2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)
Windsor Oceanico Hotel, Rio de Janeiro, Brazil, November 1-4, 2016

Safety Goals and Functional Safety Requirements for Actuation Systems of Automated Vehicles*

Torben Stolte[1], Gerrit Bagschik[1], and Markus Maurer[1]

***Abstract*— Increasing automation of vehicle guidance is one of the major trends in the automotive industry. Some auto makers have announced that automated vehicles will be deployed in public traffic by the end of this decade (level 4 in sense of the definition of SAE, level 5 later). Until then, one central challenge is ensuring functional safety of automated vehicles. Still, it is not clear how safety concepts for automated vehicles can be designed appropriately. This affects all parts of vehicle automation systems: environment perception, decision making, and actuation. In this contribution we derive safety goals and functional safety requirements according to ISO 26262 for actuation systems of automated vehicles systematically, following a systems theory based approach. The findings summarize elaborate measures to be implemented in actuation systems of automated vehicles when operated without human supervision.**

I. Introduction

One of the major trends in the automotive industry is increasing automation of vehicle guidance. Still, the challenge exists to ensure and substantiate safety of vehicles operating without human supervisor corresponding to SAE levels 3 (until handing over to the driver), 4, and 5 [12]. On the one hand, it is not clear how systems operating in open environments with a non-quantifiable set of operational scenarios can be validated [16]. On the other hand, system designs must be found which enable the safe operation of automated vehicles in open environments.

According to recent statements from industrial contributors in the field of vehicle automation, the first highly automated vehicles will be introduced into the market by the end of this decade. Yet, safety concepts and corresponding safety requirements of automated vehicles are only partially discussed in the ITS community. In our understanding, this is crucial before deploying automated vehicles in public traffic.

In order to promote discussions about safety concepts of automated vehicles, we present *safety goals*[2] and *functional safety requirements*[2] for vehicle actuation systems in this contribution. As depicted in Fig. 1, we understand vehicle actuation systems as comprising all components required for moving an automated vehicle along a trajectory generated by a vehicle automation controller. This includes actuators such as steering, brakes, and drives, but also superimposed control loops controlling wheel rotational dynamics and overall vehicle dynamics in terms of trajectory follow control.

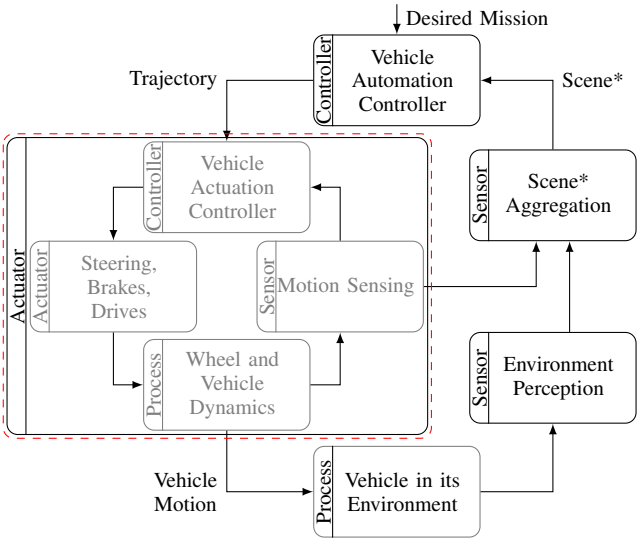

Fig. 1. Vehicle actuation system (dashed) as actuator in a generic control loop of a vehicle automation system; *For definition cf. [15]

In Section II of this paper, related work regarding safety goals and functional safety requirements of automated vehicles is presented. Section III contains a description of a systematic top-down approach for deriving safety goals and functional safety requirements based on systems theory. This analysis' main results are given in Section IV followed by an evaluation in Section V, while detailed tables with all identified safety goals and functional safety requirements can be found in the Appendix.

II. Related Work

In a previous paper, we demonstrated that vehicle actuation systems must be considered for ensuring functional safety of automated vehicles [14]. Yet, few publications are known to us which address functional safety of vehicle actuation systems of automated vehicles. Due to the absence of a human driver, supervision and failure correction must be implemented in electronic systems. For this, aspects such as actuator topology, necessary degree of redundancy, suspension kinematics, as well as designs of controllers must be considered.

As actuators are completely controlled by electronic systems, actuation in the context of automated driving is

*Our research is partially funded by the German Federal Ministry of Economics and Technology (BMWi) within the scope of the project *aFAS* [13].

