2016 IEEE Intelligent Vehicles Symposium (IV)
Gothenburg, Sweden, June 19-22, 2016

Identification of Potential Hazardous Events for an Unmanned Protective Vehicle

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

***Abstract*—The project *Automated Unmanned Protective Vehicle for Highway Hard Shoulder Road Works* (aFAS) aims to develop an unmanned protective vehicle to reduce the risk of injuries due to crashes for road workers. To ensure functional safety during operation in public traffic the system shall be developed following the ISO 26262 standard. After defining the functional range in the item definition, a hazard analysis and risk assessment has to be done. The ISO 26262 standard gives hints how to process this step and demands a systematic way to identify system hazards. Best practice standards provide systematic ways for hazard identification, but lack applicability for automated vehicles due to the high variety and number of different driving situations even with a reduced functional range. This contribution proposes a new method to identify hazardous events for a system with a given functional description. The method utilizes a skill graph as a functional model of the system and an overall definition of a scene for automated vehicles to identify potential hazardous events. An adapted Hazard and Operability Analysis approach is used to identify system malfunctions. A combination of all methods results in operating scenes with potential hazardous events. These can be assessed afterwards towards their criticality. A use case example is taken from the current development phase of the project aFAS.**

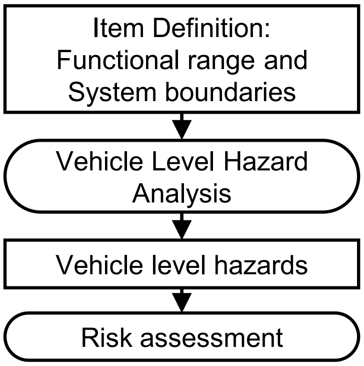

Fig. 1. Concept phase of ISO 26262 standard (simplified) with process steps (rounded) and work products (cornered) [2, Part 3]

I. Scope of work

The project *Automated Unmanned Protective Vehicle for Highway Hard Shoulder Road Works* (aFAS[1]) aims to develop an unmanned protective vehicle to reduce the risk of injuries by crashes for road workers. The unmanned protective vehicle follows a leading vehicle in a defined distance on the hard shoulder of a highway without a safety driver or human supervision. On- and off-ramps are passed in very close distance to the leading vehicle. A detailed outline of the project aFAS and the main objectives are described in [1]. Despite the operation on a hard shoulder of a highway this project aims to show the first operation of an unmanned vehicle in public traffic on German roads. Due to safety criticality the system shall be developed applying the ISO 26262 standard [2] for ensuring functional safety. The project is currently in the concept phase of the reference development process proposed by the ISO 26262 standard, which is shown in Figure 1. After defining the range of features and the functional system boundaries in the *item definition*, the system is inspected with regards to criticality during operation and the risk to other traffic participants in the *hazard analysis and risk assessment* (HARA). The first step of the HARA is the scene analysis (for a definition of the term scene see [3] and Section IV-C), which shall identify operational scenes where malfunctioning behavior of the system can lead to mishaps which are called potential hazardous events. The ISO 26262 standard uses the term situation which equals the term scene defined in [3] and is called *scene* for this contribution. These scenes thus describe the correct use and the misuse of the item in a foreseeable way. A methodology for the identification of such scenes is the main focus of this contribution.

According to the ISO 26262 standard, the hazardous events "shall be determined systematically by using adequate techniques" and "based on the item's functional behaviour; therefore, the detailed design of the item does not necessarily need to be known." [2, Part 3] The proposed techniques are brainstorming, checklists, quality history, Failure Mode and Effects Analysis (FMEA) and field studies [2, Part 3]. Due to the variety of operational situations, non-structured brainstorming and checklists do not seem to be a legitimate way for covering all relevant situations. A quality history or field studies are not available because the *unmanned protective*

[1] German abbreviation for *Automatisch fahrerlos fahrendes Absicherungsfahrzeug für Arbeitsstellen auf Autobahnen*

978-1-5090-1821-5/16/$31.00 ©2016 IEEE

vehicle will be the first of its type, therefore examples of current protective vehicles can be used as a base. It has to be noticed that the major difference that no human operator is available in the vehicle leads to other (more or different) hazardous events. The classical FMEA needs a detailed design of the analyzed system, which per definition is not available in the concept phase. A review of the ISO 26262 standard by Van Eikema Hommes points out that “the lack of guidance on hazard identification and elimination hinders the standards ability to sufficiently provide safety assurance” [4]. For these reasons this contribution proposes a novel systematic method for the identification of potential hazardous events for the unmanned protective vehicle.

