Hazard Analysis and Risk Assessment for an Automated Unmanned Protective Vehicle*

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

***Abstract*— For future application of automated vehicles in public traffic, ensuring functional safety is essential. In this context, a hazard analysis and risk assessment is an important input for designing functionally vehicle automation systems. In this contribution, we present a detailed hazard analysis and risk assessment (HARA) according to the ISO 26262 standard for a specific Level 4 application, namely an unmanned protective vehicle operated without human supervision for motorway hard shoulder roadworks.**

I. Introduction

The automation of the driving task is probably the most challenging field of research in the automotive context. Level 4 and Level 5 systems – according to the definition of SAE [1] – combine the unlimited set of operational scenarios encountered in public traffic with the absence of human supervision. This implies highest demands regarding functional safety throughout the development of these systems. Thus, the applicability of the ISO 26262 standard [2] – the most recent standard for designing safety-relevant electronic systems in the automotive context – must be examined.

Following the ISO 26262 standard, a hazard analysis and risk assessment (HARA) is required in order to determine the criticality of the system under consideration. The results of the HARA strongly influence the efforts to be undertaken in the subsequent development steps for ensuring functional safety. Normally, the results of HARAs are not published and thus cannot be discussed in the scientific community due to reasons of non-disclosure. This also applies to the field of vehicle automation.

However, exceptionally high demands regarding system implementation and its safety result from the missing human supervision. Hence, in-depth discussions about functional safety are crucial before deploying automated vehicles in public traffic. In this contribution, we present the complete results of a HARA conducted for a specific Level 4 application. The paper structures as follows: We introduce the project aFAS and the functionality to be implemented in the project in Section II. In Section III, we define relevant terms, describe the HARA approach, and highlight important results. Finally, Section IV contains the implications on designing vehicle automation systems. Complete results of the conducted HARA can be taken from the Appendix.

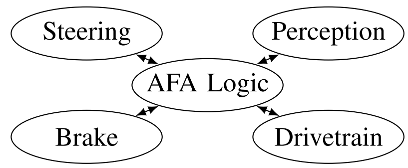

Fig. 1. Dependence of AFA Logic and connected elements

II. System Description & Project Context

The project aFAS[2] aims at developing an unmanned operation of a protective vehicle (AFA[3]) on the hard shoulder of highways in Germany, cf. [3]. The vehicle is operated without supervision on hard shoulders only and with low speed of up to 12 km/h. The automated operation consists of three operating modes complemented by the *Manual Mode* which comprises the normal operation of the AFA with a human driver. *Safe Halt* serves as initial operating mode as well as for switching between *Follow Mode* and *Coupled Mode*. Furthermore, *Safe Halt* is activated if the system leaves functional system boundaries. In *Follow Mode*, the AFA follows the leading vehicle, which conducts the actual work such as cleaning the hard shoulder, in a defined distance of about 90 m. To follow the leading vehicle and to stay on the hard shoulder, the AFA perceives the leading vehicle as well as lane markings of the hard shoulder by environment sensors. In *Coupled Mode*, the AFA follows the leading vehicle in close distance of about 10 m in order to pass acceleration and deceleration lanes. This is primarily realized through motion data of the leading vehicle. For transmitting system states and commands (e. g. changes of operating modes), the vehicles communicate via radio.

For the HARA presented in the following (cf. Section III), we concentrated on the parts that are specific for the automated operation in order to reduce the complexity that arises when considering the entire vehicle. The considered functionality is summarized in terms of the item[4] called AFA Logic. However, for unmanned operation additional elements are required, namely drivetrain, brakes, steering and environment perception. These elements are connected with the AFA Logic as depicted in Fig. 1. Hence, safety requirements can be inherited between connected elements.

*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 our partners and colleagues for their support of our work as well as the reviewers for the high quality review.

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

[2]German abbreviation for "Automated Unmanned Protective Vehicle for Highway Hard Shoulder Road Works"

[3]German abbreviation for "Automated Unmanned Protective Vehicle"

[4]Defined as "system or array of systems to implement a function at the vehicle level, to which ISO 26262 is applied" [2, 1.69]

III. Hazard Analysis and Risk Assessment

A. Terminology

A major contribution of the ISO 26262 standard is the definition of more than 100 terms related to functional safety of automotive electric/electronic systems. Yet, some terms must be further clarified for automated driving. In the context of the HARA, the terms *hazard*, *hazardous event*, *operational situation*, and *malfunctioning behavior* are the most common terms encountered. The term *hazard* [2, 1.57] is defined as “potential source of harm”, which is consistent to other definitions in safety engineering, e. g. [4], [5]. The definition used in the ISO 26262 standard specifies that a hazard is caused by *malfunctioning behavior*. *Malfunctioning behavior* itself is either caused by failures or unintended behavior of the system [2, 1.73]. Hence, the definitions of *hazard* and *malfunctioning behavior* are applicable for automated driving.

Furthermore, combining *operational situation* and *hazard* yields a *hazardous event* [2, 1.59]. In contrast to *hazard* and *malfunctioning behavior*, the ISO 26262 standard’s definitions of the terms *operational situation* and *hazardous event* are vague with respect to automated driving. A similar vagueness can be found in [4] and [5]. An *operational situation* is defined as “scenario that can occur during a vehicle’s life” [2, 1.83], equaling the terms *situation* and *scenario*. However, both terms – together with the term *scene* – are widely used in the context of automated driving and must be distinguished from each other according to Ulbrich et al. [6], who present a comprehensive literature review regarding these terms. Ulbrich et al. define and substantiate a *scene* as an all-encompassing snapshot of an environment together with the self-representation of all actors and observers contained (objective *scene*). In the real world, a scene is always subjective for each observer. A *situation* is derived from the subjective *scene* perceived by a traffic participant. It contains all necessary premises to derive suitable driving decisions. A *scenario* is the temporal concatenation of related *scenes*. Hence, we utilize the term *operational scenario* in preference to *operational situation* in the following since an objective exterior view is what is required for conducting a HARA.

The vagueness of the term *hazardous event* results from the linguistic ambiguity of the term *event*. This ambiguity is not resolved in the ISO 26262 standard. *Event* either addresses a period of time or – in a physical/technical sense – a point of time [7]. In engineering, one would consider the latter as intended meaning, yet the temporal interpretation is meant by the ISO 26262 standard in our understanding. What is actually required for obtaining a classification of safety criticality, is an *operational scenario* combined with a *hazard*. Thus, we utilize the term *hazardous scenario* in preference to *hazardous event* in the following.