[1]Torben Stolte, Gerrit Bagschik, and Markus Maurer are with the Institute of Control Engineering at Technische Universität Braunschweig, 38106 Braunschweig, Germany. {stolte,bagschik,maurer}@ifr.ing.tu-bs.de

[2]Terms according to ISO 26262 [4, Part 1]. *Safety goals* are top-level safety requirements, which are further detailed by functional and technical safety requirements. *Functional safety requirements* specify system behavior and measures required for functional safety without respecting technical implementations. In contrast, *technical safety requirements* describe technical implementations required for safety.

strongly linked to automotive by-wire systems such as steer-by-wire or brake-by-wire. Several publications address safety aspects connected to by-wire actuators. A comprehensive overview of publications regarding functional safety of by-wire systems in the automotive domain is given by Bergmiller [2]. Aspects such as redundancy regarding the structure of electronic control units, sensors, actuators, and power supply, as well as fault-tolerant and deterministic communication network topology is required to a certain extent. Additionally, Bergmiller extends these considerations towards a safety concept for the experimental vehicle MOBILE of Technische Universität Braunschweig. The vehicle features brake-by-wire, steer-by-wire, and throttle-by-wire at each wheel individually. Still, the vehicle is controlled by a human driver.

Although these contributions address many aspects that are potentially highly relevant for actuation systems of automated vehicles as well, they focus on human-controlled by-wire systems. In contrast, Hörwick presents a safety concept for partially automated vehicle system (SAE level 3) [3]. This system still requires a human driver as a fallback layer, yet Hörwick identified safety requirements which are potentially applicable to highly or fully automated vehicles (SAE levels 4 and 5). Among these, Hörwick lists safety requirements for vehicle actuation systems. He demands redundantly controllable brakes and redundant steering actuators. These are supported by generating yaw moment by differential braking in case of steering loss. Furthermore, inertial sensors and connected motion estimation are supposed to be designed redundantly.

Raste considers safety goals and safety requirements for a SAE level 3 system, too [9]. In line with our understanding, Raste sees trajectories as input to vehicle actuation systems. For vehicle actuation systems, he introduces redundancy structures consisting of two parallel paths. The first path executes the normal operation, while the second path is in hot-standby. The second path can take over control in case the first path malfunctions. Again, elements such as redundant design of controllers, actuators, sensors, as well as power supply are met. Additionally, Raste presents some safety goals regarding steering. These can be summed up by *unintended steering must be avoided* and *intended steering must be ensured.*

Reschka presents general deliberations regarding functional safety of automated vehicles [11]. Reschka also generally requires redundant design of sensors, actuators, and power supply for ensuring functional safety of automated vehicles which also applies to actuation systems. Beyond this, he argues in line with Bergmiller [2] that functional redundancies can be beneficial for ensuring functional safety. Utilization of functional redundancies is proposed by Kim [5], too.

Altogether, basic considerations regarding safety mechanisms of actuations systems in the context of automated driving have been discussed widely. However, no systematic derivation of safety goals and functional safety requirements has been performed yet.

III. Selected Approach

As the most recent standard available, the international standard ISO 26262 [4] must be applied with respect to ensuring functional safety of the functionality of automated vehicles. ISO 26262 requires determination of safety goals as part of hazard analysis and risk assessment and derivation of functional safety requirements which are performed during the concept phase of a development process [4, Part 3, 7.4.4 and 8.4.2]. In our previous paper [14], we utilized the *System-Theoretic Process Analysis* (STPA) in order to examine vehicle actuation systems systematically regarding malfunctional behavior which is a required input for a hazard analysis and risk assessment. Consistent with Raste [9] as well as Mallya [8], we utilize STPA again for determining safety goals and deriving functional safety requirements for actuation systems of automated vehicles systematically.

Leveson developed STPA as one of a growing set of methods subsumed as *System Theoretic Accident Model and Processes*[3] [6]. As STAMP/STPA is based on systems theory, safety relevant systems are modeled in terms of control loops. Within these control loops, STPA targets systematic identification of unsafe control actions and associated causes. STPA consists of three basic steps: Step 0 contains establishing fundamentals for subsequent steps, Step 1 identifies unsafe control actions, and Step 2 consists of an analysis of causes of the identified unsafe control actions. With these results, safety requirements can be derived on different levels of abstraction.

The fundamentals established in Step 0 comprise, among others, accident and hazard identification as well as modeling the considered system as hierarchical control structure. For example, in Fig. 1 the vehicle actuation system as actuator itself contains subordinate control loops.

For identifying unsafe control actions in *Step 1*, Leveson proposes four basic assumptions for control actions being unsafe [6, pp. 213]. These are:

- A control action required is not provided or is not followed.
- A control action is provided although not required.
- A potentially safe control action is provided too early, too late, at the wrong time, or in the wrong sequence.
- A control action required for safety is stopped too soon or applied too long.

Applying these assumptions on the control actions of a system yields a list of unsafe control actions. For each of the identified control actions, top-level safety requirements can be derived, namely safety goals in terms of ISO 26262.

Step 2 of STPA comprises a causal analysis. In general, Step 2 is the most challenging part of STPA because it requires more experience compared to Step 1 as less guidance is provided [7]. By examining not only control

[3]The terminology related to STAMP is strongly influenced by systems theory. Hence, Levenson utilizes the term *safety constraint* in place of *safety requirement*, cf. [7]. For better readability and due to not yet consistent terminology related to STAMP, we utilize terminology of ISO 26262 in this paper [4, Part 1].