II. Understanding of the Term Hazard for Automated Vehicles

The ISO 26262 standard defines a hazard as “potential source of harm (1.56) caused by malfunctioning behavior (1.73) of the item (1.69)”, where *harm* is “physical injury or damage to the health of persons”. *Malfunctioning behavior* is defined as a “failure (1.39) or unintended behavior of an item (1.69) with respect to its design intent” [2, Part 1]. According to Ericson [5] a hazard is a “before” state which transits to a mishap (or accident) through hazardous components and risk factors (Fig. 2). Ericson further states that a hazard consists of *hazardous elements*, *initiating mechanisms* and *targets* in the so called hazard triangle (Fig. 3). Following this definition and structure of a hazard, the malfunctioning behavior results from hazardous elements. These elements cause mishaps because of initiating mechanisms (hazardous events). The main objective of the HARA is to identify all components of the triangle and afterwards to remove or mitigate at least one of the components for each hazardous event in the functional safety concept.

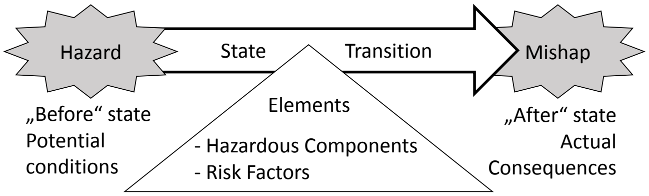

Fig. 2. Coherence of hazard and mishap according to [5]

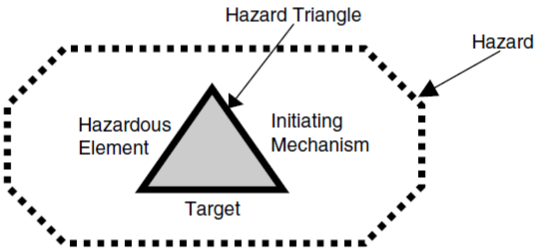

Fig. 3. Hazard triangle [5]

Applying these definitions to vehicle guidance systems, the targets are other traffic participants and occupants of an automated vehicle. There are three types of targets as ISO 26262 standard defines harm as damage or injury to persons: other vehicles including occupants, cyclists and pedestrians. The physical hazardous element is kinetic energy of the host vehicle and other traffic participants. This energy is influenced or regulated by functions, which are provided by the system. Because there is no detailed technical solution available in the concept phase of development, functions are meant as an abstract description and not implemented functions. The initiating mechanisms can be a malfunctioning behavior of the system or operation of the vehicle guidance system outside its functional system boundaries including the operational environment and weather. Malfunctioning behavior itself cannot cause any harm without a scene including the environment of the vehicle which it is operating in. To complete the representation of a hazard, the whole scene or at least the relevant components around the vehicle have to be described. This information can be taken or generated from the item definition and serve as input for the hazard analysis.

III. Related Work

The related work in the field of hazard analysis and hazard identification for automated vehicles is separated into two sections, because there is some recent work and many standards available. The recent work provides an overview of current activities regarding the ISO 26262 standard and the traditional techniques section lists related standards.

A. Recent work

Different authors [6] [7] propose the scene-situation-matrix to identify hazardous events, but provide no method how to generate a complete set of relevant scenes for the item except expert knowledge in brainstorming. This matrix can be used as a preliminary hazard identification method which contains a first guess of the system-risk. Luo et al. [8] propose a modeling approach for safety case reasoning which covers hazardous events but do not mention how these events are generated. Cuenot et al. [9] provide a model based-safety analysis for the system development phase in the ISO 262626 standard [2, Part 4]. The system development phase is based on the concept phase and provides a detailed system design. But it needs a functional safety concept to implement, which is derived from the HARA and the safety analysis in the concept phase. Concluding the recent publications in the automotive domain, there seems to be potential towards systematic identification of hazards based on a functional system description.

