Definition and identification of system boundaries of highly automated driving

David Wittmann
Institute of Automotive Technology
Technische Universität München
Garching, Germany
Email: wittmann@ftm.mw.tum.de

Cheng Wang
AUDI AG
Ingolstadt, Germany
Email: cheng.wang@audi.de

Markus Lienkamp
Institute of Automotive Technology
Technische Universität München
Garching, Germany
Email: lienkamp@ftm.mw.tum.de

***Abstract*—The safety of a highly automated driving system depends firstly on the specified system behavior including the behavior on functional system boundaries and secondly on the handling of system errors in the sense of deviations in the specification. The proposed safety evaluation considers these two aspects. A specification space is introduced to enable a clear definition and derivation of possible functional system boundaries based on traffic scenarios. A two-staged surveillance concept is presented to handle uncertainties in boundary detection. The method is illustrated by an exemplary derivation of functional system boundaries.**

I. Introduction

Automated and autonomous driving captured a remarkable amount of the automotive concerned headlines in recent years. On one hand this attention is caused by the potential fulfillment of a human vision. On the other hand the entrance of large and public known technology companies widened public interest. The presence of the subject increased the expectations of customers, awaiting automated driving systems available in all possible situations. While the potential customer focuses mainly on the availability of such systems, the manufacturer has to consider the safety and its validation. The challenges and requirements in these topics essentially depend on the level of automation, often mixed up in public perception.

Considering the implementation of highly automated driving (following the definition of German BASt [1], respectively SAEs conditional automation [2]), which has the goal to release the driver from his surveillance task, all relevant functional boundaries have to be detected by the system. Only if all functional system boundaries are handled properly, a safe operation of such system is possible.

To handle the whole complexity of this topic, it is suggested to handle the system boundaries for automated driving as follow. Firstly, all relevant boundaries have to be identified, which is a challenging task since a highly automated car is a complex system, navigating through a complex environment. Secondly, a specific definition is needed to enable a traceable description required for safety related documentation. And last but not least sufficient strategies to detect and to react or avoid these functional system boundaries have to be developed.

The remainder of the paper is organized as follows. In the following chapter a general approach for safety evaluation for highly automated vehicles is presented and the role of functional system boundaries within is stated. Next related work concerning functional system boundaries of automated driving as well as definition of traffic scenarios is presented. Following a specification space is introduced which enables a structured description of functional system boundaries. Based on these considerations a two-staged surveillance concept is proposed in chapter VI. In chapter VII potential functional system boundaries of an exemplary highly automated highway application are derived, followed by a conclusion and outlook on the following work.

II. General concept for safety evaluation

The development of a safety concept for automated driving is based on a comprehensive evaluation of possible risks, caused by the system, since safety is the ”absence of unreasonable risk” ([3, p.14]). The definition of unreasonable risk depends on ”valid societal moral concepts” ([3, p.18]) and has to be discussed ethically and juridically , which is out of scope this concept.

Next to this theoretical discussion, the risk of a system should be ”as low as reasonable practicable” (ALARP) [4, p.16]. To achieve this goal and to guide this process, safety standards exist for specific scopes. For example the safety standard considering functional safety of E/E-components in the automotive domain is ISO26262 [3]. It recommends a safety life-cycle to ensure functional safety of the considered item. In the concept phase the following proceeding is defined. Based on a specific item definition the risk caused by functional failures is analyzed and needed measures to reduce the risk of these failures are derived based on Automotive Safety Integrity Levels (ASIL) [5].

But the risk caused by a highly automated driving system exceeds the scope of the ISO26262, since additional sources of harm are relevant apart from malfunctioning behavior of E/E components considered in the norm. These sources can be exemplary the failure of mechanical components of the car or performance limitations of the perception of environment. Therefore we present an approach for comprehensive safety evaluation.

To handle the different sources of risk, two main categories are defined. Firstly, whether the system acts as specified and therefore is within the defined functional system boundaries. Secondly, whether system errors occurred. The detailed definition of functional system boundaries is stated in chapter IV. The system errors involve all errors which can lead to failures

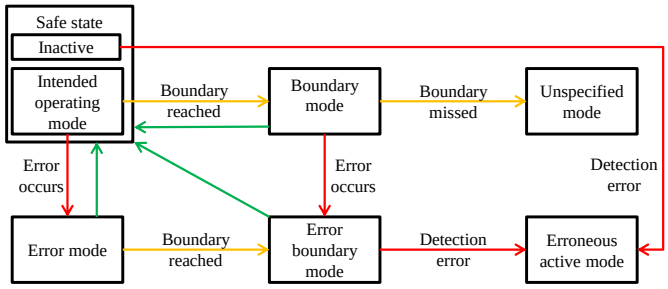


Fig. 1. Possible system modes considering the critical dimensions of system boundaries and system errors

i.e. deviations from the specified system behavior following the definition of Gietelink [6, p.44].