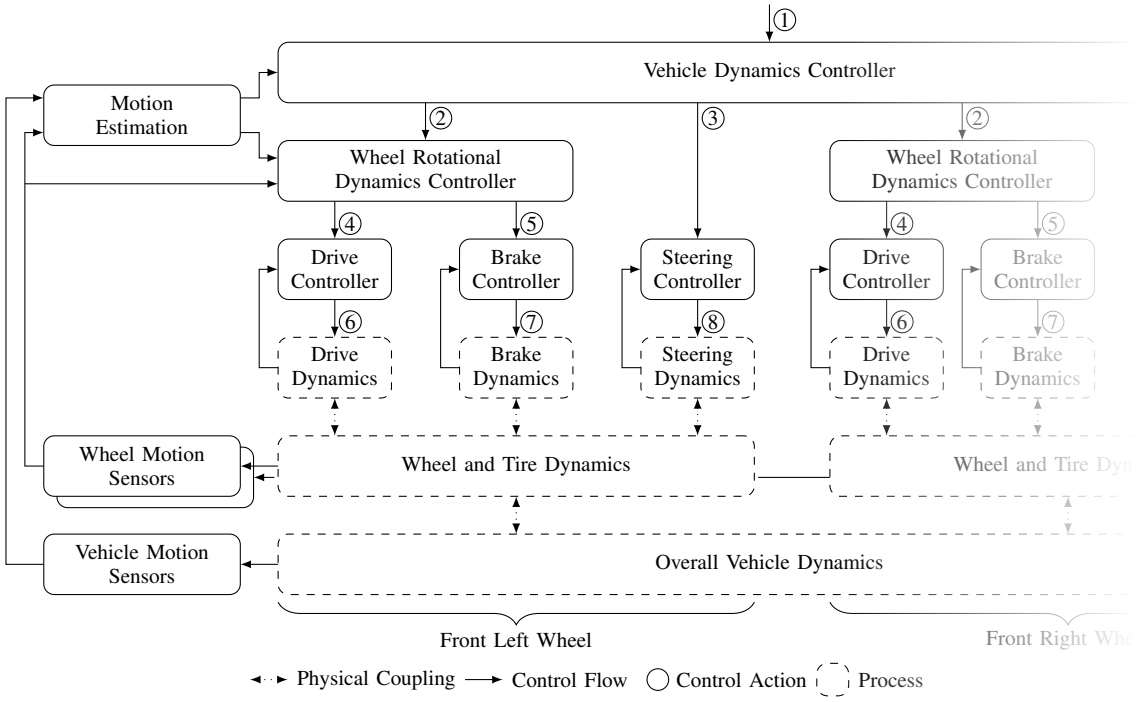

Fig. 2. Control structure of actuation systems of automated vehicles [14]

actions but all parts of the established control structure, potential causes for unsafe control actions are identified. Subsequently, these causes can be addressed in according functional safety requirements. Leveson provides guidance to users for applying Step 2 in the form of a reference control loop that demonstrates how each part can cause unsafe control actions [6, pp. 92]. Table I sums up potential causes taken from the reference control loop. However, Leveson also states that additional causes can exist.

IV. Analysis

Applying these three steps to actuation systems of automated vehicles yields the following findings.

A. Fundamentals

Regarding vehicle actuation systems, the fundamentals, which we identified in our previous paper [14], are adopted for the purpose of this contribution. As depicted in Fig. 1, a trajectory is the control input of vehicle actuation systems. Thus, the main functionality of vehicle actuation systems is trajectory follow control. Consequently, the related hazard is that the vehicle is not following its intended trajectory. This can potentially result in an accident by colliding with other traffic participants or stationary objects.

The derived control structure as central input for the following steps is given in Fig. 2. The structure is based on the actuator topology of the experimental vehicle MOBILE featuring all-wheel steering, all-wheel drive, and electromechanical brakes [2]. By summarizing or omitting actuators, the structure can be adopted to different actuator topologies. For instance, coupling two steered front wheels yields front axle steering or omitting front wheel drives yields rear axle drive. Yet, the identified control actions immanent to vehicle actuation systems remain the same.

Found control actions – listed in Table II – summarize the functionalities of vehicle actuation systems. At this point of the analysis, it is not clear how functionalities will be technically implemented later. Due to the top-down approach followed here, selected functionalities can be implemented accessing different parts of the control loop. For instance, either brakes or drives can be used for anti-spin control. Thus, some control actions are allocated to multiple control outputs. Furthermore, control outputs of vehicle actuation systems are normally quasi-continuous while control outputs considered in STAMP/STPA are usually discrete (e.g. ”open

TABLE I
Causal Factors for Control Actions Becoming Unsafe According to Leveson [6]

Component	Causal Factor
Controller	Inadequate control algorithm
	Process model inconsistent, incomplete, or incorrect
	Inappropriate, ineffective, or missing control action
Sensor	Inadequate or missing feedback
	Feedback delays
	Measurement inaccurancies
	Inadequate operation
Actuator	Inadequate operation
	Delayed operation
Process	Component Failure
	Conflicting Control Actions
	Changes over time
	Unidentified or out-of-range disturbances
	Process input missing or wrong