B. Approach

For conducting a HARA, a linear reference process is illustrated in the ISO 26262 standard [2, Part 3], which rather addresses the interdependencies of single steps than necessary iterations to reach completeness. Warg et al. [8] describe an iterative process for developing HARAs in the context of automated driving. The process we applied in regard to the AFA Logic is similar to the approach proposed by Warg et al. and is depicted in Fig. 2. Yet, our approach differs from the approach of Warg et al. in certain aspects and extends it as well: While Warg et al. take a *preliminary feature description* as initial input resulting in an item definition during the process, our process input is a well advanced item definition.

Furthermore, we introduce two loops instead of one for refining the work products. Effects of both loops on the AFA Logic are described in the following subsection. The *item refinement* – comparable to the function refinement of Warg et al. [8] – describes extending or (in most cases) narrowing the functional range of the item under consideration. By this means, the merely functional consideration of the item according to the ISO 26262 standard is supplemented by considering technical feasibility, e. g. due to limited project resources or not yet available technology. In contrast, the *safety refinement* does not affect the functional range. Rather, it aims at refining the determined hazardous scenarios in order to enable technically realizable safety concepts through reaching more precise and definite safety goals. The safety refinement is comparable to the procedure to reach completeness of HARAs of Johansson [9].

Apart from refinement, each iteration loop consists of six steps. In the first step, functionalities are extracted from the item definition. Subsequently, potential malfunctioning behavior and related hazards are derived in the second and third step, respectively. The combination of hazards and operational scenarios derived from the item definition then yields the hazardous scenarios in the fourth step. Determining *Automotive Safety Integrity Levels* (ASILs) and safety goals are the fifth and the sixth step in Fig. 2, which are strongly linked.

C. Results

We developed the HARA together with experts from the industrial members of the aFAS consortium[1], in iterative group meetings. As mentioned, the complete results can be found in the Appendix. In the following, we highlight selected results that affect functional range, environment perception, human machine interface (HMI), and user interaction, as well as central control logic. Table I presents the identified safety goals. Its order – as the HARA’s numbering

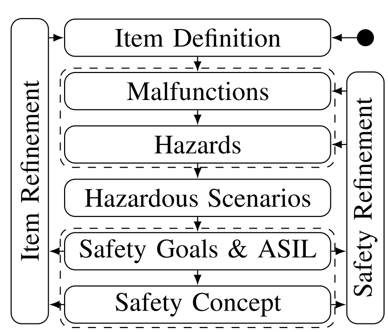

Fig. 2. Process of HARA generation and refinement

TABLE I

PROTECTIVE VEHICLE'S SAFETY GOALS FOR UNMANNED OPERATION

ID	Safety Goal
	All operating modes
SG01	Unintended and not permitted operating mode change must be prevented.
SG02	Intended and permitted operating mode change must be ensured.
SG07	Display of actual operating mode in HMI must be ensured.
	Manual Mode
SG04	Unintended anti-lock brake actuation must be prevented.
SG05	Unintended acceleration must be prevented.
SG16	Anti-lock functionality must be ensured.
SG17	Unintended steering actuation must be prevented
	Follow Mode, Coupled Mode, Safe Halt
SG03	Steering actuation beyond specification must be prevented.
SG06	Detection of driver intervention must be ensured.
SG08	Unintended slow acceleration must be prevented.
SG09	Deceleration to standstill must be ensured.
SG10	Leaving tolerance ranges must trigger operating mode change to Safe Halt.
SG11	Maximum velocity must not be exceeded.
SG12	Overrunning hard shoulder markings must be prevented.
SG13	Detection of and reaction to (deceleration to standstill) relevant obstacles (humans, vehicles, etc.) must be ensured.
SG14	Identification of leading vehicle must be ensured.
SG15	Detection of missing leading vehicle and operating mode change to safe halt must be ensured.

in the Appendix – illustrates the several iterations necessary to obtain a result commonly accepted among the contributors. For instance, safety goal SG16 was added in a later iteration, although strongly connected to safety goal SG04.

Initially, the functional range was supposed to include automated unmanned operation on the motorway's right lane as well, in order to be capable of driving around obstacles on the hard shoulder. During *item refinement*, however, the functional range was reduced, as this feature was technically too challenging due to limited project resources. Accordingly, the unmanned operation was restricted to hard shoulders as well as acceleration and deceleration lanes, both with a limited velocity of 10 km/h (plus 2 km/h tolerance).

An example for the above mentioned *safety refinement* loop are safety goals SG03 and SG12. Safety goal SG12 was established in one of the first iterations effecting high ASIL ratings on all involved components, namely environment perception, AFA Logic, and actuators. In subsequent iterations, we differentiated between unintended steering actuation beyond the specification of the item definition (up to full steering actuation) and unintended steering actuation within the specification. This results in different hazardous scenarios which were rated separately. Consequently, safety goal SG03 was introduced, which targets at limiting the maximum steering angle and thereby reduces the effects of malfunctioning behavior of other system elements. Due to the limited steering angle, the AFA will intrude the right lane of the motorway with less lateral velocity. Thus, the controllability rating can be reduced as other traffic participants can react more appropriately. By this means, the limitation of the steering angle in automated operation gains the former high ASIL rating (ASIL D) of safety goal SG12 while the rating of safety goal SG12 is reduced (ASIL B).

The previous reduction of the ASIL rating of safety goal SG12 also affects the functional block of the AFA Logic, which must be implemented with ASIL B as well. In discussions prior to the project start, a group of experts from the consortium underestimated the efforts to be undertaken for implementing the AFA Logic as well as of the human machine interaction. If the operating mode is wrongly displayed, the AFA could intrude the right lane of the motorway and cause severe accidents, cf. HARA IDs 37 and 37a in the Appendix. Consequently, the correct display of the actual operating mode must be ensured (safety goal SG07, ASIL A). Both aspects illustrate the high demands on all system parts which originate from the missing human supervision.

The HARA's results concerning the environment perception are of particular interest, since automated vehicles are operated in an open environment where they encounter an infinite set of operational scenarios. For the AFA, safety goals SG12 and SG13 address environment perception. While safety goal SG12 obtained an ASIL B rating, the detection and reaction to obstacles on the path are rated with QM since persons involved in the scenarios can generally control the scenarios due to the low velocity of the AFA.

As already depicted in Fig. 1, the AFA Logic is connected to further items. Although a HARA is a top-down procedure, at some points technical aspects must be considered. In the planned system implementation of the unmanned operation, the AFA Logic has access to steering and brakes. In particular, the technical implementation of the brake system creates potential for malfunctioning behavior. Therefore, the manual operation must be considered in the HARA as well. As the malfunctioning behavior can create critical outcome in several scenarios, the related safety goals obtain highest ASIL ratings. This means that elements connected to the AFA Logic inherit according safety requirements.

