture of a BSF that fully safeguards the desired behavior of an ADS for an automated vehicle. In most of the safeguarding concepts from literature, it is assumed that the vehicle environment is always perceived by the perception system according to reality. Thus, false-negative object detections, e.g. due to damaged or decalibrated sensors, are neglected. Also, failures of sensors or the entire ADS are barely addressed in the literature.

4 Behavior Safety Framework

4.1 Definitions

In this chapter, we define the terminology that we use for the development of the BSF.

Automated Driving System (ADS)
First, we present our definition of an automated driving system (ADS), which is shown in Figure 1.

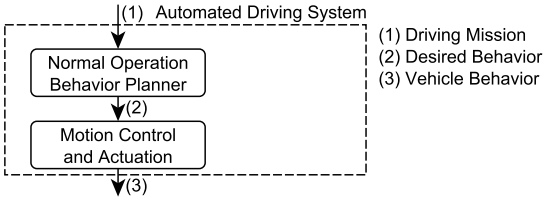

Figure 1: Definition of the ADS.

The input to the ADS is a desired driving mission. The normal operation behavior planner contains all functional submodules of sensing and planning that are required for the automated driving task. This includes the submodules for collection and interpretation of environmental sensor data, the localization and dynamic state estimation of the ego-vehicle, the prediction of future object behavior and the desired behavior planning. The result is the desired vehicle behavior, which is expressed as a desired trajectory. It contains information about desired poses and dynamics of the ego-vehicle for the upcoming time. The result from the motion control and actuation is the real vehicle behavior.

Due to a variety of possible combinations of the functions of an automated vehicle, different ADS configurations are conceivable. Some of the functions can be AI-assisted

and different strategies for environment interpretation or desired behavior planning can be pursued. However, end-to-end learning is excluded by this ADS architecture. Otherwise, an intervening safety function can not be integrated.

Behavior Safety Framework (BSF)
The BSF extends this basic ADS by adding safeguarding functions. In order not to reduce the solution space in advance, we do not define specific interfaces of interaction between the BSF and the other modules in Figure 1 for now.

Safe State
For the definition of the safe state, we use the definition from ISO/TR 4804 [16]: A safe state is an “operating mode that is reasonably safe”.

Safety of Desired Behavior
Regarding the desired behavior of the automated vehicle, the terms 'safety' and 'unsafety' need to be defined. Blokland and Reniers [18] do not directly refer to automated vehicles but in general to industrial safety and state that there is actually "no commonly agreed upon definition of 'safety' nor of its opposite 'unsafety'. Today, safety is mostly defined by an absence of accidents". According to this, situations with near misses are still considered to be safe and furthermore, a situation can only be classified as safe or unsafe retrospectively. Since we have to evaluate a priori whether the desired behavior is safe, we cannot use this definition. A dictionary definition of unsafety is the "exposure to danger or risk" [19]. Junietz [20] defines it in a similar, but more detailed way in the context of automated driving: a system is in an unsafe state, if "the corresponding risk is not accepted" . For the following considerations, we use the definition of Junietz.

4.2 Requirements

In this chapter, we define requirements for our BSF to safeguard the desired behavior of an automated vehicle. The task of this framework is to maintain the safe state of an automated vehicle, even with unsafe desired behavior. This shall not be performed by our BSF verifying the algorithms of the ADS, but by verifying the result of the ADS. This result is the planned desired behavior, usually defined as desired trajectory. Additionally, an appropriate risk-minimizing reaction shall be triggered in the event of detected unsafe desired behavior.

The BSF is comparable to a horse in a carriage team. The coachman leads the horse with the harness to a desired behavior. So in most cases the coachman influences the behavior of the horse. However, if a coachman leads a horse into a roadside ditch, the horse will reject this desired behavior and stop the carriage before the roadside ditch to avoid being injured. In this case, we cannot claim that the horse verifies the planning of the coachman, but only the result of the planning. In the same way, we do not presume to verify the algorithms of an ADS, but to verify that the automated vehicle does not pose an unreasonable risk.

The first requirement describes this basic functionality, from which further requirements are derived. We use the definition for the minimal risk condition as described in ISO/TR 4804 [16] and ISO/DIS 21448 [17].