TABLE II
CONTROL ACTIONS OF THE CONTROL OUTPUTS DEPICTED IN FIG. 2

Control Output	Control Action
①	Set new target trajectory
②	Set new target wheel torque
③	Set new target steering angle
④	Change drive brake torque
④	Change target brake torque
④	Perform anti-lock control
④	Perform anti-spin control
⑤	Change target brake torque
⑤	Perform anti-lock control
⑤	Perform anti-spin control
⑥	Apply drive torque
⑦	Engage brake
⑧	Hold steering angle
⑧	Change steering angle

door"). To address this, we considered the control outputs from a functional perspective [14]. Consequently, some control outputs feature multiple control actions.

B. Determining Safety Goals

We already showed [14], that each identified control action possesses unsafe control actions regarding all four assumptions Leveson suggests for conducting STPA. Yet, as our previous contribution had a different scope, we did determine neither safety goals nor functional safety requirements. In order to determine safety goals, we considered each unsafe control action and defined a corresponding safety goal[4]. As the superordinate vehicle automation controller is out of scope of this paper, we assume it functioning as intended, which is in line with ISO 26262 [4, Part 3, 7.4.2.2.2]. Thus, the trajectory input ① is not considered. However, analyzing an entire automated vehicle would require this.

For a detailed list of considered unsafe control actions and defined safety goals see Table IV in the Appendix. Table III summarizes the determined safety goals. Each control action obtains two safety goals. For each control action, these two safety goals are structured similarly. On the one hand, the first safety goal demands that the control action must be executed when required for safe operation. On the other hand, this control action must *only* be executed when required for safe operation. We suppose the term *required* to contain logical as well as timing aspects.

C. Derivation of Functional Safety Requirements

Once safety goals are determined, functional safety requirements can be derived. For this, the control structure depicted in Fig. 2 was examined by means of the reference control loop and the related causal factors for unsafe control actions of Leveson [6, pp. 92]. Detailed results are displayed in Table V in the Appendix.

With reference to the basic components of a control loop – controller, actuator, sensor, and process – basic principles are recurrently applied. For sensors, it is required to compensate for missing feedback of single sensors. Simultaneously, cycle time and jitter must be within acceptable bounds. Furthermore, sensors must indicate their operational status, such that consuming components can evaluate whether the received signals are suitable for proper operation.

Processes refer to each system dynamic controlled by a controller. As a foundation for safety, we require state-of-the-art electrical and mechanical design. Still, changes of the process over time (wear, electrical/mechanical aging) and even failures can occur. Hence, an important part of the derived functional safety requirements is monitoring. Monitoring addresses not only electrical but also mechanical components of the processes and is accompanied by feeding back perceived process degradations to the superordinate controller. This also comprises out-of-range or unidentified disturbances (e.g. an implausible system state vector). For wheel rotational and overall vehicle dynamics, control actions can be conflicting, for example when at one wheel the brake is engaged while the drive applies a positive torque. Therefore, control actions applied to the same process must target the same process behavior.

As each controller serves as an actuator within a superimposed control loop, controllers and actuators are considered together. First of all, applied control algorithms must be capable of handling model uncertainties and disturbances. The underlying dynamics model must be sufficiently precise and the internal representation of the process state must comply with the physical process state. The latter also relates to the sensor requirements stated above. Furthermore, in-time actuation is required. Thus, appropriate execution time and execution jitter are required for executing control commands. Again, monitoring is required, here regarding proper functioning of the control algorithm as well as regarding

TABLE III
SAFETY GOALS FOR VEHICLE ACTUATION SYSTEMS OF AUTOMATED VEHICLES

ID	Safety Goal
SG01	VDC must set a new target wheel torque when required.
SG02	VDC must set a new target wheel torque only when required.
SG03	VDC must set a new target steering angle when required.
SG04	VDC must set a new target steering angle only when required.
SG05	WRDC must change target brake torque when required.
SG06	WRDC must change target brake torque only when required.
SG07	WRDC must change target drive torque when required.
SG08	WRDC must change target drive torque only when required.
SG09	Anti-lock control must be performed only when required.
SG10	Anti-lock control must be performed when required.
SG11	Anti-spin control must be performed only when required.
SG12	Anti-spin control must be performed when required.
SG13	Drive Controller must apply drive torque when required.
SG14	Drive Controller must apply drive torque only when required.
SG15	Brake Controller must engage brake when required.
SG16	Brake Controller must engage brake only when required.
SG17	SC must change steering angle when required.
SG18	SC must change steering angle only when required.
SG19	SC must hold steering angle when required.
SG20	SC must hold steering angle only when required.