IV. DISCUSSION AND RELATED WORK

Although the functional range considered in the aFAS project is small compared to functional ranges of future automated vehicles, several implications can be derived from our experiences made. The presented HARA is primarily based on the experience and knowledge of the involved contributors from industry and academia with a range of experience from one to more than ten years. Despite the small functional range, the contributors agree on that it was challenging to take all relevant aspects into account in order to reach consistency between item definition and HARA. This reflects in the several iterations necessary to reach a common result. Using only expert knowledge might lead to missed scenarios and thus to building unsafe systems. Consequently, we expect that HARAs for systems featuring more comprehensive functional ranges must be supported by methods and tools. The approach for refining item and safety aspects described in subsection III-B appears suitable in general. However, more distinguished methods must be developed for single steps in order to gain appropriate results.

As input to the HARA process, the AFA Logic's item definition is written in natural language, supported by some tables and figures. All functionalities considered in the

HARA were extracted manually. This was a process taking several iterations since functionalities had not been considered or had initially been defined contradictory. For items with a wider functional range, item definitions with a more extensive utilization of semi-formal or even formal notations are necessary for ensuring proper identification of all relevant functions and related malfunctioning behavior. Moreover, this eases traceability between item definition and HARA.

For targeting completeness of hazardous scenarios, different approaches for identifying hazards and operational scenarios can be found in literature. Comparable to the approach in the aFAS project, Johansson [9] suggests experts to challenge each single hazardous scenario. If they do not find additional scenarios that lead to new safety goals, the list is likely to be complete states Johansson. However, correct ASIL ratings are required besides completeness of safety goals. Thus, the aFAS consortium also considered ASIL ratings of hazardous scenarios with the same safety goals. Warg et al. [8] propose an identification of both hazards as well as operational scenarios based on tree structures. Out of the aFAS consortium, Bagschik et al. [10] propose an approach for deriving all relevant hazardous scenarios systematically by combining operating modes, functions (derived by skill graphs), malfunctions (derived by a HAZOP analysis), and scene discretization. However, suitability of these approaches still needs to be proven for systems of future automated vehicles in terms of considering all relevant scenarios. The first two approaches need to prove their suitability for automated vehicles with a wider functional range. In contrast, the approach of Bagschik et al. creates automatically an extensive list of scenarios. However, each scenario must be assessed manually regarding safety criticality.

Once hazardous scenarios are identified, the next challenge is determining the ASIL classification. As already mentioned, the classification for the unmanned operation of the AFA is based on expert knowledge. A few aspects of the exposure – such as the rate of emergency stopping vehicles – are justified by investigations of the aFAS consortium. Severity and controllability are purely based on experts' contribution. Furthermore, standards such as the SAE J2980 standard [11] are of limited contribution for the project aFAS since they do not consider operations on the hard shoulder and focus on vehicle motion control systems. In general, controllability of hazardous scenarios is very low for Level 4 or Level 5 applications with passengers. The controllability of hazardous scenarios without passengers – as in the project aFAS – is determined by surrounding traffic participants. For future application of automated vehicles, methods for objectification of the parameters must be discussed. At least, evolving standards such as the SAE J2980 standard [11] towards automated driving can support a common understanding.

So far, we conclude that methods for a systematic consideration of each HARA step can be found in literature. Consequently, one can argue that a holistic systematic HARA process is beneficial, as i. a. presented by Kemmann and Trapp [12] as well as by Beckers et al. [13]. Kemmann and Trapp [12] introduce *A Structured Approach for Hazard Analysis and Risk Assessments* (SAHARA), which systematically considers each HARA step. The authors consequently use model based approaches for item definition, hazard identification, as well as for classification of controllability, severity, and exposure. Beckers et al. [13] emphasize utilization of UML based notation. This ensures the traceability throughout the HARA process and enables potential for formal verification. Still, single HARA steps in the approach of Becker et al. strongly depend on expert knowledge. For both approaches, proof of applicability to automated vehicles must be furnished.

V. Conclusion

The example of the unmanned protective vehicle reveals challenges during a HARA for automated vehicles operated without human supervision. It was demonstrated that conventional HARA approaches are of limited suitability, especially for future applications with a wider functional range. Consequently, already existing systematic approaches must be evolved towards automated driving functionalities without human supervision. For this, an in-depth consideration of each single HARA step is required. Furthermore, for merging the two worlds of automated driving and functional safety, clarification of used terminology is crucial to reach a common understanding.

References

[1] SAE, "Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles," Society of Automotive Engineers, Standard J3016, 2016.

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

[3] 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 (ITSC)*, Las Palmas, Spain, 2015.

[4] IEC, "IEC 61508: Functional safety of electrical / electronic / programmable electronic safety-related systems," International Electrotechnical Commission, International Standard, 2010.

[5] ISO, "ISO/IEC GUIDE 51: Safety Aspects - Guidelines for Their Inclusion in Standards," International Organization for Standardization, Geneva, Switzerland, International Standard, 2014.

[6] 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)*, Las Palmas, Spain, 2015.

[7] Oxford Dictionaries, "Definition of 'event' in English," https://en.oxforddictionaries.com/definition/event.

[8] F. Warg, M. Gassilewski, J. Tryggvesson, V. Izosimov, A. Werneman, and R. Johansson, "Defining Autonomous Functions Using Iterative Hazard Analysis and Requirements Refinement," in *Computer Safety, Reliability, and Security*, A. Skavhaug, J. Guiochet, E. Schoitsch, and F. Bitsch, Eds. Cham, Germany: Springer Internat. Publishing, 2016.

[9] R. Johansson, "The Importance of Active Choices in Hazard Analysis and Risk Assessment," in *CARS – Critical Automotive Applications: Robustness & Safety*, Paris, France, 2015.

[10] G. Bagschik, A. Reschka, T. Stolte, and M. Maurer, "Identification of potential hazardous events for an Unmanned Protective Vehicle," in *2016 IEEE Intelligent Vehicles Symposium (IV)*, 2016.

[11] SAE, "Considerations for ISO 26262 ASIL Hazard Classification," SAE International, Standard J2980, 2015.

[12] S. Kemmann and M. Trapp, "SAHARA – A Systematic Approach for Hazard Analysis and Risk Assessment," in *Proceedings of the SAE World Congress 2011*, Detroit, MI, USA, 2011.

[13] K. Beckers, M. Heisel, T. Frese, and D. Hatebur, "A structured and model-based hazard analysis and risk assessment method for automotive systems," in *2013 IEEE 24th International Symposium on Software Reliability Engineering (ISSRE)*, Pasadena, CA, USA, 2013.