Requirement 1 *The BSF shall transition the ego vehicle to a minimal risk condition in case of an identified unsafety of the desired behavior.*

Thus, the BSF shall perform an emergency maneuver to maintain the safe state of the automated vehicle. To avoid collisions with obstacles during the emergency stop maneuver, the BSF shall have the capability to perceive and interpret the relevant vehicle environment.

As addressed in Requirement 1, in case of detected unsafe states, the task of the safety framework is to achieve a minimal risk condition or to reduce the hazard and risk to an acceptable level by appropriate intervention in the vehicle behavior. For this, it is also crucial that unsafe states are identified fast enough.

Requirement 2 *The BSF shall detect unsafeties in the desired behavior and generate a suitable intervention fast enough to reduce the risk to an acceptable level.*

The detection of those unsafeties in the desired behavior includes on the one hand to be aware of whether the capabilities of the ADS-modules are sufficient to plan a safe desired behavior. This can involve the collection and interpretation of environmental sensor data, the localization and dynamic state estimation of the ego-vehicle, the prediction of future object behavior and the desired behavior planning. On the other hand, potential accidents with static or dynamic objects caused by performing the desired behavior shall also be detected.

Requirement 3 *The BSF shall be aware of whether the current capabilities of the vehicle are sufficient for safe vehicle operation.*

Requirement 4 *The BSF shall detect whether performing the desired behavior would lead to an accident.*

The safety framework shall be able to actively influence the vehicle behavior. Therefore it shall be able to set interface-compliant commands to the corresponding actuators for longitudinal and lateral vehicle movement. This can be done either directly by actuator commands or indirectly by sending the desired emergency behavior to the motion controller.

Requirement 5 *The BSF shall have direct or indirect access to the relevant actuators of the vehicle.*

In case of functional deficiencies of the BSF itself, the safety of the vehicle cannot be ensured anymore. Thus, they also need to be detected.

Requirement 6 *The capabilities of the BSF shall be monitored online.*

As a part of the ADS, the BSF is critical for the safety of the vehicle behavior. The safety framework shall therefore fulfill high safety requirements. To ensure this, the dedicated functionality must be verifiable, which corresponds to the seventh requirement.

Requirement 7 *The safety and functionality of the BSF shall be testable and verifiable.*

4.3 Functional Architecture

Figure 2 illustrates the generic functional architecture of the BSF. The desired behavior planned by the normal operation behavior planner is the input of the BSF. The BSF has five functional submodules: the ADS health state data reception, the environment perception data reception, the interpretation of the relevant environment, the emergency behavior generation and the safe behavior selection.

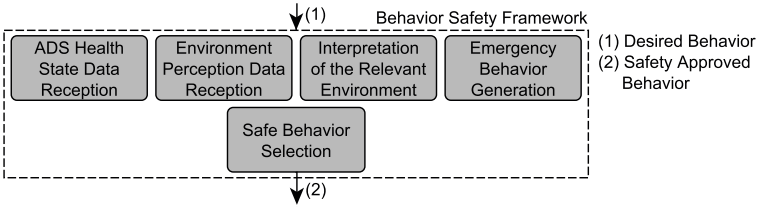

Figure 2: Generic functional architecture of the BSF.

The lefthand submodule in Figure 2 receives information about the capabilities of the automated driving system based on the status and health data of the ADS submodules. These capabilities enable an evaluation of the safety of the desired behavior. The environment perception and the environment interpretation functions are required for two tasks. On the one hand, they need to verify whether the desired behavior is safely compatible with the environment or whether e.g. collisions may occur. On the other hand, depending on the kind of emergency strategy, they might be required for planning a safe emergency behavior, which is done by the righthand submodule in Figure 2. The last one is the safe behavior selection, which chooses either the originally planned desired behavior or the emergency behavior to be sent to the motion controller or directly to the relevant actuators of the vehicle. This decision is based on the results of the other submodules and thus always leads to a safety approved behavior output of BSF. The presented architecture only specifies the required functions represented by submodules. In order to keep the BSF generic, we do not define data flow or interfaces between them.

5 Evaluation and Discussion

We developed our architecture of a BSF based on the requirements given in Section 4.2. For verification we apply two approaches. In Subsection 5.1, we formally compare the capabilities of our generic architecture with the specified requirements. In Subsection 5.2, we use two different ADS configurations for verification. Once again, we compare the requirements presented in Section 4.2 with the capabilities of these ADS configurations.