VDC: Vehicle Dynamics Controller
WRDC: Wheel Rotational Dynamics Controller
SC: Steering Controller

[4]According to ISO 26262, an *Automotive Safety Integrity Level* (ASIL) must be assigned to each safety goal. However, this is strongly dependent on specific functionalities of vehicle automation systems and related operational scenarios. This goes beyond the scope of this contribution.

the operational state of controller and controlled process. Last but not least, controllers need to be designed fail-operational. Fail-operational requirements can be mitigated to fail-safe requirements, presumed it can be proven that failures can be compensated for in any case by utilizing functionally redundant actuation. Yet, this strongly depends on an automated vehicle's actuator topology and the maximal capabilities of its actuators.

Common to all parts of the control system, continuous and sufficient power supply is required in order to ensure proper functionality.

V. Evaluation

Due to missing or inaccessible similar analyses, it is hard to validate whether the safety goals and functional safety requirements found are, on the one hand, complete and, on the other hand, appropriate to serve as top-level safety requirements for actuation systems of automated vehicles.

Regarding the determination of safety goals, partial results presented by Raste [9] indicate that at least the double consideration of each control action is suitable. Furthermore, preliminary results of a hazard analysis and risk assessment conducted within the project *aFAS*[5] also show similar results to some extent [1]. For instance, two safety goals are assigned regarding braking: 1. Brake actuation must be ensured when actuation is required. 2. Undesired braking must be avoided. In contrast, for steering, only avoiding of undesired actuation is demanded. Due to low velocities during automated operation, the vehicle can be stopped in case no steering request is executed. For automated vehicles with a more comprehensive functional range as considered in this paper, i.a. higher velocities, this is not a suitable solution.

Just as for safety goals, no direct comparison for derived functional safety requirements is available. Generally, the functional safety requirements we derived reutilize principles and mechanisms quoted in Section II. As human drivers are completely out of the loop, all tasks related to driving must be executed by electronic systems. This includes continuous evaluation of the actual capabilities of the vehicle in sense of a self-representation as – among others – recently discussed by Bergmiller for by-wire actuation [2] or Reschka et al. for automated driving [10]. This is already addressed in the functional safety requirements derived in this paper. For instance, unusual noise originating from suspensions can refer to a loose mechanical linkage. Yet, it is not clear whether all measures presented are sufficient or – in contrast – are at least partially too excessive. Consequently, the functional safety requirements generically derived in this paper must be challenged in reference to suitability.

[5]Automatisch fahrerlos fahrendes Absicherungsfahrzeug für Arbeitsstellen auf Autobahnen (German: Automated Unmanned Protective Vehicle for Highway Hard Shoulder Road Works). Within the project, the consortium targets developing an unmanned protective vehicle for road works on German highway hard shoulders, cf. [13]. The vehicle will be operated without a safety driver and without supervision at low speeds up to 10 kph during public traffic on hard shoulders of German highways. Ensuring functional safety is one of the key aspects of the project.

VI. Conclusion

In this paper, we systematically determined safety goals and derived functional safety requirements for actuation systems of automated vehicles. The findings imply, that measures must be adopted which go beyond state-of-the-art of recent production vehicles for ensuring functional safety of automated vehicles. Despite high importance for series deployment of automated vehicles, safety requirements are hardly discussed within the ITS community. Hence, we would like to put these findings forward to discussion.

ACKNOWLEDGMENT

We would like to thank our project partners from the *aFAS* consortium and our colleagues for their support of our work.

References

[1] aFAS Consortium, *Hazard Analysis and Risk Assessment of the Project aFAS*, T. Stolte, G. Bagschik, and A. Reschka, Eds., Apr. 2016, Version 00-00-10, unpublished preliminary project result.

[2] P. J. Bergmiller, "Towards Functional Safety in Drive-by-Wire Vehicles," Dissertation, Technische Universität Braunschweig, Braunschweig, Germany, 2015.

[3] M. Hörwick, "Sicherheitskonzept für hochautomatisierte Fahrerassistenzsysteme," Dissertation, Technische Universität München, Munich, Germany, 2011.

[4] ISO, "ISO 26262: Road vehicles - Functional Safety," International Organization for Standardization, Geneva, Switzerland, Standard ISO 26262:2011, Nov. 2011.

[5] J. Kim, R. R. Rajkumar, and M. Jochim, "Towards dependable autonomous driving vehicles: a system-level approach," *ACM SIGBED Review*, vol. 10, no. 1, pp. 29–32, 2013.

[6] N. G. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety*. Cambridge, MA, USA: MIT Press, 2011.

[7] N. G. Leveson and J. Thomas, "An STPA Primer," 2013.

[8] A. Mallya, V. Pantelic, M. Adedjouma, M. Lawford, and A. Wassyng, "Using STPA in an ISO 26262 Compliant Process," in *Computer Safety, Reliability, and Security*, ser. Lecture Notes in Computer Science, A. Skavhaug, J. Guiochet, and F. Bitsch, Eds. Springer International Publishing, Sep. 2016, no. 9922, pp. 117–129.

[9] T. Raste, "Fallback Strategy for Automated Driving Using STPA," Amsterdam, The Netherlands, Oct. 2015.