Appendix

Table II displays the HARA developed in the project aFAS. Omitted and alphanumeric IDs reflect the iterative process of HARA development during item and safety refinement, cf. subsection III-B. Several IDs were discarded while the ID numbering was not adjusted, in order to preserve traceability between different HARA versions.

TABLE II

Results of Hazard Analysis and Risk Assessment of the Automated Operation of the Unmanned Protective Vehicle

ID	Operating Mode	Function	Malfunction	Hazardous Scenario and Consequence	S	Rationale	E	Rationale	C	Rationale	A	SG
1	Manual Mode	Operating mode change	Unintended or not permitted transition to other operating mode	Drive on road in convoy (up to 90 km/h, depending on speed limiter). Operating mode change to *Safe Halt* leads to unpredictable deceleration ($4\,m/s^2$ in *Safe Halt* according to Item Definition) to standstill. The same applies when changing to *Coupled Mode* or *Follow Mode*, as these operating modes then will be operated beyond accepted parameters which causes an operating mode change to *Safe Halt*. Deceleration leads to rear-end collision of succeeding vehicle.	S2	Assuming succeeding traffic participants use seat belts and brakes intuitively, the collision will happen with medium velocity which leads to severe injuries.	E4	Drive to and from location of road works via roads and motorways occurs for each road work.	C2	Traffic participants not complying with traffic rules is commonly observable on German motorways (exceeded velocities, tailgating, etc.). Reaction time 1.5 s, distance 35 m, deceleration $-6\,m/s^2$.	B	SG01
2	Manual Mode	Steer	Unintended steering	Drive on road or motorway. Unpredictable swerving from lane leads to collision with other traffic participants.	S3	Road: Head-on collision with oncoming traffic, tree etc. motorway: Collision with moving traffic. Both scenarios can lead to severe or fatal injuries.	E4	Drive to and from location of road works via roads and motorways occurs for each road work.	C3	Experience of Bosch Automotive Steering: Full steering angle due to failures is not controllable.	D	SG17
3	Manual Mode	Brake	Unintended braking with anti-lock functionality	Drive on road in convoy. Unpredictable maximum deceleration with anti-lock functionality leads to rear-end collision of succeeding vehicle. Malfunction possible due to the planned technical implementation.	S2	Assuming succeeding traffic participants use seat belts and brakes intuitively, the collision will happen with medium velocity which leads to severe injuries.	E4	Drive to and from location of road works via roads and motorways occurs for each road work.	C3	Traffic participants not complying with traffic rules is commonly observable on German motorways (exceeded velocities, tailgating, etc.). Reaction time 1.5 s, distance 35 m, deceleration $-6\,m/s^2$	C	SG04
4	Manual Mode	Brake	Unintended braking without anti-lock functionality	Drive on road or motorway. Unpredictable maximum deceleration without anti-lock functionality leads to locking tires. Lateral guidance is not possible, the AFA becomes uncontrollable. The AFA leaves its lane and collides with stationary objects or other vehicles. Malfunction possible due to the planned technical implementation.	S3	Collision with uncontrollable vehicle at high velocities leads to severe or fatal injuries.	E4	Drive to and from location of road works via roads and motorways occurs for each road work.	C3	According to ISO26262-3, Table B4: Failure of brakes $\rightarrow$ brakes unintendedly stopping the vehicle	D	SG16
5	Manual Mode	Drive	Unintended acceleration	Drive on road in convoy. Unintended acceleration leads to rear-end collision with preceding vehicle.	S3	Traffic participant skids, resulting crash leads to severe and life-threatening injuries.	E4	Drive to and from location of road works via roads and motorways occurs for each road work.	C0	Controllable in general. Due to inertia enough time for driver of AFA to react, driver brakes intuitively.	QM	SG05
7	Manual Mode	HMI	HMI displays wrong operating mode	*No Hazard: Only road workers with special training are deployed on AFA. In* Manual Mode*, the AFA is driven as usual. A wrong display of operating modes leads to no more than short confusion.*	S0	—	E0	—	C0	—	QM	—
8	Safe Halt	Detection of driver intervention	Driver intervention is not detected	Test operation on hard shoulder, driver intervention is not detected.	S0	Driver intervention not detected in *Safe Halt* does not lead to a hazardous event.	E0	Driver intervention not detected in *Safe Halt* does not lead to a hazardous event.	C0	Driver intervention not detected in *Safe Halt* does not lead to a hazardous event.	QM	SG06
9	Safe Halt	HMI	HMI displays wrong operating mode	*No Hazard: AFA and leading vehicle in standstill. Operating mode change can only be triggered by operator in leading vehicle.*	S0	—	E0	—	C0	—	QM	—
10	Safe Halt	Operating mode change	Unintended or not permitted transition to *Manual Mode*	Truck convoy on right lane. AFA on hard shoulder starts to roll (slope, automatic gearbox). This leads to unpredictable behavior including intrusion into right lane. Truck avoids AFA, following truck touches AFA as the AFA is masked by first truck.	S2	Collision with high differential velocity, vehicles slightly touch.	E4	Scenario (sloped road, traffic on right lane) usually met at each deployment.	C2	AFA drifts slowly (e. g. 0.4 m/s lateral) into right driving lane. Despite of masking by truck in front, following traffic is normally able to recognize this and react appropriately (braking, avoiding).	B	SG01
10a	Safe Halt	Operating mode change	Unintended or not permitted transition to *Manual Mode*	Moving car traffic on right lane. AFA on hard shoulder starts to roll (slope, automatic gearbox). This leads to unpredictable behavior including intrusion into right lane. Car on right lane collides with visible AFA.	S3	Collision with high differential velocity.	E4	Scenario (sloped road, traffic on right lane) usually met at each deployment.	C1	AFA drifts slowly (e. g. 0.4 m/s lateral) into right driving lane. Following traffic is easily able to recognize this and react appropriately (braking, avoiding).	B	SG01
11	Safe Halt	Operating mode change	Unintended or not permitted transition to *Coupled Mode*	*No Hazard: Supervision works as defined in* Coupled Mode*. Immediate operating mode change to* Safe Halt *since conditions for* Coupled Mode *are not met (distance to leading vehicle, transmission of odometry data of leading vehicle etc.)*	S0	—	E0	—	C0	—	QM	—
12	Safe Halt	Operating mode change	Unintended or not permitted transition to *Follow Mode*	*No Hazard: Due to necessary boundary conditions,* Follow Mode *cannot be retained. Operating mode changes back to* Safe Halt.	S0	—	E0	—	C0	—	QM	—
13	Safe Halt	Operating mode change	Intended and permitted transition to *Manual Mode* is not executed	*No Hazard: AFA still in standstill.*	S0	—	E0	—	C0	—	QM	—
14	Safe Halt	Operating mode change	Intended and permitted transition to *Coupled Mode* is not executed	*No Hazard: AFA still in standstill.*	S0	—	E0	—	C0	—	QM	—
15	Safe Halt	Operating mode change	Intended and permitted transition to *Follow Mode* is not executed	*No Hazard: AFA still in standstill.*	S0	—	E0	—	C0	—	QM	—
16	Safe Halt	Longitudinal guidance	Unintended (slow) acceleration	Truck convoy on right lane. AFA on hard shoulder starts to roll (slope, automatic gearbox). This leads to unpredictable behavior including intrusion into right lane. Truck avoids AFA, following truck touches AFA as the AFA is masked by first truck.	S2	Collision with high differential velocity, vehicles slightly touch.	E4	Scenario usually met at each deployment.	C2	AFA drifts slowly (e. g. 0.4 m/s lateral) into right driving lane. Despite of masking by truck in front, following traffic is normally able to recognize this and react appropriately (braking, avoiding).	B	SG08
16a	Safe Halt	Longitudinal guidance	Unintended (slow) acceleration	Moving car traffic on right lane. AFA on hard shoulder starts to roll (slope, automatic gearbox). This leads to unpredictable behavior including intrusion into right lane. Car on right lane collides with visible AFA.	S3	Collision with high differential velocity.	E4	Scenario usually met at each deployment.	C1	AFA drifts slowly (e. g. 0.4 m/s lateral) into right driving lane. Following traffic is easily able to recognize this and react appropriately (braking, avoiding).	B	SG08