5.1 Formal Verification

For formal verification, the capabilities of the generic architecture of our BSF are compared to the requirements. Our architecture includes the emergency behavior generation submodule. This module generates the emergency behavior to maintain the safe state of the automated vehicle. Thus, our architecture satisfies Requirement 1. Requirement 2

requires a sufficiently fast safety response of the BSF in case of unsafe desired behavior. A formal verification of this requirement is not possible, since it is dependent on the specific implementation of the BSF. It will be verified in practical testing.

To monitor the health of the ADS, our architecture provides the ADS health state monitoring submodule. This submodule is used to determine the capabilities of the vehicle and compare them with the requirements for the driving mission. Requirement 3 is therefore fulfilled. We also added the submodules for environment perception data reception and interpretation of the relevant environment to satisfy Requirement 4.

Our modular architecture of the BSF allows a functional separation of the submodules, so that the desired behavior of different ADS configurations can be monitored with our framework. Defined interfaces to the relevant vehicle actuators enable sending commands corresponding to the desired behavior and thus, Requirement 5 is fulfilled. All submodules of the BSF determine their own health status, so that the health status of the BSF can be aggregated. As a result, our generic architecture also fulfills Requirement 6. The modularity of the BSF enables individual testability of the submodules. The functional separation between the normal operation behavior planner and our BSF allows the BSF to be tested independently of the ADS. Our BSF thus also meets Requirement 7.

5.2 Application

To demonstrate the technical implementation of the BSF, we introduce two examples. Section 5.2.1 illustrates the example of trajectory monitoring in the context of an AI-driven ADS. As another example, we use a fallback system for an automated vehicle in Section 5.2.2. Both systems are used in an automated vehicle equipped with an ADS that is designed for level 4 according to SAE J3016, as presented in Section 4.1.

5.2.1 Safety Check Module for Monitoring AI Planned Trajectories

The so called Safety Check (SC) module is developed in the scope of the project PRORETA 5 [21]. As Nascimento et al. [22] point out in their study, besides their great potential in various fields of automated driving, AI-approaches also pose risks regarding safety. Safeguarding the results of these AI algorithms and thus the vehicle behavior is the motivation of the SC concept. Consequently, the SC only uses conventional approaches without AI in order not to have the same AI-caused safety issues as the modules of the normal operation behavior planner. Since the considered ODD includes a speed limit of 30 km/h, braking to standstill is mostly preferable to evasion maneuvers in safety critical situations. Thus, the approach to reach a minimal risk condition is to decelerate to standstill along the path of the last safe trajectory. This emergency strategy does not require additional environmental sensors, so no extra hardware is needed for the SC concept.

In the ADS, the SC module is placed between the normal operation behavior planner and the motion controller. That means that the desired behavior of the normal operation behavior planner, which is represented by a desired trajectory, is first checked by the SC module before being sent to the motion controller if no unsafe condition is identified.

As shown in Figure 3, the SC module contains the submodules for environment verification & trajectory safety check and for the system health check. The SC has access to the same sensor data as all other modules in the ADS but uses diversitary approaches of interpreting them. It is also able to detect sensor degradations for environmental or

vehicle dynamic sensors. The safety of the desired trajectory is checked by verification of the environmental perception of the normal operation behavior planner and by looking for collision-critical objects in and around the driving corridor. The system health check submodule observes all functional modules in the ADS as well as all sensors that sense the environment or the dynamic behavior of the vehicle. If any of them fails, the state of the ADS is considered to be unsafe. Both submodules in the SC are sending out Boolean safety flags to the trajectory selection. Based on their values, the trajectory selector chooses either the desired trajectory from the normal operation behavior planner or an emergency trajectory instead, which is provided by the righthand submodule in Figure 3.