[10] A. Reschka, G. Bagschik, S. Ulbrich, M. Nolte, and M. Maurer, "Ability and skill graphs for system modeling, online monitoring, and decision support for vehicle guidance systems," in *2015 IEEE Intelligent Vehicles Symposium (IV)*, Jun. 2015, pp. 933–939.

[11] A. Reschka, "Safety Concept for Autonomous Vehicles," in *Autonomous Driving*, M. Maurer, J. C. Gerdes, B. Lenz, and H. Winner, Eds. Berlin, Heidelberg, Germany: Springer Berlin Heidelberg, 2016, pp. 473–496.

[12] SAE, "Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems," Society of Automotive Engineers, Standard J3016, Jan. 2014.

[13] 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*, Sep. 2015, pp. 672–677.

[14] T. Stolte, R. S. Hosse, U. Becker, and M. Maurer, "On Functional Safety of Vehicle Actuation Systems in the Context of Automated Driving," in *Advances in Automotive Control 2016*, Norrköping, Sweden, Jun. 2016, pp. 586–591.

[15] S. Ulbrich, T. Menzel, A. Reschka, F. Schuldt, and M. Maurer, "Defining and Substantiating the Terms Scene, Situation, and Scenario for Automated Driving," in *2015 IEEE 18th International Conference on Intelligent Transportation Systems (ITSC)*, Sep. 2015, pp. 982–988.

[16] H. Winner, M. Graupner, and W. Wachenfeldt, "How to Address the Approval Trap for Autonomous Vehicles (Keynote)," in *2015 IEEE 18th International Conference on Intelligent Transportation Systems (ITSC)*, Sep. 2015.

APPENDIX

TABLE IV
UNSAFE CONTROL ACTIONS AND SAFETY GOALS OF ACTUATION SYSTEMS OF AUTOMATED VEHICLES

CA	Unsafe Control Action	Safety Goal	Index
②	A new target wheel torque is not set although required.	VDC must set a new target wheel torque when required.	SG01
②	A new target wheel torque is set although not required.	VDC must set a new target wheel torque only when required.	SG02
②	A new target wheel torque is set too late.	VDC must set a new target wheel torque when required.	SG01
②	A new target wheel torque is applied too long.	VDC must set a new target wheel torque when required.	SG01
②	A new target wheel torque is released too soon	VDC must set a new target wheel torque when required.	SG01
③	New target steering angle is not set although required.	VDC must set a new target steering angle when required.	SG03
③	A new target steering angle is set although not desired.	VDC must set a new target steering angle only when required.	SG04
③	A new target steering angle is set too late.	VDC must set a new target steering angle when required.	SG03
③	A new target steering angle is applied too long.	VDC must set a new target steering angle when required.	SG03
④⑤	Target brake torque is not changed although required.	WRDC must change target brake torque when required.	SG05
④⑤	Target brake torque is changed although not required.	WRDC must change target brake torque only when required.	SG06
④⑤	Target brake torque is changed too late.	WRDC must change target brake torque when required.	SG05
④⑤	Target brake torque is applied too long.	WRDC must change target brake torque when required.	SG05
⑤	Target drive torque is not changed although required.	WRDC must change target drive torque when required.	SG07
⑤	Target drive torque is changed although required.	WRDC must change target drive torque only when required.	SG08
⑤	Target drive torque is changed too late.	WRDC must change target drive torque when required.	SG07
⑤	Target drive torque is applied too long.	WRDC must change target drive torque when required.	SG07
④⑤	Anti-lock control is performed although not required.	Anti-lock control must be performed only when required.	SG09
④⑤	Anti-lock control is not performed although required.	Anti-lock control must be performed when required.	SG10
④⑤	Anti-lock control is performed too late.	Anti-lock control must be performed when required.	SG10
④⑤	Anti-lock control is performed too soon.	Anti-lock control must be performed only when required.	SG09
④⑤	Anti-spin control is performed although not required.	Anti-spin control must be performed only when required.	SG11
④⑤	Anti-spin control is not performed although required.	Anti-spin control must be performed when required.	SG12
④⑤	Anti-spin control is performed too late.	Anti-spin control must be performed when required.	SG12
④⑤	Anti-spin control is performed too soon.	Anti-spin control must be performed only when required.	SG11
⑥	Drive torque is not applied although required.	Drive Controller must apply drive torque when required.	SG13
⑥	Drive torque is applied although not required.	Drive Controller must apply drive torque only when required.	SG14
⑥	Drive torque is applied too late.	Drive Controller must apply drive torque when required.	SG13
⑥	Drive torque is applied too long.	Drive Controller must apply drive torque only when required.	SG14
⑦	Brake torque is not applied although required.	Brake Controller must engage brake when required.	SG15
⑦	Brake torque is applied although not required.	Brake Controller must engage brake only when required.	SG16
⑦	Brake torque is applied too late.	Brake Controller must engage brake when required.	SG15
⑦	Brake torque is applied too long.	Brake Controller must engage brake only when required.	SG16
⑧	Steering angle is not changed although required.	SC must change steering angle when required.	SG17
⑧	Steering angle is changed although it is required not to change.	SC must change steering angle only when required.	SG18
⑧	Steering angle changes too late.	SC must change steering angle when required.	SG17
⑧	Steering angle is changed too long.	SC must hold steering angle when required.	SG19
⑧	Steering angle is not held although required.	SC must hold steering angle when required.	SG19
⑧	Steering angle is held although it is required to change.	SC must hold steering angle only when required.	SG20
⑧	Steering angle is held too late.	SC must hold steering angle when required.	SG19
⑧	Steering angle is held too long.	SC must change steering angle when required.	SG17