Continued on next page

ID: Identifier for hazardous scenario as in original document, S: Severity* (S0–S3), E: Exposure* (E0–E4), C: Controllability* (C0–C3), A: ASIL Rating (QM, ASIL A–D), SG: ID of Safety Goal (cf. Table I); *For reference cf. [2, Part 3] and [11]

TABLE II: Continued from previous page

ID	Operating Mode	Function	Malfunction	Hazardous Scenario and Consequence	S	Rationale	E	Rationale	C	Rationale	A	SG
17	Safe Halt	Longitudinal guidance	Unintended maximum deceleration	*No Hazard: Maximum deceleration unproblematic, as AFA decelerates from very low velocity. Moreover, transition from* Manual Mode *to* Safe Halt *only possible in standstill.*	S0	—	E0	—	C0	—	QM	—
18	Safe Halt	Longitudinal guidance	No stop	Truck convoy on right lane. As there is no environment perception active in *Safe Halt*, intrusion into right lane is possible. Truck avoids AFA, following truck touches AFA as the AFA is masked by first truck.	S2	Collision with high differential velocity, vehicles slightly touch.	E4	*Safe Halt* active at each deployment.	C2	AFA drifts slowly (e. g. 0.4 m/s lateral) into right driving lane. Despite of masking by truck in front, following traffic is normally able to recognize this and react appropriately (braking, avoiding).	B	SG09
18a	Safe Halt	Longitudinal guidance	No stop	Moving car traffic on right lane. As there is no environment perception active in *Safe Halt*, intrusion into right lane is possible. Car on right lane collides with visible AFA.	S3	Collision with high differential velocity.	E4	*Safe Halt* active at each deployment.	C1	AFA drifts slowly (e. g. 0.4 m/s lateral) into right driving lane. Following traffic is easily able to recognize this and react appropriately (braking, avoiding).	B	SG09
19	Safe Halt	Longitudinal guidance	No stop	Obstacle, e. g. an emergency stopping vehicle, on hard shoulder. A person stands between vehicle and AFA. AFA collides with vehicle.	S2	Very low velocity of AFA. Person between AFA and vehicle. This is expected to lead to severe yet not fatal injuries	E2	Obstacles on hard shoulder occur approximately once per week. A vehicle stopping between AFA and leading vehicle is even more unlikely.	C1	People between AFA and obstacle can easily react to a non-stopping AFA by stepping aside due to its low velocity.	QM	SG09
19a	Safe Halt	Longitudinal guidance	No stop	Obstacle, e. g. an emergency stopping vehicle, on hard shoulder, passengers in vehicle. AFA collides with vehicle.	S0	Very low velocity of AFA. No injuries expected as people in vehicle are protected by passenger cabin.	E2	Obstacles on hard shoulder occur approximately once per week. A vehicle stopping between AFA and leading vehicle is even more unlikely.	C3	People in a stopping vehicle only have a very small chance to react to the AFA colliding unexpectedly. Driver might press the brake pedal intuitively.	QM	SG09
24	Coupled Mode	Operating mode change	Unintended or not permitted transition to *Manual Mode*	Truck convoy on right lane. AFA on acceleration or deceleration lane. *Manual Mode* without human driver. This leads to unpredictable behavior including intrusion into right lane. Truck avoids AFA, following truck touches AFA as the AFA is masked by first truck.	S2	Collision with high differential velocity, vehicles slightly touch.	E4	Passing acceleration and deceleration lanes occurs on each deployment.	C2	AFA drifts slowly (e. g. 0.4 m/s lateral) into right driving lane. Despite of masking by truck in front, following traffic is normally able to recognize this and react appropriately (braking, avoiding).	B	SG01
24a	Coupled Mode	Operating mode change	Unintended or not permitted transition to *Manual Mode*	Moving car traffic on right lane. AFA on acceleration or deceleration lane. *Manual Mode* without human driver. This leads to unpredictable behavior including intrusion into right lane. Car on right lane collides with visible AFA.	S3	Collision with high differential velocity.	E4	Passing acceleration and deceleration lanes occurs on each deployment.	C1	AFA drifts slowly (e. g. 0.4 m/s lateral) into right driving lane. Following traffic is easily able to recognize this and react appropriately (braking, avoiding).	B	SG01
25	Coupled Mode	Operating mode change	Unintended or not permitted transition to *Safe Halt*	Moving traffic on right lane. AFA stops on acceleration or deceleration lane. Vehicles entering or leaving the motorway collide with AFA.	S2	Rear-end collision with reduced velocity	E4	Passing acceleration and deceleration lanes occurs on each deployment.	C0	Driver of vehicle changing to deceleration lane is already braking or ready for braking. Vehicle on acceleration lane in general has moderate velocity.	QM	SG01
26	Coupled Mode	Operating mode change	Unintended or not permitted transition to *Follow Mode*	Moving traffic on right lane. AFA stops on acceleration or deceleration lane in order to build up required distance for *Follow Mode*. Vehicles entering or leaving the motorway collide with AFA.	S2	Rear-end collision with reduced velocity	E4	Passing acceleration and deceleration lanes occurs on each deployment.	C0	Driver of vehicle changing to deceleration lane is already braking or ready for braking. Vehicle on acceleration lane in general has moderate velocity.	QM	SG01