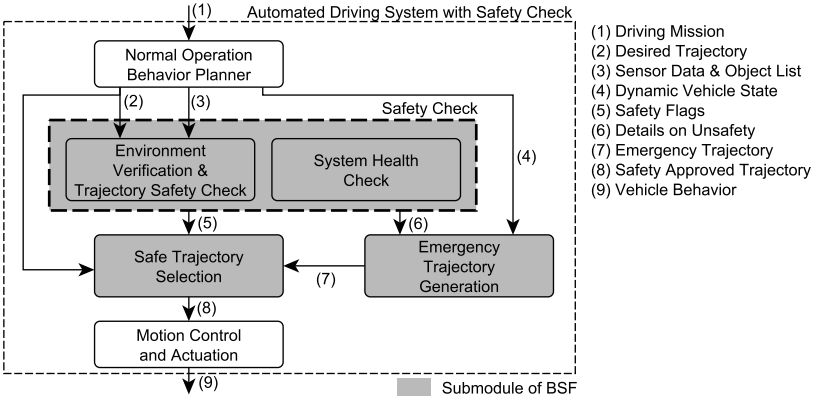

Figure 3: Functional sketch of the Safety Check module.

Comparing this application to the generic BSF, all of the submodules defined in Figure 2 are covered. The ADS health state data reception of the generic BSF corresponds to the system health check. The emergency behavior generation and the safe behavior selection correspond to the emergency trajectory generation and the safe trajectory selection, respectively. The environment perception of the generic BSF is not separately shown in Figure 3, because the perception system of the normal operation behavior planner is used. The environment interpretation of the generic BSF is implemented as an environment verification in the SC, as described above.

Regarding the requirements defined in Section 4.2, Requirements 1 and 3 are met by the ADS with SC. Degraded capabilities of the vehicle that are not sufficient for safe operation are identified by the submodules inside the safety check box in Figure 3. In case of unsafety, an emergency trajectory is immediately generated and sent to the motion controller to transition the vehicle to standstill. This also happens in case of collision-critical objects, that are detected by the environment verification and trajectory safety check. Requirement 4 is thus met. Since the environmental perception and interpretation is reduced to a verification task along the desired driving corridor and the emergency trajectory generation only adapts the speed profile along the path of the desired trajectory, computation time related issues are not expected. This satisfies Requirement 2.

The emergency trajectory uses the same format as the desired trajectory from the normal operation behavior planning, so the motion controller can process both kinds of

trajectories in the same way. Therefore, indirect access to the relevant vehicle actuators is given and the ADS with SC also meets Requirement 5. In case of SC breakdown, the safe trajectory selection gets no information about the safety of the desired trajectory and thus does not forward any trajectory to the motion control. If the motion control has to wait too long for a new trajectory, it initiates an emergency stop by itself and thereby covers Requirement 6. However, this is not supposed to happen due to reliable design of the SC module. The ADS with the SC is designed in a modular way using clearly defined interfaces. This enables testing individual modules and thus fulfills Requirement 7.

The presented SC architecture is easy to be implemented and promising for driving at low speed. For higher velocities, the simple emergency strategy of the SC concept is not reasonable anymore. Then, the planning of collision-free emergency paths to standstill that differ from the originally planned path is more important. A safety concept that also considers higher velocities than the SC module is presented in the following section.

5.2.2 Emergency Stop System Safe Halt

For a second application, we use the emergency stopping system Safe Halt for an automated vehicle [15]. The functional architecture is presented in Figure 4. This emergency stop system is engaged when the capabilities of the automated vehicle are no longer sufficient for the safe performance of its driving mission. The emergency stop system provides a minimal risk maneuver that leads the automated vehicle to the minimal risk condition. The minimal risk maneuver is monitored for collision objects by means of an independent environment perception system.

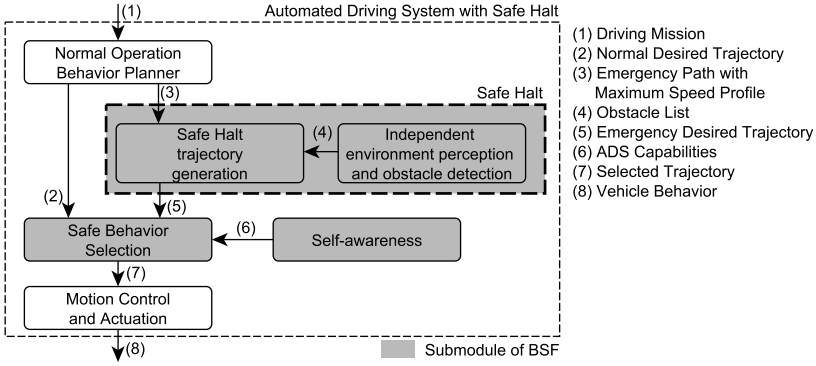

Figure 4: Functional sketch of the ADS with *Safe Halt* emergency stop application.