This separation between functional system boundaries and system errors enables a distinction of different system modes as illustrated in figure 1. Therein a transition to the right corresponds to a system boundary and a transition down corresponds to a system error. We define the intended operation mode of a system inside the functional system boundaries in the absence of system errors as part of the safe state. Following the vocabulary of ISO26262 [3] the safe state includes the intended operating mode and the inactive mode if the risk is reasonable. Consequently the boundaries have to be defined as such, that the intended operation mode is reasonable safe.

Reaching a boundary still in absence of errors leads to a transition to a boundary mode. This mode includes the specified adequate reaction on this boundary to transfer the system back to a safe state. Since some boundaries of highly automated driving can be safety critical and even the best imaginable reaction on them may not prohibit a hazard, these states can be a source for residual risk of such a system. Therefore the definition of the boundaries and reaction should be in accordance with the accepted residual risk. The unspecified mode can arise from incomplete specification of system boundaries or performance limitations. Due to infinite possible scenarios this cannot be a negligible source of residual risk.

Since the highly automated driving system can deviate from the specified behavior throughout all imaginable errors, three relevant error modes exist. The nominal error mode is reached by any system error occurring during intended operation mode. Similar to the boundary mode an adequate detection and reaction mechanism should be specified to return the system to the safe state. Even worse, system errors can occur during boundary modes, leading to a so called error boundary mode. Through the combination of a critical boundary and a system error, a safe reaction is even more challenging and therefore a higher residual risk can be expected.

Last but not least the system can be active outside the specified functional system boundaries because of system errors, named erroneous active mode. This can be caused by an activation even though not all activation requirements are fulfilled or through a not detected boundary. Since the behavior of the system in this state cannot be foreseen, it is a considerable source of risk.

A comprehensive safety concept for highly automated driving has to address all of these states. The residual risk of all states has to be evaluated and a sufficient handling and return to the safe state has to be ensured. To match the chosen definition, functional system boundaries have to be selected as such that no unreasonable level of risk exists in the intended operating mode. To enable a systematic definition and evaluation of reasonable system boundaries, this paper gives a definition of a specification space, describing all relevant scenarios and boundaries. The definition of scenario used will be detailed in chapter IV.

III. RELATED WORK

Many publications focus on possible solutions for particular system limitations of automated driving. Since this paper attempts to present an overview of possible system limitations, only such publications are mentioned in this section.

Hörwick [7] presented a general safety and watchdog concept for automated driving and therefore defined system boundaries as indicators for situations, the HAF was not designed for or cannot handle [7, p.72]. He distinguished four categories: 1) functional boundaries: depend on the functional specification of the system 2) external influences: like driver actions, environmental conditions (ice) or defect vehicle parts 3) internal errors: such as faults in hardware or software of the system and 4) situate implausibilities: a second stage surveillance detects situations which should not occur when everything works correctly. While this general clustering seems reasonable, it was just used for a few sample boundaries regarding a traffic jam pilot and not for systematic derivation of potential boundaries. Furthermore the distinction between external influences and functional boundaries can be misleading since the functional specification should include the reaction on external influences. But there is also a clear distinction between system errors (internal errors) and system boundaries.

Another list of potential functional system boundaries and detection possibilities is presented by Reschka [8] as part of the safety concept for Braunschweigs Stadtpilot project. Without further clustering five performance criteria are presented. Four of them could be dedicated to the category of system errors, namely position accuracy, viewing area, system operation status and system reaction time. The fifth criteria treats the estimated grip value. Since this safety concept is only intended to support the safety driver, no claim on completeness is necessary and the criteria are motivated by feasibility and usability.

Gietelink [6] presents methods to investigate impacts on advanced driver assistance systems (ADAS). Therefore possible disturbances and faults are listed. Impacts on ADAS are environmental and ambient conditions like ”temperature, rain, snow, light, vibration, electro mechanic disturbances and fog” [6, p.43] as well as the driver are mentioned without further methodology.