CA: Control Action (cf. Fig. 2), VDC: Vehicle Dynamics Controller, WRDC: Wheel Rotational Dynamics Controller, SC: Steering Controller

TABLE V
FUNCTIONAL SAFETY REQUIREMENTS FOR ACTUATION SYSTEMS OF AUTOMATED VEHICLES

Component	Type	Causal Factor	Functional Safety Requirement
Drive-internal Sensors	Sensor	Inadequate or missing feedback	Inadequate or missing feedback must be recognized and compensated for.
		—"—	Continuous and sufficient power supply for drive-internal sensors.
		Feedback delays	Updated feedback must be available in required cycle time and jitter.
		Measurement inaccuracies	Sufficient measurement accuracy for drive operation must be ensured.
		Inadequate operation	Monitoring of operational state of drive-internal sensors and report to controller.
Brake-internal Sensors	Sensor	Inadequate or missing feedback	Inadequate or missing feedback must be recognized and compensated for.
		—"—	Continuous and sufficient power supply for brake-internal sensors.
		Feedback delays	Updated feedback must be available in required cycle time and jitter.
		Measurement inaccuracies	Sufficient measurement accuracy for drive operation must be ensured.
		Inadequate operation	Monitoring of operational state of drive-internal sensors and report to controller.

Continued on next page

Table V: Continued from previous page

Component	Type	Causal Factor	Functional Safety Requirement
Steering-internal Sensors	Sensor	Inadequate or missing feedback	Inadequate or missing feedback must be recognized and compensated for.
		——"——	Continuous and sufficient power supply for steering-internal sensors.
		Feedback delays	Updated feedback must be available in required cycle time and jitter.
		Measurement inaccuracies	Sufficient measurement accuracy for drive operation must be ensured.
		Inadequate operation	Monitoring of operational state of drive-internal sensors and report to controller.
Wheel Motion Sensors	Sensor	Inadequate or missing feedback	Inadequate or missing feedback must be recognized and compensated for.
		——"——	Continuous and sufficient power supply for wheel motion sensors.
		Feedback delays	Updated feedback must be available in required cycle time and jitter.
		Measurement inaccuracies	Sufficient measurement accuracy for drive operation must be ensured.
		Inadequate operation	Monitoring of operational state of drive-internal sensors and report to controller.
Vehicle Motion Sensors	Sensor	Inadequate or missing feedback	Inadequate or missing feedback must be recognized and compensated for.
		——"——	Continuous and sufficient power supply for vehicle motion sensors.
		Feedback delays	Updated feedback must be available in required cycle time and jitter.
		Measurement inaccuracies	Sufficient measurement accuracy for drive operation must be ensured.
		Inadequate operation	Monitoring of operational state of drive-internal sensors and report to controller.
Motion Estimation	Sensor	Inadequate or missing feedback	Inadequate or missing feedback must be recognized.
		——"——	Continuous and sufficient power supply for motion estimation.
		Feedback delays	Updated feedback must be available in required cycle time and jitter.
		Measurement inaccuracies	Sufficient measurement accuracy for wheel rotational dynamics control and vehicle dynamics control must be ensured.
		Inadequate operation	Monitoring of operational state of drive-internal sensors and report to controller.
Brake Dynamics	Process	Component failure	Electrical and mechanical design according to state of the art.
		——"——	Monitoring of electrical and mechanical components and report to superordinate controller.
		Conflicting control actions	Does not apply, only one controller.
		Changes over time	Monitoring of electrical and mechanical components and report to superordinate controller.
		Unidentified or out-of-range disturbances	Brake controller must recognize brakes operating beyond design limits and react appropriately (e.g. failure state).
		Process input missing or wrong	Continuous and sufficient power supply for brake.
Drive Dynamics	Process	Component failure	Electrical and mechanical design according to state of the art.
		——"——	Monitoring of electrical and mechanical components and report to superordinate controller.
		Conflicting control actions	Does not apply, only one controller.
		Changes over time	Monitoring of electrical and mechanical components and report to superordinate controller.
		Unidentified or out-of-range disturbances	Drive controller must recognize drive operating beyond design limits and react appropriately (e.g. failure state).
		Process input missing or wrong	Continuous and sufficient power supply for drive.
Steering Dynamics	Process	Component failure	Electrical and mechanical design according to state of the art.
		——"——	Monitoring of electrical and mechanical components and report to superordinate controller.
		Conflicting control actions	Does not apply, only one controller.
		Changes over time	Monitoring of electrical and mechanical components and report to superordinate controller.
		Unidentified or out-of-range disturbances	Steering controller must recognize steering operating beyond design limits and react appropriately (e.g. failure state).
		Process input missing or wrong	Continuous and sufficient power supply for steering.
Wheel and Tire Dynamics	Process	Component failure	Design of suspension kinematics, wheel, and tires according to state of the art.
		——"——	Monitoring of suspension kinematics, wheel, and tire as well as report to superordinate controller.
		Conflicting control actions	Exclusion of drive and brake actuation with different.
		Changes over time	Monitoring of suspension kinematics, wheel, and tire as well as report to superordinate controller.
		Unidentified or out-of-range disturbances	Brake and drive controller must recognize wheel operating beyond design limits and react appropriately (e.g. failure state).
		Process input missing or wrong	Does not apply, no additional process input.
Overall Vehicle Dynamics	Process	Component failure	Considered with wheel and tire dynamics.
		Conflicting control actions	Control actions of the vehicle dynamics controller must target the same vehicle motion.
		Changes over time	Considered with wheel and tire dynamics.
		Unidentified or out-of-range disturbances	Vehicle dynamics controller must recognize vehicle dynamics operating beyond limits of handling and react appropriately.
		Process input missing or wrong	Does not apply, no additional process input.