B. Traditional hazard analysis techniques

1) Hazard and Operability Analysis (HAZOP):

The Hazard and Operability Analysis (HAZOP) is a structured technique for examining a defined system, with the objective of identifying potential hazards in the system and identifying potential operability problems with the system [10]. Originally developed by the Institute of Chemical

Industry (ICI) in the early 1970s [11], HAZOP studies were intended to analyze chemical plants. Over the years HAZOP was applied to other fields like nuclear power plants, the petroleum industry, food and water industries and railways. The key idea of HAZOP is to bring an interdisciplinary team together to assess proposed system deviations which are generated by combining an item with system parameters and specified guide words. An example is a valve which generates too much flow, where *valve* is the item, *flow* is the parameter and *too much* are the guide word(s). The HAZOP method seems not to be applicable to vehicular systems without any modifications, because there are no guide words for the specific tasks of an automated vehicle available in the standard.

2) Failure Mode and Effects Analysis (FMEA):

The Failure Mode and Effects Analysis (FMEA) is used to identify effects on the operability of the system caused by failures in subsystems, hardware components or system functions [12]. Originally developed by the U.S. military in 1949 [5], the standard was adapted for the automotive industry by the Ford Motor Company and was consolidated in 1993 by the Automotive Industry Action Group (AIAG). Ericson [5] describes an analysis based on a functional model which describes *what* the system does and not *how* the functions are implemented in hard- and software. This design FMEA (DFMEA) should be initiated right after the project start and during the concept phase. DFMEA depends on design-responsibility, interfaces and interactions and the architecture of the system. The architecture can be expressed with block diagrams, interface diagrams, functional diagrams, structure trees and schematic illustrations. The item definition provides the information to get a functional model for the item under investigation. Based on this information the system functions (e.g. transforms, operates, contains) are expressed by requirements. The analysis process identifies which components can fail and how this failure affects the requirements. “The effects of the failure mode should be considered against the next level up assembly, the final product, and the end customer when known.”[12] The difficulty for a driverless vehicle at the system level is to identify a complete or at least representative set of scenes where the effects can be investigated. The (D)FMEA does not cover effects on the environment but can give hints how the system fails.

3) Fault Tree Analysis (FTA):

The Fault Tree Analysis (FTA) is a deductive method for finding (basic) causes for unwanted events (malfunctions or malfunctioning behavior) in the system. For this analysis a given effect of a system failure is analyzed in a Fault Tree to identify the components which can cause the effect [13]. The FTA can be used to assess which components in the system can cause the malfunctioning behavior in a hazardous event. Fault Trees are derived from a detailed system design and are developed mainly for hardware analysis and a calculation of fault rates. The functional safety concept, which is developed after the HARA, then shall mitigate or prevent failures in the identified system components.

4) Event Tree Analysis (ETA):

The Event Tree Analysis (ETA) builds Event Trees, which are investigated according to the effect on the system (item) [14]. This method evaluates if the implemented safety mechanisms reduce or prevent the hazard from occurring. The ISO 26262 standard demands from the hazard analysis and risk assessment that it should be processed without “safety mechanisms intended to be implemented or that have already been implemented in predecessor items shall not be considered” [2, Part 3]. The ETA can be used to assess whether a functional safety concept is able to prevent or mitigate hazardous events but not to identify them.

IV. Approach for identification of potential hazardous events

This section introduces the novel approach for identifying potential hazardous events (cf. Fig 4). The following parts show which entities were chosen to identify the events for the described unmanned protective vehicle. A hazardous event consists of the current operating mode which is performed, a function with a specific malfunction and the current scene around the vehicle. The next sections show how to identify these parts systematically and which values were chosen for the identification in the project aFAS.