In the work mentioned functional system boundaries are listed, based on experience or feasibility. To support a complete derivation and explicit definition of functional system boundaries of highly automated driving, we propose to consider all relevant scenarios within the system could be active. There are several approaches for the description of traffic situations.

Reichart [9, p.43] defined a traffic situation a spatial and temporal constellation of the traffic relevant influence

parameters in the work environment of traffic participants. He explicitly distinguished the driving situation (objective relevant situation) and the driver situation (subjective recognized part of the driving situation) since he tried to evaluate the reliability of human drivers. Furthermore, he used a classification scheme to describe the driving situation considering type, route and traffic flow. By presenting an evaluation method for the similarity of different traffic situations, also several relevant parameters for roads, nodes and environment conditions are introduced [9, p.107-109].

Domsch [10] proposed utilization of a situation catalog based on Reicharts considerations for development, specification and evaluation of driver assistance systems. Therefore he proposes parameters for the main categories, driver, environment and vehicle.

Geyer et al. [11] developed an ontology to describe use-case and scenario catalogs. Their fundamental ontology is based on scenes, describing dynamic elements, scenery and driving instructions. The combination of scenes with the ego vehicle behavior, including potential behavior of the driver or an automation, are labeled situations. Scenarios then describe the activity of the driver or the automation and can therefore consist of one or several situation sequences. Based on this ontology Geyer describes the application of his top down approach in [12, p.44 et sqq.]. He combines all possible classes of scenery elements and then removes unreasonable combinations. Subsequently dynamic objects and the maneuver of the ego vehicle are added.

IV. DEFINITION OF FUNCTIONAL SYSTEM BOUNDARIES

The approach presented in this work for risk evaluation needs a precise description for functional system boundaries. These include a clear distinction between scenarios inside and outside the specification, since we propose a scenario based methodology (cf. [10]) for this evaluation. The concept of scenario definition is leaned on the ontology of Geyer et al. [11].

The main idea is to introduce a specification space which is able to describe all possible imaginable traffic scenarios by concurrently providing manageable complexity. Furthermore the specification space should support the derivation of critical scenarios. To fulfill these requirements, it is necessary that all possibly relevant aspects can be described in the specification space and the defined categories should be intuitive to support the consideration of all aspects while defining specific boundaries. But to provide manageable complexity, the described scenarios do not have to include every possible dimension, in contrast to Geyers ontology which is always based on static environment. By declaration of boundary scenarios a clear definition of system boundaries is enabled.

As a result the specification space $SpecS$ is defined as follows. The whole specification space contains all possible scenarios. To enable a clear description of these scenarios it encompasses five subspaces, namely static environment, traffic dynamics, environmental conditions, state of the ego vehicle and passenger actions, as visualized in figure 2.

$$SpecS := stat \times traf \times env \times egost \times psg \tag{1}$$

Within this space, all functional handled scenarios of a specific system can be enclosed by the corresponding functional system boundaries.

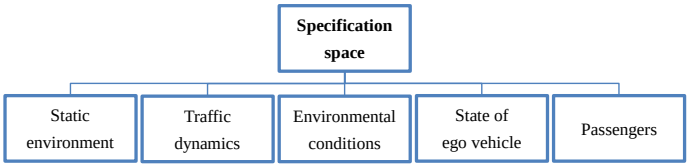


Fig. 2. Main categories of the specification space

The static environment $stat$ describes the relevant environment of the vehicle which does not change during the driving maneuver throughout this environment. The traffic dynamics $traf$ consist of the states and dynamic behavior of all active traffic participants who influence the actual scenario. Environmental conditions env cover all physical influences manipulating the static environment which can, but do not have to change during the maneuver. Since the specification space is intended to define an automated driving function, the vehicle itself is not part of the system considered and hence the vehicle state $egost$ is part of the $SpecS$. And last the passengers in the automated vehicle occupy a special role and are therefore described in psg including their interaction with the system.

These general subspaces are further subdivided in specific subcategories leading to a specification space with n dimensions. The essential point of this concept is, that a scenario can be described in the last detail by definition of all single definition parameters, but can also be stated quite generally by leaving most of them as arbitrary. Since the relevance of the parameter set depends on the considered system, the definition of these parameters of the specification space can be adapted and supplemented.