Continued on next page

Table V: Continued from previous page

Component	Type	Causal Factor	Functional Safety Requirement
Steering Controller	Controller, Actuator	Inadequate control algorithm	Control algorithm robust against uncertainties of the steering dynamics model and disturbances.
		Process model inconsistent, incomplete, or incorrect	Sufficiently precise and validated steering dynamics model.
		—"—	Process variables must comply with the physical process state.
		Inappropriate, ineffective, or missing control action	Continuous and sufficient power supply for steering controller.
		—"—	Fail-operational design of steering controller.
		—"—	Monitoring of operational state of steering controller and process and report to superordinate controller.
		Inadequate operation	Fail-operational design of steering.
		Delayed operation	Operation of steering controller must be provided in required cycle time and jitter.
Brake Controller	Controller, Actuator	Inadequate control algorithm	Control algorithm robust against uncertainties of the brake dynamics model and disturbances.
		Process model inconsistent, incomplete, or incorrect	Sufficiently precise and validated brake dynamics model.
		—"—	Process variables must comply with the physical process state.
		Inappropriate, ineffective, or missing control action	Continuous and sufficient power supply for brake controller.
		—"—	Fail-operational design of brake controller.
		—"—	Monitoring of operational state of brake controller and process and report to superordinate controller.
		Inadequate operation	Fail-operational design of brake.
		Delayed operation	Operation of brake controller must be provided in required cycle time and jitter.
Drive Controller	Controller, Actuator	Inadequate control algorithm	Control algorithm robust against uncertainties of the drive dynamics model and disturbances.
		Process model inconsistent, incomplete, or incorrect	Sufficiently precise and validated drive dynamics model.
		—"—	Process variables must comply with the physical process state.
		Inappropriate, ineffective, or missing control action	Continuous and sufficient power supply for drive controller.
		—"—	Fail-operational design of drive controller.
		—"—	Monitoring of operational state of drive controller and process and report to superordinate controller.
		Inadequate operation	Fail-operational design of drive.
		Delayed operation	Operation of drive controller must be provided in required cycle time and jitter.
Wheel Rotational Dynamics Controller	Controller, Actuator	Inadequate control algorithm	Control algorithm robust against uncertainties of the wheel rotational dynamics model and disturbances.
		—"—	Fault-tolerant wheel rotational dynamics control algorithm.
		Process model inconsistent, incomplete, or incorrect	Sufficiently precise and validated wheel rotational dynamics model.
		—"—	Process variables must comply with the physical process state.
		Inappropriate, ineffective, or missing control action	Continuous and sufficient power supply for wheel rotational dynamics controller.
		—"—	Fail-operational design of wheel rotational dynamics controller.
		—"—	Monitoring of operational state of wheel rotational dynamics controller and process and report to superordinate controller.
		Inadequate operation	Covered by underlying control loops.
		Delayed operation	Operation of wheel rotational dynamics controller must be provided in required cycle time and jitter.
Vehicle Dynamics Controller	Controller, Actuator	Inadequate control algorithm	Control algorithm robust against uncertainties of the vehicle dynamics model and disturbances.
		—"—	Fault-tolerant vehicle dynamics control algorithm.
		Process model inconsistent, incomplete, or incorrect	Sufficiently precise and validated vehicle dynamics model.
		—"—	Process variables must comply with the physical process state.
		Inappropriate, ineffective, or missing control action	Continuous and sufficient power supply for vehicle dynamics controller.
		—"—	Fail-operational design of vehicle dynamics controller.
		—"—	Monitoring of operational state of vehicle dynamics controller and process and report to superordinate controller.
		Inadequate operation	Covered by underlying control loops.
		Delayed operation	Operation of vehicle dynamics controller must be provided in required cycle time and jitter.
Table concluded			