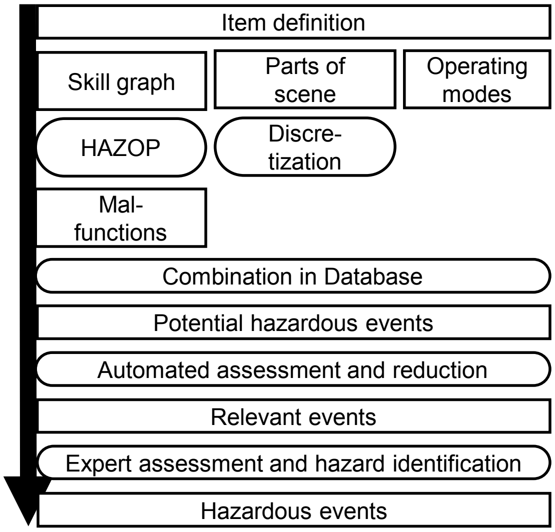

Fig. 4. Proposed methodology for identification of potential hazardous events with work products (cornered) and process steps (rounded)

A. Operating Modes

The vehicle guidance system of the unmanned protective vehicle is planned to operate in four modes [1]. The first one is the *Manual Mode*, in which the unmanned protective vehicle is controlled by a human and acts like a normal vehicle. There is no operation of the vehicle guidance system in this

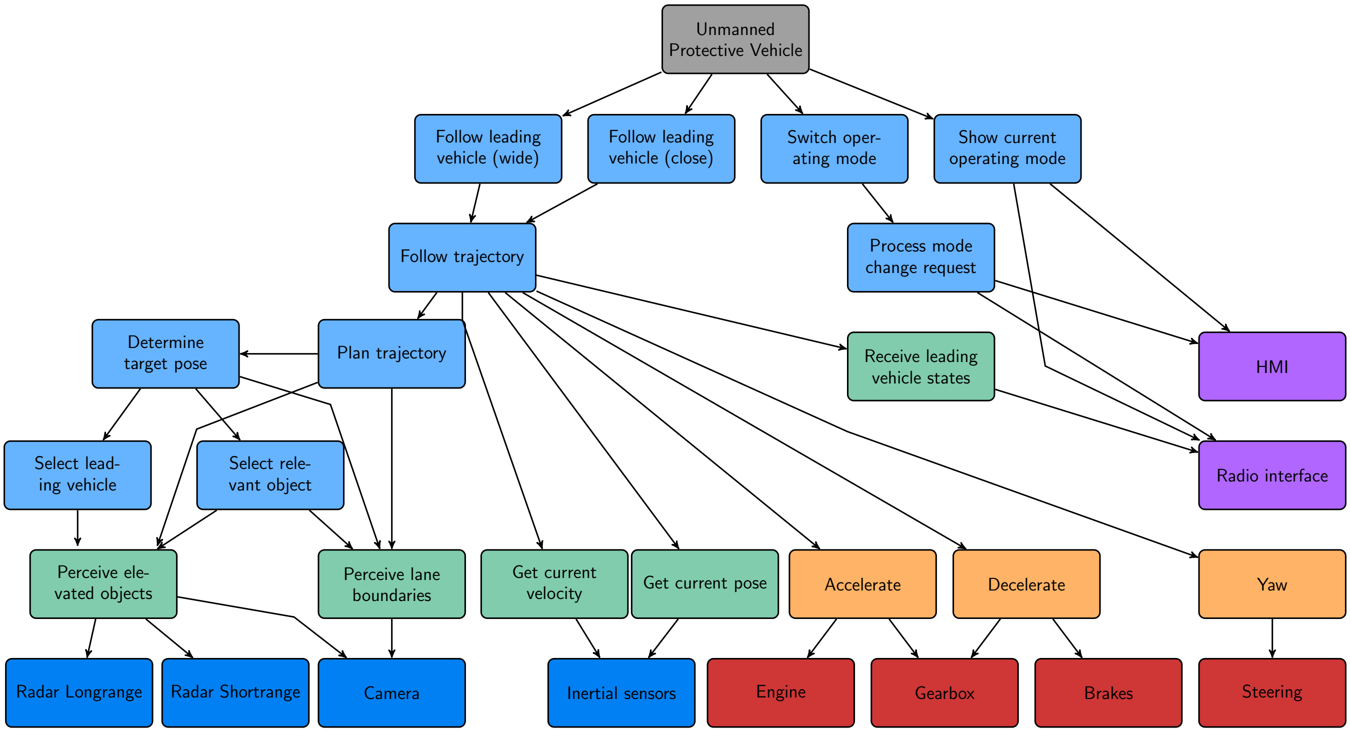

Fig. 5. Skill graph of the unmanned protective vehicle categorized in main (grey), perception (green), planning (light blue), action (orange), sensors (blue), actuators (red) and input-output (purple), HMI: Human Machine Interface