To enable the definition of complex scenarios while leaving the complexity of the specification space at a manageable level, a scenario can also be assembled by a sequence of scenes which are also defined in the specification space.

$$Scenario = ((scene_1, ..., scene_n) \mid scene_i \in SpecS \forall i); \tag{2}$$

A. Static environment

To generate an entire description of $stat$, a top down approach from a global to a local view is used. Starting with the global land mass, it can be limited by the selection of countries as a first step. Second the domain can be bounded, namely highway, rural, urban and off-road. Since off-road is not in the focus of civil development of automated driving, further parameters are derived at means of road infrastructure consisting of nodes connected by roads. Therefore one category describes the kind of nodes and another the properties of the roads. These road properties include the road profile, the static road conditions as well as the three dimensional course of the road. The effective traffic rules are directly linked to the corresponding roads and nodes. Since it may be relevant for safety evaluation, an additional category labels special cases like bridges, tunnel or roadworks.

$$stat = (country, domain, nodes, road, special) \tag{3}$$

B. Traffic dynamics

This static environment can now be overlaid by dynamic descriptions. First of all, dynamics of a scenario consists of traffic dynamics describing the traffic participants included and their behavior. Since there can be a remarkable large amount of relevant traffic participants whose behavior is strongly depending on each other and on the infrastructure, it is challenging to handle this complexity. Therefore the approach enables a scalable description and depending on the intended use of the scenario, only the most relevant dynamics from the ego vehicle viewpoint are described. Generally a dynamic scene can be described by an initial state and the transition of this state during the scene. Depending on the purpose of the scene, the behavior of an object can be defined in detail over time or only the aimed target state of the object can be given.

For an intuitive description and clustering of scene dynamics, these scenes can be described as maneuvers. There are several approaches to define a set, covering all possible maneuvers. Nagel and Enkelman [13] stated a set of 17 primitive maneuvers to describe all necessary options of an automated vehicle. Tölle [14] reduced this set to 9 maneuvers by clustering similar ones.

As can be seen, the clustering in maneuvers is not definite and since the relevant traffic dynamics are obviously strongly dependent on the driven static environment, an adaption to the defined static environment is reasonable. But the presentation of an extensive maneuver catalog supports the findings of relevant dynamics. Therefore the following clustering is proposed. The traffic dynamics can be assembled by the ego vehicle's behavior including the initial state and all directly relevant object behaviors.

$$traf = (obj_{ego}, obj_1, ...obj_N) \tag{4}$$

These behaviors can be described in the first step by the 17 primitive maneuvers mentioned of [13] for normal traffic participants. Considering other traffic participants like bicyclists and pedestrians an adapted description is needed, i.e. replacing parking maneuvers by entering or crossing the road. With this definition, also traffic lights can be considered as objects.

$$obj_x = (initialstate, maneuver) \tag{5}$$

To define possible boundary scenes, these maneuvers can be further detailed and described with concrete dynamic behavior, like deceleration values or distances in which these maneuver occur.

In addition to these general maneuvers also special scenarios exceeding the normal traffic maneuvers can occur. These include collisions, obstacles or special traffic participants like utility vehicles.

C. Environmental conditions

Additional the environmental conditions env can have a remarkable influence on the drivability of a specified scenario. Therefore friction, sight conditions, temperature, wind and potential coverings of static environment has to be defined in this category.

$$env = (friction, sight, temp, wind, covering) \tag{6}$$

The subcategory $sight$ is not restricted to the sight conditions of visible light in this context. Therefore also the influence on other physical sensor principles is covered.

D. Ego vehicle and Passengers

With the preceding categories, the environment of the ego vehicle is sufficiently described, the last two categories are with respect to the state of the ego vehicle $egost$ and the passengers inside it psg. To reduce the complexity of the automated driving system, only the sensors, logic and actuator interfaces are considered as part of the system. Hence the functionality of the vehicle itself which is also provided to a normal driver is considered as part of the specification space. Special attention has to be paid to differences in interfaces used by the system in comparison to a driver.

The passengers inside the automated vehicle are obviously not part of the automated system, but can have a considerable impact on the scene, especially in which operational mode the automation should be.