This ADS configuration includes all submodules of the generic BSF that we presented in Chapter 4. If the capabilities of this ADS with Safe Halt are compared with the requirements in Section 4.2, this ADS configuration meets Requirement 1, because the emergency stop system with the independent environment perception is able to transition the vehicle to a minimal risk condition even with severe degradation of the normal operation behavior planner.

The demonstrated ADS configuration with Safe Halt meets Requirement 2 in a prototype implementation. By providing the normal desired trajectory and the emergency

trajectory in parallel, switching between both in the behavior selection is performed with minimal latency. The aggregation of the vehicle capabilities and the comparison with the requirements for the driving mission is also performed sufficiently fast in a prototypical implementation to enable a suitable desired behavior response.

Requirement 3 is satisfied by self-awareness determining vehicle capabilities and comparing them to driving mission requirements. If these capabilities are not sufficient for the driving mission, the behavior selection switches from the normal desired trajectory to the emergency trajectory and the vehicle performs an emergency stop behavior. The Safe Halt functionality provides collision free trajectories based on the separated environment perception. The system therefore fulfills Requirement 4.

The modular architecture of Safe Halt is integrated into the generic ADS architecture in an interface-compliant manner. The interfaces between the normal operation behavior planner, the safe behavior selector and the Safe Halt emergency stop are defined. This definition allows motion control and actuation to be used for the emergency stop maneuver as well. The presented ADS configuration thus fulfills Requirement 5.

The emergency stop system Safe Halt reports its health status to the ADS self-awareness. The system therefore also meets Requirement 6. Due to the modular architecture of Safe Halt, the modules are testable separately. The system thus also fulfills requirement 7.

Overall, this example shows that the generic architecture of the BSF can also be inserted into this ADS configuration and still meet all the requirements for a BSF. The architecture of the BSF enables the safeguarding of the desired behavior of automated vehicles even in the case of complete failures of the normal operation behavior planner.

6 Conclusion

In this paper, we present a generic architecture for a BSF for an automated vehicle with a level 4 ADS according to SAE J3016. We demonstrate the application of the architecture in two different ADS configurations. The verification of these applications indicate that the presented architecture is also valid for other ADS configurations. Our generic architecture of a BSF can be used to safeguard complex, possibly AI-supported, desired behavior planners as well as emergency stop systems to transition an automated vehicle to a minimal risk condition when needed. We see a further need for research in the reliable determination of vehicle capabilities in order to identify unsafe trajectories by an ADS internal evaluation. Our future work aims at verification and validation of the presented architecture. This will be done by experimental tests using silent testing methods in the automated vehicle under real conditions.

Acknowledgments

We kindly thank Continental AG for their great cooperation within PRORETA 5, a joint research project of TU Darmstadt, University of Bremen, TU Iaşi and Continental.This research is also accomplished within the project “UNICARagil” (FKZ 16EMO0286). We acknowledge the financial support for the project by the Federal Ministry of Education and Research of Germany (BMBF).

References

[1] National Transportation Safety Board, "Collision Between a Car Operating With Automated Vehicle Control Systems and a Tractor-Semitrailer Truck Near Williston, Florida, May 7, 2016.," Highway Accident Report NTSB HAR-17/02, National Transportation Safety Board, 2017.

[2] National Transportation Safety Board, "Collision Between Vehicle Controlled by Developmental Automated Driving System and Pedestrian, Tempe, Arizona, March 18, 2018," Highway Accident Report NTSB HAR-19/03, National Transportation Safety Board, 2019.

[3] Society of Automotive Engineers, "SAE J3016: Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems.," 2021.

[4] S. Shalev-Shwartz, S. Shammah, and A. Shashua, "On a Formal Model of Safe and Scalable Self-driving Cars," *arXiv:1708.06374 [cs, stat]*, Oct. 2018. arXiv: 1708.06374.

[5] D. Nistér, H.-L. Lee, J. Ng, and Y. Wang, "The Safety Force Field," white Paper, Nvidia, 2019.

[6] R. De Iaco, S. L. Smith, and K. Czarnecki, "Universally Safe Swerve Manoeuvres for Autonomous Driving," *arXiv:2001.11159 [cs]*, Jan. 2020. arXiv: 2001.11159.