mode. When the unmanned protective vehicle is located at the working spot, the mode has to be switched to *Safe Halt*. In this mode the vehicle comes to a stop within the smallest possible distance or stands still. This is used as the operational safe mode in case of a system failure or to start automated operation. The automated driving functions are operated in *Follow Mode* and *Coupled Mode*. Passing of acceleration and deceleration lanes is done in the *Coupled Mode*, in which the unmanned protective vehicle drives with a very small gap between the two vehicles. In this mode the leading vehicle's current states of actuators are sent to the unmanned protective vehicle via the radio interface to enable the operation in such close gaps. This functionality is based on the work of the KONVOI [15] project. *Follow Mode* is planned to be the main operation. In this mode the unmanned protective vehicle has a gap of about 100 m to the leading vehicle. It acts like an adaptive cruise control with stop and go feature and follows the hard shoulder like a lane keeping system.

B. Functions and malfunctions

According to Fig. 1 the item definition is the input for the HARA defining the unmanned protective vehicle in a functional way including system boundaries and operational environment. From this informal document a skill graph, which describes the functionality with all dependencies, can be created. In this case a skill is an abstract description of an activity which the system has to provide to fulfill the intended task [16]. The item definition describes a system by the functional behavior and the system goals or mission. Note that there should be no technical concepts in this part of the development process. The system goals can then be divided into several sub-activities which have dependencies on each other. For example has the task *following a lane* dependencies on *perceiving a lane* and *control the vehicles dynamic state*. By modeling skills in a graph the system can be described from top-level goals or purpose over functional (and non-technical) dependencies to bottom sinks and sources which describe system boundaries. Reschka et al. investigated the concept of skill graphs for appliance in vehicle guidance systems [17]. Note that the terms skills and abilities were interchanged. Fig. 5 shows the resulting skill graph, which was extracted from the item definition. For the purpose of describing vehicle guidance systems, the skills are separated into seven different categories:

- System skill (grey)
- Sensors (blue)
- Actuators (red)
- Input-Output (e.g. HMI) (purple)
- Perception skills (green)
- Planning skills (light blue)
- Action skills (orange)

The main or system skill describes the system itself and covers the overall functionality. The underlying skills describe the system in a hierarchical way. Beginning from the main tasks (following the lead vehicle and switching operating modes) in the different operating modes. Skills are connected with arrows showing their dependencies to each other. For example the skill *select relevant object* has dependencies on a skill which perceives the object and another which perceives the hard shoulder boundaries to identify if an object is relevant or not.

To identify possible malfunctions we use the categorization of skills in combination with an adopted HAZOP methodology. Hwang and Jo [18] used a modified *HAZOP-R* (Railway) method in combination with a Preliminary Hazard Analysis (see [5, chap. 5]) to identify hazardous events for a railway signaling system. Trains mainly differ from vehicles because they are moving on rails and are coordinated by a central system. In our adaption the HAZOP-*item* is one skill of the categories perception, planning or action. The system parameters have to be defined according to the chosen skill. For example *Perceive objects* has parameters like *relative position*, *extent* and *speed* for detected objects. At this point we introduce keywords for the skill categories as follows:

- Perception skills: No, nonexistent, erroneous, too large, too small
- Planning skills: Not relevant, Relevant {*parameter e.g. object*} not, conflicting, physically not possible
- Action skills: Absent, wrong, unattended, too large, too small

We used the keywords to generate possible malfunctions for each skill in combination with a parameter of the skill. For example, we used *plan trajectory* (skill) planned a *physically not possible* (keyword) *turn rate* (parameter) in the trajectory. The chosen categories fit for the reduced use case and system complexity of the unmanned protective vehicle. Vehicle guidance systems with a wider functional range may need more detailed categories to declare usable guide words.