V. Derivation of functional system boundaries

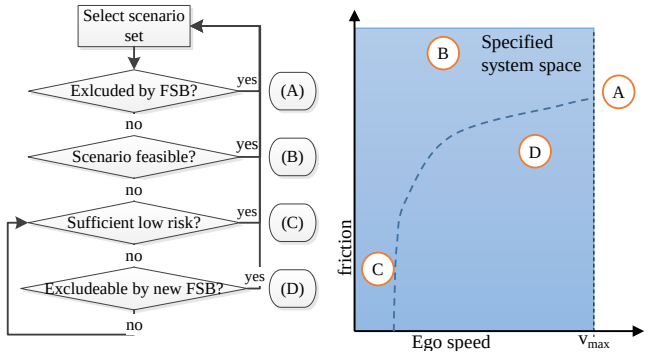
The general approach to derive functional system boundaries consists of the selection and evaluation of an arbitrary scenario defined in the specification space. Note the definition in the specification space allows a scalable level of detail and a scenario can therefore be quite general by determining only selected parameters thus representing a quantity of more detailed scenarios. For each scenario there are four possibilities: (A) the scenario is already excluded by functional system boundaries, (B) the system can handle the scenario, considering performance and safety, (C) the residual risk of these scenarios are acceptable low or (D) the scenario has to be excluded by system boundaries.

The approach is shown as flow diagram in figure 3 (a) and illustrated as a strongly simplified example, only showing two of the n dimensions of the specification space in 3 (b). As can be seen, the maximum velocity of the ego vehicle is already bounded by v_{max}, hence scenario (A) is excluded. Scenario (B) is classified as feasible since the friction-speed combination is not problematic. Because of low speed (C) may be classified as sufficiently safe, whereas (D) has to be excluded by a new functional system boundary, coupling the maximum speed with the friction. Obviously there are infinite possible scenarios. But as can be seen in the example, the clear structure of the specification space enables the definition of relevant boundaries for single dimensions of the space, like speed of the ego vehicle as well as combined boundaries like the friction dependent maximum speed.

VI. Derivation of surveillance concept

As defined in chapter II the boundary state includes a sufficient reaction of the system on the obtained system boundary to return to the safe state. Therefore it is necessary for the boundary to be detected by the system.

For most functional system boundaries of automated driving there are technical detection possibilities. In some cases these are already available in mass-produced cars like pedal



(a) approach

(b) simplified exemplary illustration of specification space

Fig. 3. In a) the approach to iterate to sufficient functional system boundaries (FSB) is visualized in a flow chart. The single steps are illustrated in b) by an exemplary 2-D illustration of the n-dimensional specification space, only visualizing the subcategories ego speed and friction coefficient

sensors to detect a driver intervention. In many cases the detection will have higher safety requirements, since a detection shifts from a supporting warning function to a safety critical system component. Especially for the detection of functional system boundaries outside the ego vehicle, this is a challenging situation. There is not always a redundant path feasible in these cases.

Therefore we propose a two stage surveillance concept. The first stage consists of the direct detection of functional system boundaries or internal errors. Through the direct detection an adapted reaction is possible.

But since remaining uncertainties of detection mechanisms exist, a second surveillance stage is needed. Hörwick introduced such an idea with his situational unplausibilities [7, p.86] to detect situations which should not have occurred in normal operational mode, including the violation of functional system boundaries as well as undetected system errors. However, he claims a valid environment perception to detect these unplausibilities. Since this cannot be stated in general, we integrate this idea into the risk based approach. Therefore the approach evolves from the simple binary decisions illustrated in figure 3 to a probabilistic model. Since the detection of a functional system boundary depends on the performance of the detection, the risk evaluation integrates the probability of missing the detection. A schematic example of a 90% detection rate for a system boundary is illustrated in figure 4. By adding additional plausibility checks, the risk of an intentionally excluded scenario can be decreased by excluding detectable parts of it. The idea of these plausibility checks based on specific parameters, characteristic for a subset of the excluded scenario and hence reducing the undetected occurrence. This idea is illustrated in figure 4 with an exemplary additional plausibility check excluding 80% of the hazard scenario. With this principle the residual risk of functional system boundaries can be reduced to an accepted level. In the example the residual risk is only caused by 10% of the remaining 20% of the scenario.

VII. Case Study Highway Application

To show the usability of the introduced categories, a case study of a highly automated driving system for highways is

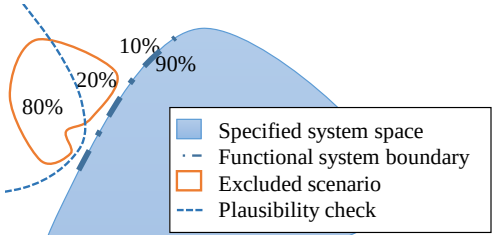


Fig. 4. Illustration of a second stage surveillance of functional system boundaries to reduce the probability of boundary violations

presented, listing possible system boundaries for conceivable reasons.