27	Coupled Mode	Operating mode change	Intended and permitted transition to *Manual Mode* is not executed	*No Hazard: Only for testing purposes. Driver can stop AFA pneumatically by foot brake.*	S0	—	E0	—	C0	—	QM	—
28	Coupled Mode	Operating mode change	Intended and permitted transition to *Safe Halt* is not executed	Truck convoy on right lane. Operating mode change to *Safe Halt* when exceeding functional system boundaries is not executed. This leads to unpredictable behavior including intrusion into right lane. Truck avoids AFA, following truck touches AFA as the AFA is masked by first truck.	S2	Collision with high differential velocity, vehicles slightly touch.	E4	Passing acceleration and deceleration lanes occurs on each deployment.	C2	AFA drifts slowly (e. g. 0.4 m/s lateral) into right driving lane. Despite of masking by truck in front, following traffic is normally able to recognize this and react appropriately (braking, avoiding).	B	SG02
28a	Coupled Mode	Operating mode change	Intended and permitted transition to *Safe Halt* is not executed	Moving car traffic on right lane. Operating mode change to *Safe Halt* when exceeding functional system boundaries is not executed. This leads to unpredictable behavior including intrusion into right lane. Car on right lane collides with visible AFA.	S3	Collision with high differential velocity.	E4	Passing acceleration and deceleration lanes occurs on each deployment.	C1	AFA drifts slowly (e. g. 0.4 m/s lateral) into right driving lane. Following traffic is easily able to recognize this and react appropriately (braking, avoiding).	B	SG02
30	Coupled Mode	Longitudinal and lateral guidance	Vehicle does not follow in defined distance (tolerance range lateral or longitudinal)	Truck convoy on right lane. AFA follows leading vehicle with lateral and longitudinal offsets which exceed the tolerance ranges. AFA is partially driving on right lane. Truck avoids AFA, following truck touches AFA as the AFA is masked by first truck.	S2	Collision with high differential velocity, vehicles slightly touch.	E4	Passing acceleration and deceleration lanes occurs on each deployment.	C0	Traffic participants can control the AFA protruding into the right lane as the warning device is active as well as lateral and Longitudinal guidance function as intended apart from the lateral offset.	QM	SG10
30a	Coupled Mode	Longitudinal and lateral guidance	Vehicle does not follow in defined distance (tolerance range lateral or longitudinal)	Moving car traffic on right lane. AFA follows leading vehicle with lateral and longitudinal offsets which exceed the tolerance ranges. AFA is partially driving on right lane. Car on right lane collides with visible AFA.	S3	Collision with high differential velocity.	E4	Passing acceleration and deceleration lanes occurs on each deployment.	C0	Traffic participants can control the AFA protruding into the right lane as the warning device is active as well as lateral and Longitudinal guidance function as intended apart from the lateral offset.	QM	SG10
31	Coupled Mode	Longitudinal guidance	Vehicle exceeds maximum speed of 12 km/h	Truck convoy on right lane. The functional components are designed for velocities up to 12 km/h. AFA drives at not excessively higher velocity. AFA exceeds functional system boundaries. This leads to unpredictable behavior including intrusion into right lane (e. g. oscillating steering angle control). Truck avoids AFA, following truck touches AFA as the AFA is masked by first truck.	S2	Collision with high differential velocity, vehicles slightly touch.	E4	Passing acceleration and deceleration lanes occurs on each deployment.	C2	AFA drifts slowly (e. g. 0.4 m/s lateral) into right driving lane. Despite of masking by truck in front, following traffic is normally able to recognize this and react appropriately (braking, avoiding).	B	SG11
31a	Coupled Mode	Longitudinal guidance	Vehicle exceeds maximum speed of 12 km/h	Moving car traffic on right lane. The functional components are designed for velocities up to 12 km/h. AFA drives at not excessively higher velocity. AFA exceeds functional system boundaries. This leads to unpredictable behavior including intrusion into right lane (e. g. oscillating steering angle control). Car on right lane collides with visible AFA.	S3	Collision with high differential velocity.	E4	Passing acceleration and deceleration lanes occurs on each deployment.	C1	AFA drifts slowly (e. g. 0.4 m/s lateral) into right driving lane. Following traffic is easily able to recognize this and react appropriately (braking, avoiding).	B	SG11
33	Coupled Mode	Longitudinal guidance	Unintended deceleration	Moving traffic on right lane. AFA stops on acceleration or deceleration lane. Vehicles entering or leaving the motorway collide with AFA.	S2	Rear-end collision with reduced velocity	E4	Passing acceleration and deceleration lanes occurs on each deployment.	C0	Driver of vehicle changing to deceleration lane is already braking or ready for braking. Vehicle on acceleration lane in general has moderate velocity.	QM	SG04

Continued on next page

ID: Identifier for hazardous scenario as in original document, S: Severity* (S0–S3), E: Exposure* (E0–E4), C: Controllability* (C0–C3), A: ASIL Rating (QM, ASIL A–D), SG: ID of Safety Goal (cf. Table I); *For reference cf. [2, Part 3] and [11]