C. Scenes

Ulbrich et. al [3] recently reviewed many definitions of the term *scene* and defined a consolidated definition as:
"A scene describes a snapshot of the environment including the scenery and dynamic elements, as well as all actors and observers self-representations, and the relationships among those entities. Only a scene representation in a simulated world can be all-encompassing (objective scene, ground truth). In the real world it is incomplete, incorrect, uncertain, and from one or several observers points of view (subjective scene)."
Thus, a scene consists of the three main parts *dynamic elements*, *scenery* and *self-representations of actors and observers* as shown in Fig. 6. For the purpose of defining scenes for the unmanned protective vehicle we chose the following entities:

- Road infrastructure
- Road infrastructure width
- Road infrastructure curvature
- Traffic constellation
- Maximum velocity of moving traffic
- Weather conditions
- Object constellation on hard shoulder
- Driving state of the unmanned protective vehicle
- Malfunction as part of self-representation

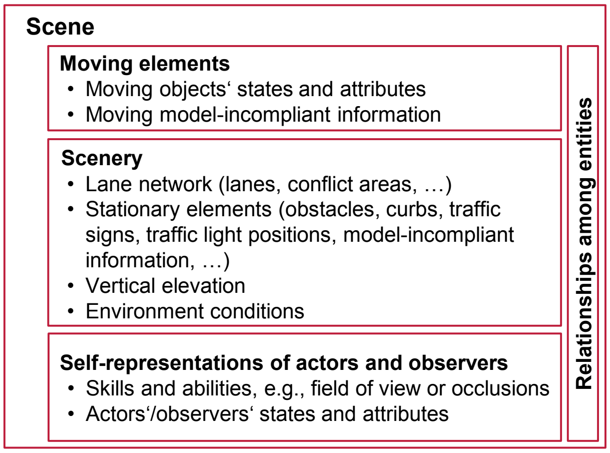
Scene
Moving elements
• Moving objects' states and attributes
• Moving model-incompliant information
Scenery
• Lane network (lanes, conflict areas, …)
• Stationary elements (obstacles, curbs, traffic signs, traffic light positions, model-incompliant information, …)
• Vertical elevation
• Environment conditions
Self-representations of actors and observers
• Skills and abilities, e.g., field of view or occlusions
• Actors'/observers' states and attributes
Relationships among entities

Fig. 6. Parts of a scene according to [3]

The selected entities describe the operational environment for the reduced operating scenario of the unmanned protective vehicle and were identified by using information from the item definition. Road infrastructures are described by a right and a left infrastructure in relation to the unmanned protective vehicle. We added additional information to the scenes which exceed the functional system boundaries according to the item definition. This will be used to identify potential hazardous events, in which the vehicle has no malfunctions but is operated outside these boundaries. These scenes can lead to mishaps without a malfunction or functional error and can be declared as a system boundary consideration. The next challenge is to choose a level of discretization for each component of the scene. As the hazard identification aims at generating top-level system hazards, we chose to use nearly binary discretization. Choosing an appropriate level of discretization is a crucial step because too-detailed scenes can distort the risk assessment. Very detailed scenes are more improbable than top level scenes and result in a lower exposure rating and this leading to a lower *automotive safety integrity level* (ASIL) [2, Part 3] classification. We choose a high level of discretization because the generated scenes shall provide a base for an expert team predicting the systems behavior in a given scene. In our case the road infrastructures have *solid markings*, *dashed markings*, *guardrails* and *turf*. The infrastructure width, infrastructure curvature and the weather conditions were set to *valid* or *invalid*. The traffic constellation and the maximum velocity is chosen to *moving traffic* with *no limitation* according to the item definition. The object constellation on the hard shoulder can contain *no object*, *solid object* (like a car) or *vulnerable object*. The driving state of the unmanned protective vehicle is either *stopped*, *driving at 10 km/h* or *driving at 80 km/h*. This level of detail allows a very simplified and qualitative consideration of the operational scenes.

D. Database

After identifying all necessary components to describe events we have to generate the potential hazardous events. For this step we created a SQL-database, where a permutation of all scenes is stored. To analyze only relevant events, the database filtered scenes with following the constraints:

- the function is not performed in the operating mode,
- multiple failures or functional system boundary exceeding or a combination of both exist,
- the malfunction is not relevant in scene (e.g. relevant object not considered in the scene where no objects are in place).

In conformity with the ISO 26262 standard, multiple failures are not selected as relevant. A functional system boundary exceedance is interpreted as a single failure for this contribution. The relevant potential hazardous events then give an operating scene of the vehicle with a malfunction or system boundary exceeding in a defined operating mode as shown in Table I.