A. Restriction of static environment

In the first step, the drivable static environment is defined following the order in equation 3. In our example the system should be limited to a specific country e.g. Germany. This can be caused by juristic or actuarial considerations. This leads directly to national borders as functional system boundaries.

Like stated above, the domain is restricted to highways. The obvious impact of the domain on the available set of nodes and roads can be seen as pre-selection of subsets in these categories. The subset of nodes is already strongly restricted by the domain, since they mainly consist of highway start/end, acceleration/exit ramps and highway junctions. With the restriction on highways the node highway-end has to be a functional system boundary. While the same stands for the ego-vehicle driving on an exit ramp. The passing of an on-ramp could be excluded in a meaningful matter, if the system is not able to act cooperatively.

Analogously the road subset may be restricted by special requirements for the profile, e.g. the existence of a emergency lane, for the road conditions, e.g. quality of the surface, for the course, e.g. maximal curvature and also by the traffic rules, e.g. exclusion of unlimited maximum speed as is relevant in Germany.

As previously mentioned there can be special cases not yet covered by previous categories or which could be additionally labeled. Possible cases are tunnels, bridges, tollgates, border crossing stations and also roadworks. While the first four cases describe special cases of the static infrastructure they may lead to additional risks, roadworks have to be regarded as special cases since the originally intended environment is manipulated and can be ambiguous.

B. Specification of traffic dynamics

While the static environment can be restricted relatively easy and the violation of these restrictions is mainly caused by the movement of the ego vehicle in the specific situation, the traffic dynamics are mainly dependent on other traffic participants. However, the definition of specific functional system boundaries is required to separate dynamics handled by the system and those which exceed the specification. With these boundaries the system performance required can be specified and adequate test cases can be derived at. Furthermore possible maneuvers not handled, serve as a basis to quantify the residual

risk of such a system. Most of these violations can be caused by irregular behavior of other traffic participants.

Using the nomenclature presented in equations 4 and 5, the general dynamics can be described by the dynamic states and maneuvers of the traffic participants involved. To define reasonable functional system boundaries, the considerations start with the ego vehicle only and successively add additional traffic participants. Starting with the dynamic state of the ego vehicle, some major functional boundaries can be set. First of all, the speed driven can be limited respecting perception and control capabilities as well as physical limits. Analogously the maximum vehicle dynamics, i.e. yaw rate, side slip angle or accelerations could be restricted for normal driving maneuvers. Furthermore the position of the ego vehicle could be limited to specific lanes.

Next possible maneuvers of the ego vehicle are considered. Obviously not all of the proposed 17 principle maneuvers are relevant for a highway scenario, like parking or turning. In this case it could be reasonable to use domain specific maneuver catalogs to focus the derivation of relevant traffic scenes. These maneuver descriptions are just a clustering of the general traffic scenario description introduced in IV to ease human understanding. Also the specified maneuver dynamics can be defined where appropriate.

C. Environmental conditions

The environmental conditions are a prime example for the proposed approach to iterate ideal functional boundaries. Obviously conditions like the friction coefficient are only relevant in few scenarios with strong accelerations. Since heavy deceleration is physically not feasible on low friction, this scenario should be excluded. Therefore the speed can be reduced during low friction to exclude scenarios with larger accelerations shown exemplary in figure 3 (b). But since the detection of low friction, especially on local spots, is one of the most challenging perception problems for automated driving, also a more conservative exclusion of low friction might be necessary, using the proposed second surveillance step proposed in chapter VI. This could be realized by excluding scenarios which might lead to low friction like heavy precipitation or low temperatures. Like implied in figure 4 this does not lead to a complete exclusion of low friction scenarios, but can reduce the probability of their occurrence.

The sight of all sensors can be affected by environmental conditions like fog, heavy rain or also other radar or infrared sources. The specific value of these functional system boundaries depend on the specific sensor set and their sensibility to such potential disturbances. The possible detection of false positive and the non detection of false negatives is a fundamental source of risk and therefore the definition and detection of such boundaries is an important task.

Wind and temperature are relevant in extreme occurrences and the covering of relevant signs or markings by greenery or leaves can be a relevant problem in automated driving.

D. Boundaries caused by the ego vehicle or passengers

As defined, this category describes requirements of the automation system for the vehicle. First of all this includes a working chassis with no flat tires but also general function of the drivetrain and brake system. Also some boundaries like attached trailers or open doors should be considered.