[7] C. B. S. T. Molina, J. R. d. Almeida, L. F. Vismari, R. I. R. González, J. K. Naufal, and J. Camargo, "Assuring Fully Autonomous Vehicles Safety by Design: The Autonomous Vehicle Control (AVC) Module Strategy," in *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, pp. 16–21, June 2017. ISSN: 2325-6664.

[8] T. Stolte, A. Reschka, G. Bagschik, and M. Maurer, "Towards Automated Driving: Unmanned Protective Vehicle for Highway Hard Shoulder Road Works," in *2015 IEEE 18th International Conference on Intelligent Transportation Systems*, (Gran Canaria, Spain), pp. 672–677, IEEE, Sept. 2015.

[9] C. Pek, S. Manzinger, M. Koschi, and M. Althoff, "Using online verification to prevent autonomous vehicles from causing accidents," *Nature Machine Intelligence*, vol. 2, pp. 518–528, Sept. 2020.

[10] T. Stahl, M. Eicher, J. Betz, and F. Diermeyer, "Online Verification Concept for Autonomous Vehicles – Illustrative Study for a Trajectory Planning Module," in *2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC)*, p. 7, 2020.

[11] J. Funke, M. Brown, S. M. Erlien, and J. C. Gerdes, "Collision Avoidance and Stabilization for Autonomous Vehicles in Emergency Scenarios," *IEEE Transactions on Control Systems Technology*, vol. 25, pp. 1204–1216, July 2017.

[12] J. Hilgert, K. Hirsch, T. Bertram, and M. Hiller, "Emergency path planning for autonomous vehicles using elastic band theory," in *Proceedings 2003 IEEE/ASME International Conference on Advanced Intelligent Mechatronics (AIM 2003)*, vol. 2, (Kobe, Japan), pp. 1390–1395, IEEE, 2003.

[13] A. Mehmed, M. Antlanger, W. Steiner, and S. Punnekkat, "Forecast Horizon for Automated Safety Actions in Automated Driving Systems," in *Computer Safety, Reliability, and Security* (A. Romanovsky, E. Troubitsyna, and F. Bitsch, eds.), vol. 11698, pp. 113–127, Cham: Springer International Publishing, 2019. Series Title: Lecture Notes in Computer Science.

[14] A. Reschka, *Fertigkeiten-und Fähigkeitengraphen als Grundlage des sicheren Betriebs von automatisierten Fahrzeugen im öffentlichen Straßenverkehr in städtischer Umgebung*. PhD Thesis, Technische Universität Braunschweig, Braunschweig, 2017.

[15] S. Ackermann and H. Winner, "Systemarchitektur und Fahrmanöver zum sicheren Anhalten modularer automatisierter Fahrzeuge.," in *13. Workshop Fahrerassistenzsysteme und automatisiertes Fahren*, (Walting), 2020.

[16] ISO, "ISO/TR 4804:2020 - Road vehicles — Safety and cybersecurity for automated driving systems — Design, verification and validation," 2020.

[17] ISO, "ISO/PAS 21448 -Road vehicles - Safety of the intended functionality," 2019.

[18] P. Blokland and G. Reniers, "Measuring (un)safety. A broad understanding and definition of safety, allowing for instant measuring of unsafety," *Chemical Engineering Transactions*, vol. 77, pp. 253–258, Sept. 2019.

[19] Dictionary.com, "Definition of unsafety." `https://www.dictionary.com/browse/unsafety`, Sept. 2021.

[20] P. Junietz, *Microscopic and Macroscopic Risk Metrics for the Safety Validation of Automated Driving*. PhD Thesis, Technische Universität Darmstadt, Darmstadt, 2019.

[21] TU Darmstadt, "PRORETA 5," 2021. `https://www.proreta.tu-darmstadt.de/proreta/index.en.jsp`, visited 2021-11-05.

[22] A. M. Nascimento, L. F. Vismari, C. B. S. T. Molina, P. S. Cugnasca, J. B. Camargo, J. R. d. Almeida, R. Inam, E. Fersman, M. V. Marquezini, and A. Y. Hata, "A Systematic Literature Review About the Impact of Artificial Intelligence on Autonomous Vehicle Safety," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 12, pp. 4928–4946, 2020.