TABLE I
EXAMPLE OF A POTENTIAL HAZARDOUS EVENT

Mode	Follow Mode
Function	Select relevant object
Malfunction	Relevant object not considered
Road infrastructure	Solid line (left) and turf (right)
Object constellation	Vulnerable object
Curvature, width and weather	valid
Traffic constellation	Moving traffic with no limitation
Driving state	Driving at 10 km/h

The scene in Table I was classified as *hazardous* because the vulnerable object, which can be either a human or an animal, would be injured if the vehicle does not stop. Based on these hazardous events, the top-level system hazards can be identified and afterwards be assessed in the risk assessment step of the HARA.

V. RESULTS

The number of scenes created for the unmanned protective vehicle according to the discretization from Section IV-C is 145 with 108 scenes classified as relevant. This classification is based on whether there is no or only one system boundary exceedance. We identified 16 functions with 37 malfunctions and the four operating modes for creation of the potential hazardous events. Table II shows the numbers of generated and filtered events of the database. The great decrease after filtering all generated events to relevant events can be explained by four factors shown in Table III. The first point of automated reduction is decided by whether a specific function is operated in a certain operating mode. In Manual Mode a roadworker is driving the unmanned protective vehicle like a normal truck, thus only acting skills are used in Manual Mode and the number of relevant events is significantly reduced. Safe Halt and Coupled Mode are using a reduced set of system functionality as both do not perceive lane boundaries and Safe Halt not even objects.

TABLE II
NUMBERS OF GENERATED AND CLASSIFIED EVENTS

Mode	**Events**	**Relevant**	**Hazardous**
Manual Mode	5328	373	238
Safe Halt	5328	344	105
Follow Mode	5328	377	170
Coupled Mode	5328	368	237

TABLE III
MAJOR FACTORS OF FILTERING RELEVANT EVENTS

The function with a specific malfunction is not performed in operating mode			
Manual Mode	Safe Halt	Follow Mode	Coupled Mode
2592	864	0	648
Only one malfunction or system boundary exceedance is allowed			
Manual Mode	Safe Halt	Follow Mode	Coupled Mode
864	720	1296	864
The combination of malfunction and scene is (physically) invalid			
Manual Mode	Safe Halt	Follow Mode	Coupled Mode
1331	666	666	666
Scene is not relevant for operating mode			
Manual Mode	Safe Halt	Follow Mode	Coupled Mode
0	2664	2664	2664

Second influence on the number of relevant events is the selection of only one malfunction or system boundary exceedance. This criterion comes from the ISO 26262 standard where only single point of failures are considered. The number of relevant events will increase significantly, if two or more malfunctions are evaluated.

Due to automated generation of the events without any physical or formal modeling, there are plenty of events which are (physically) not possible or just not meaningful. For example is an event with the malfunction *existing object not recognized* in a scene where *no object* is located on the hard shoulder not meaningful.

Last of all some scenes are not possible for some operating modes. The reduction of 2664 events in all automated operating modes is explained by scenes where the velocity of the unmanned protective vehicle is at 80 km/h. This state is only relevant for Manual Mode as the maximum velocity in the automated modes is limited to 10 km/h.

The relevant events then were assessed by a team of experts as to whether they are hazardous or not. We can not provide proof of completeness since the development process is still on-going and to the best of our knowledge there is no measure for completeness. For validation purposes, a next step is to compare the resulting hazards from this approach with the identified hazards by a team of experts.

VI. CONCLUSION AND FUTURE WORK

The generated potential hazardous events and the (plausibility) filtering in a database result in a systematic way to identify top level system hazards for an unmanned protective vehicle with a very limited use case but the first planned unmanned operation in public traffic. A drawback of the proposed method is that there are several events leading to the same hazards and the same ASIL classification. For example the infrastructure width does not have any impact on how the actuating skills, like accelerating the vehicle, perform. This topic can be addressed by using equivalence classes for parts of a scene towards selected skills and with this reduce the total number of events by not loosing information about critical events. A difficulty in choosing equivalence classes is to prove that no potential hazardous event is omitted. These equivalence classes could be identified by having a look at skill categories with regard to single parts or categories of the overall scene definition. Another focus is to extend this method for vehicle guidance systems with a wider use case, like the project *Stadtpilot* [19]. The first step for this purpose is to generate an item definition and to describe the operational environment in inner cities. Due to the situational complexity of this environment the functions for evaluating and reducing the total number of events must be extended because there is a huge amount of possible events.