TABLE II: Continued from previous page

ID	Operating Mode	Function	Malfunction	Hazardous Scenario and Consequence	S	Rationale	E	Rationale	C	Rationale	A	SG
34	Coupled Mode	Radio communication	Vehicle drives without radio communication	AFA stops due to inconsistent data of radio communication and environment perception on acceleration or deceleration lane. Vehicles entering or leaving the motorway collide with AFA.	S2	Rear-end collision with reduced velocity	E4	Passing acceleration and deceleration lanes occurs on each deployment.	C0	Driver of vehicle changing to deceleration lane is already braking or ready for braking. Vehicle on acceleration lane in general has moderate velocity.	QM	SG10
35	Coupled Mode	Lateral guidance	Steering angle change beyond maximum specification (angle & change rate)	AFA drifts with up to maximum possible yaw rate into right lane.	S3	Collision with high differential velocity.	E4	Passing acceleration and deceleration lanes occurs on each deployment.	C3	AFA drifts quickly (e. g. $\gg$0.4 m/s lateral) into the right lane. It follows a circular arc to the guardrail on the left of the left lane. This is difficult to control by traffic participants.	D	SG03
36	Follow Mode	Detection of driver intervention	Driver intervention is not detected	Test operation on hard shoulder, driver intervention is not detected.	S0	Only for testing purposes. Driver can stop AFA pneumatically by foot brake.	E0	Only for testing purposes. Driver can stop AFA pneumatically by foot brake.	C0	Only for testing purposes. Driver can stop AFA pneumatically by foot brake.	QM	SG06
37	Follow Mode	HMI	HMI displays wrong operating mode	Truck convoy on right lane. Leading vehicle in standstill, AFA in *Follow Mode*. HMI displays *Safe Halt* or *Coupled Mode*. AFA starts delayed to follow leading vehicle and enters acceleration or deceleration lane. AFA exceeds functional system boundaries. This leads to unpredictable behavior including intrusion into right lane. Truck avoids AFA, following truck touches AFA as the AFA is masked by first truck.	S2	Collision with high differential velocity, vehicles slightly touch.	E4	Operation on hard shoulder occurs on each deployment.	C1	AFA drifts slowly (e. g. 0.4 m/s lateral) into right driving lane. Despite of masking by truck in front, following traffic is normally able to recognize this and react appropriately (braking, avoiding).	A	SG07
37a	Follow Mode	HMI	HMI displays wrong operating mode	Moving car traffic on right lane. Leading vehicle in standstill, AFA in *Follow Mode*. HMI displays *Safe Halt* or *Coupled Mode*. AFA starts delayed to follow leading vehicle and enters acceleration or deceleration lane. AFA exceeds functional system boundaries. This leads to unpredictable behavior including intrusion into right lane. Car on right lane collides with visible AFA.	S2	Collision with high differential velocity.	E4	Operation on hard shoulder occurs on each deployment.	C1	AFA drifts slowly (e. g. 0.4 m/s lateral) into right driving lane. Following traffic is easily able to recognize this and react appropriately (braking, avoiding).	A	SG07
38	Follow Mode	Operating mode change	Unintended or not permitted transition to *Manual Mode*	Truck convoy on right lane. *Manual Mode* without driver. This leads to unpredictable behavior including intrusion into right lane. Truck avoids AFA, following truck touches AFA as the AFA is masked by first truck.	S2	Collision with high differential velocity, vehicles slightly touch.	E4	Operation on hard shoulder occurs on each deployment.	C2	AFA drifts slowly (e. g. 0.4 m/s lateral) into right driving lane. Despite of masking by truck in front, following traffic is normally able to recognize this and react appropriately (braking, avoiding).	B	SG01
38a	Follow Mode	Operating mode change	Unintended or not permitted transition to *Manual Mode*	Moving car traffic on right lane. *Manual Mode* without driver. This leads to unpredictable behavior including intrusion into right lane. Car on right lane collides with visible AFA.	S3	Collision with high differential velocity.	E4	Operation on hard shoulder occurs on each deployment.	C1	AFA drifts slowly (e. g. 0.4 m/s lateral) into right driving lane. Following traffic is easily able to recognize this and react appropriately (braking, avoiding).	B	SG01
41	Follow Mode	Follow hard shoulder	Vehicle does not follow hard shoulder	Truck convoy on right lane. AFA intrudes right lane. Truck avoids AFA, following truck touches AFA as the AFA is masked by first truck.	S2	Collision with high differential velocity, vehicles slightly touch.	E4	Operation on hard shoulder occurs on each deployment.	C2	AFA drifts slowly (e. g. 0.4 m/s lateral) into right driving lane. Despite of masking by truck in front, following traffic is normally able to recognize this and react appropriately (braking, avoiding).	B	SG12
41a	Follow Mode	Follow hard shoulder	Vehicle does not follow hard shoulder	Moving car traffic on right lane. AFA intrudes right lane. Car on right lane collides with visible AFA.	S3	Collision with high differential velocity.	E4	Operation on hard shoulder occurs on each deployment.	C1	AFA drifts slowly (e. g. 0.4 m/s lateral) into right driving lane. Following traffic is easily able to recognize this and react appropriately (braking, avoiding).	B	SG12
42	Follow Mode	Keep defined distance	Vehicle does not follow in defined tolerance range	*No Hazard: AFA continues following hard shoulder based on lane marking. Obstacle detection functions. AFA stops if distance to leading vehicle is too large (leading vehicle out of sight, interruption of radio communication).*	S0	—	E0	—	C0	—	QM	—
43	Follow Mode	Obstacle detection	Vehicle does not react to obstacle	Obstacle, e. g. an emergency stopping vehicle, on hard shoulder. A person stands between vehicle and AFA. AFA collides with vehicle.	S2	Very low velocity of AFA. Person between AFA and vehicle. This is expected to lead to severe yet not fatal injuries	E2	Obstacles on hard shoulder occur approximately once per week. A vehicle stopping between AFA and leading vehicle is even more unlikely.	C1	People between AFA and obstacle can easily react to a non-stopping AFA by stepping aside due to its low velocity.	QM	SG13
43a	Follow Mode	Obstacle detection	Vehicle does not react to obstacle	Obstacle, e. g. an emergency stopping vehicle, on hard shoulder, passengers in vehicle. AFA collides with vehicle.	S0	Very low velocity of AFA. No injuries expected as people in vehicle are protected by passenger cabin.	E2	Obstacles on hard shoulder occur approximately once per week. A vehicle stopping between AFA and leading vehicle is even more unlikely.	C3	People in a stopping vehicle only have a very small chance to react to the AFA colliding unexpectedly. Driver might press the brake pedal intuitively.	QM	SG13
44	Follow Mode	Longitudinal guidance	Unintended deceleration	*No Hazard: AFA stops on hard shoulder with active warning device and transitions to* Safe Halt.	S0	—	E0	—	C0	—	QM	—
45	Follow Mode	Perceive leading vehicle	Vehicle keeps distance to wrong object	Truck convoy on right lane. AFA follows wrong leading vehicle which does not stop in front of acceleration or deceleration lanes. AFA exceeds functional system boundaries. This leads to unpredictable behavior including intrusion into right lane. Truck avoids AFA, following truck touches AFA as the AFA is masked by first truck.	S2	Collision with high differential velocity, vehicles slightly touch.	E1	Vehicle driving on hard shoulder for a longer period of time and with velocity $\leq$ 10 km/h occurs very rarely.	C2	AFA drifts slowly (e. g. 0.4 m/s lateral) into right driving lane. Despite of masking by truck in front, following traffic is normally able to recognize this and react appropriately (braking, avoiding).	QM	SG14
45a	Follow Mode	Perceive leading vehicle	Vehicle keeps distance to wrong object	Moving car traffic on right lane. AFA follows wrong leading vehicle which does not stop in front of acceleration or deceleration lanes. AFA exceeds functional system boundaries. This leads to unpredictable behavior including intrusion into right lane. Car on right lane collides with visible AFA.	S3	Collision with high differential velocity.	E1	Vehicle driving on hard shoulder for a longer period of time and with velocity $\leq$ 10 km/h occurs very rarely.	C1	AFA drifts slowly (e. g. 0.4 m/s lateral) into right driving lane. Following traffic is easily able to recognize this and react appropriately (braking, avoiding).	QM	SG14
46	Follow Mode	Perceive leading vehicle	Vehicle follows hard shoulder without leading vehicle	Truck convoy on right lane as well as vehicles driving on acceleration and deceleration lane. AFA does not detect begin of acceleration or deceleration lane. Thus, it exceeds its functional system boundaries. This leads to unpredictable behavior including intrusion into right lane.	S2	Collision with high differential velocity, vehicles slightly touch.	E0	Operating instructions prohibit activation of automated operation without leading vehicle.	C2	AFA drifts slowly (e. g. 0.4 m/s lateral) into right driving lane. Despite of masking by truck in front, following traffic is normally able to recognize this and react appropriately (braking, avoiding).	QM	SG15
46a	Follow Mode	Perceive leading vehicle	Vehicle follows hard shoulder without leading vehicle	Moving car traffic on right lane as well as vehicles driving on acceleration and deceleration lane. AFA does not detect begin of acceleration or deceleration lane. Thus, it exceeds its functional system boundaries. This leads to unpredictable behavior including intrusion into right lane.	S3	Collision with high differential velocity.	E0	Operating instructions prohibit activation of automated operation without leading vehicle.	C1	AFA drifts slowly (e. g. 0.4 m/s lateral) into right driving lane. Following traffic is easily able to recognize this and react appropriately (braking, avoiding).	QM	SG15
47	Follow Mode	Radio communication	Vehicle leaves range of radio communication	*No Hazard: Interruption of radio communication causes transition to* Safe Halt. *AFA stops on hard shoulder with active warning device.*	S0	—	E0	—	C0	—	QM	—