Acknowledgment

We would like to thank our partners from the project consortium consisting of MAN Truck - Bus AG (consortium leader), TRW Automotive GmbH (ZF TRW), WABCO Development GmbH, Robert Bosch Automotive Steering GmbH, Hochschule Karlsruhe, Technische Universität Braunschweig, Hessen Mobil - Road and Traffic Management, and BASt - Federal Highway Research Institute for their support. The project is partially funded by the German Federal Ministry for Economic Affairs and Energy.

References

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

[2] *Road vehicles – Functional safety*, ISO Std. 26 262, 2011.

[3] S. Ulbrich, T. Menzel, A. Reschka, F. Schuldt, and M. Maurer, "Defining and substantiating the terms scene, situation, and scenario for automated driving," in *18th IEEE International Conference on Intelligent Transportation Systems*, Las Palmas, 2015, pp. 982–988.

[4] Q. Van Eikema Hommes, "Review and Assessment of the ISO 26262 Draft Road Vehicle - Functional Safety," in *SAE Technical Paper*. SAE International, 2012.

[5] C. A. Ericson, *Hazard analysis techniques for system safety*. Hoboken: Wiley-Interscience, 2005.

[6] H.-L. Ross, *Funktionale Sicherheit im Automobil* - English title: Automotive functional safety. München: Hanser, 2013.

[7] M. Ito and K. Kishida, "An approach to manage the concept phase of ISO 26262," *Journal of Software: Evolution and Process*, vol. 26, no. 9, pp. 829–836, Sep. 2014.

[8] Y. Luo, M. van den Brand, L. Engelen, and M. Klabbers, "A modeling approach to support safety assurance in the automotive domain," in *Progress in Systems Engineering*, ser. Advances in Intelligent Systems and Computing, H. Selvaraj, D. Zydek, and G. Chmaj, Eds. Springer International Publishing, 2015, vol. 330, pp. 339–345.

[9] P. Cuenot, C. Ainhauser, N. Adler, S. Otten, and F. Meurville, "Applying model based techniques for early safety evaluation of an automotive architecture in compliance with the ISO 26262 standard," in *Embedded Real-Time Software and Systems 2014, ERTS*, Florent, France, 2014, pp. 318–329.

[10] *Hazard and operability studies (HAZOP studies): application guide*, BS IEC Std. 61 882, 2001.

[11] H. G. Lawley, "Operability studies and hazard analysis," *Chemical Engineering Progress*, vol. 70, no. 4, p. 45, 1974.

[12] *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*, BS IEC Std. 60 812, 2006.

[13] *Fault tree analysis (FTA)*, IEC Std. 61 025, 2006.

[14] *Analysis techniques for dependability - Event tree analysis (ETA)*, IEC Std. 62 502, 2010.

[15] S. Deutschle, G. C. Kessler, C. Lank, G. Hoffmann, M. Hakenberg, and M. Brummer, "Use of electronically linked konvoi truck platoons on motorways," *ATZautotechnology*, vol. 10, no. 4, pp. 20–25, 2010.

[16] A. Reschka, "Fertigkeiten- und Fähigkeitengraphen als Grundlage für den sicheren Betrieb von automatisierten Fahrzeugen in städtischer Umgebung - *English title: Skill and ability graphs as basis for safe operation of automated vehicles in urban environments*," Ph.D. dissertation, Technische Universität Braunschweig, 2016, announced.

[17] 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)*, Seoul, Korea, Jun. 2015, pp. 933–939.

[18] J. G. Hwang and H. J. Jo, "Hazard Identification of Railway Signaling System Using PHA and HAZOP Methods," *International Journal of Automation and Power Engineering (IJAPE)*, vol. 2, no. 2, 2013.

[19] T. Nothdurft, P. Hecker, S. Ohl, F. Saust, M. Maurer, A. Reschka, and J. Bohmer, "Stadtpilot: First fully autonomous test drives in urban traffic," in *2011 14th International IEEE Conference on Intelligent Transportation Systems (ITSC)*, Washington, DC, Oct. 2011, pp. 919–924.