Continued on next page

ID: Identifier for hazardous scenario as in original document, S: Severity* (S0–S3), E: Exposure* (E0–E4), C: Controllability* (C0–C3), A: ASIL Rating (QM, ASIL A–D), SG: ID of Safety Goal (cf. Table I); *For reference cf. [2, Part 3] and [11]

TABLE II: Continued from previous page

ID	Operating Mode	Function	Malfunction	Hazardous Scenario and Consequence	S	Rationale	E	Rationale	C	Rationale	A	SG
48	Follow Mode	Operating mode change	Intended and permitted transition to *Safe Halt* is not executed	Truck convoy on right lane. AFA must transit to *Safe Halt*, e. g. due to exceeding a functional system boundary. transition to *Safe Halt* does not function. AFA exceeds functional system boundaries. This leads to unpredictable behavior including intrusion into right lane (e. g. oscillating steering angle control). Truck avoids AFA, following truck touches AFA as the AFA is masked by first truck.	S2	Collision with high differential velocity, vehicles slightly touch.	E4	Operation on hard shoulder occurs on each deployment.	C2	AFA drifts slowly (e. g. 0.4 m/s lateral) into right driving lane. Despite of masking by truck in front, following traffic is normally able to recognize this and react appropriately (braking, avoiding).	B	SG02
48a	Follow Mode	Operating mode change	Intended and permitted transition to *Safe Halt* is not executed	Moving car traffic on right lane. AFA must transit to *Safe Halt*, e. g. due to exceeding a functional system boundary. transition to *Safe Halt* does not function. AFA exceeds functional system boundaries. This leads to unpredictable behavior including intrusion into right lane (e. g. oscillating steering angle control). Car on right lane collides with visible AFA.	S3	Collision with high differential velocity.	E4	Operation on hard shoulder occurs on each deployment.	C1	AFA drifts slowly (e. g. 0.4 m/s lateral) into right driving lane. Following traffic is easily able to recognize this and react appropriately (braking, avoiding).	B	SG02
49	Follow Mode	Operating mode change	Intended and permitted transition to *Manual Mode* is not executed	*No Hazard: Only for testing purposes. Driver can stop AFA pneumatically by foot brake.*	S0	—	E0	—	C0	—	QM	—
50	Follow Mode	Radio communication	Vehicle drives without radio communication	*No Hazard: Detection of lane markings and obstacles as well as HMI function as intended. AFA stops when leading vehicle stops according work instructions before passing acceleration or deceleration lanes. Then, malfunction becomes obvious by missing transition to* Coupled Mode.	S0	—	E0	—	C0	—	QM	—
51	Follow Mode	Longitudinal guidance	Vehicle exceeds maximum speed of 12 km/h	Truck convoy on right lane. The functional components are designed for velocities up to 12 km/h. AFA drives at not excessively higher velocity. AFA exceeds functional system boundaries. This leads to unpredictable behavior including intrusion into right lane (e. g. oscillating steering angle control). Truck avoids AFA, following truck touches AFA as the AFA is masked by first truck.	S2	Collision with high differential velocity, vehicles slightly touch.	E4	Operation on hard shoulder occurs on each deployment.	C2	AFA drifts slowly (e. g. 0.4 m/s lateral) into right driving lane. Despite of masking by truck in front, following traffic is normally able to recognize this and react appropriately (braking, avoiding).	B	SG11
51a	Follow Mode	Longitudinal guidance	Vehicle exceeds maximum speed of 12 km/h	Moving car traffic on right lane. The functional components are designed for velocities up to 12 km/h. AFA drives at not excessively higher velocity. AFA exceeds functional system boundaries. This leads to unpredictable behavior including intrusion into right lane (e. g. oscillating steering angle control). Car on right lane collides with visible AFA.	S3	Collision with high differential velocity.	E4	Operation on hard shoulder occurs on each deployment.	C1	AFA drifts slowly (e. g. 0.4 m/s lateral) into right driving lane. Following traffic is easily able to recognize this and react appropriately (braking, avoiding).	B	SG11
52	Follow Mode	Lateral guidance	Steering angle change beyond maximum specification (angle & change rate)	AFA drifts with up to maximum possible yaw rate into right lane.	S3	Collision with high differential velocity.	E4	Operation on hard shoulder occurs on each deployment.	C3	AFA drifts quickly (e. g. $\gg$0.4 m/s lateral) into the right lane. It follows a circular arc to the guardrail on the left of the left lane. This is difficult to control by traffic participants.	D	SG03

Table concluded — ID: Identifier for hazardous scenario as in original document, S: Severity* (S0–S3), E: Exposure* (E0–E4), C: Controllability* (C0–C3), A: ASIL Rating (QM, ASIL A–D), SG: ID of Safety Goal (cf. Table I); *For reference cf. [2, Part 3] and [11]