Last but not least, the passengers, especially the driver, motivates the most intuitive functional system boundary by activating and deactivating the system. The specific possibilities of interaction is a wide field of research, considering the optimal HMI-concept for such systems. Also the state of the driver is relevant, since he has to be able to take over after sufficient time, following the definition of a highly automated system.

VIII. Conclusion and Outlook

A general concept is presented to evaluate the risk of an automated driving system observing functional system boundaries and system errors. A methodology to define specific functional system boundaries, necessary for a structured evaluation is proposed. The introduced specification space enables an arbitrary level of detail to describe relevant scenarios and system boundaries and furthermore supports the identification of functional system boundaries. For the detection of defined system boundaries a two stage surveillance concept is proposed to handle uncertainties. For illustration, exemplary functional system boundaries are derived at for a case of actual use.

In the approach presented the step to evaluate feasibility and safety is the most challenging part. The derivation of an objective methodology will be focused in the next research steps. Furthermore the handling of system errors will be discussed in future publications.

Acknowledgment

The research project is funded and supported by the AUDI AG.

References

[1] T. M. Gasser, *Rechtsfolgen zunehmender Fahrzeugautomatisierung: Gemeinsamer Schlussbericht der Projektgruppe*, ser. Berichte der Bundesanstalt für Strassenwesen : F, Fahrzeugtechnik. Bremerhaven: Wirtschaftsverl. NW Verl. für neue Wissenschaft, 2012, vol. 83.

[2] SAE, "Taxonomy and definitions for terms related to on-road motor vehicle automated driving systems," Januar 2014.

[3] ISO, "26262-1 road vehicles - functional safety - part 1: Vocabulary," 2011-11-14.

[4] R. Bell and D. Reinert, "Risk and system integrity concepts for safety-related control systems," in *COMPASS '93: Eighth Annual Conference on Computer*, 1993, pp. 15–34.

[5] ISO, "26262-3 road vehicles - functional safety - part3: Concept phase," 2011-11-14.

[6] O. Gietelink, "Design and validation of advanced driver assistance systems," Ph.D. dissertation, Technische Universiteit Delft, Delft, 2007.

[7] M. Hörwick, "Sicherheitskonzept für hochautomoatisierte fahrerassistenzsysteme," Ph.D. dissertation, Technische Universität München, München, 2011.

[8] A. Reschka, J. R. Bohmer, T. Nothdurft, P. Hecker, B. Lichte, and M. Maurer, "A surveillance and safety system based on performance criteria and functional degradation for an autonomous vehicle," in *2012 15th International IEEE Conference on Intelligent Transportation Systems - (ITSC 2012)*, 2012, pp. 237–242.

[9] G. Reichart, *Menschliche Zuverlässigkeit beim Führen von Kraftfahrzeugen*, als ms. gedr ed., ser. Fortschritt-Berichte / VDI Mensch-Maschine-Systeme. Düsseldorf: VDI-Verl., 2001, vol. Nr. 7.

[10] C. Domsch and H. Negele, “Einsatz von referenzfahrsituationen bei der entwicklung von fahrerassistenzsystemen,” in *Aktive Sicherheit durch Fahrerassistenz*, B. Heißing, Ed., 2008.

[11] S. Geyer, M. Baltzer, B. Franz, S. Hakuli, M. Kauer, M. Kienle, S. Meier, T. Weißgerber, K. Bengler, R. Bruder, F. Flemisch, and H. Winner, “Concept and development of a unified ontology for generating test and use-case catalogues for assisted and automated vehicle guidance,” *IET Intelligent Transport Systems*, 2013.

[12] A. Weitzel, *Absicherungsstrategien für Fahrerassistenzsysteme mit Umfeldwahrnehmung*, ser. Berichte der Bundesanstalt für Strassenwesen. Fahrzeugtechnik. Bremen: Fachverlag NW, 2014, vol. Heft F 98.

[13] H.-H. Nagel, W. Enkelmann, and G. Struck, “Fhg-co-driver: From map-guided automatic driving by machine vision to a cooperative driver support,” *Mathematical and Computer Modelling*, vol. 22, no. 4-7, pp. 185–212, 1995.

[14] W. Tölle, *Ein Fahrmanöverkonzept für einen maschinellen Kopiloten*, als ms. gedr ed., ser. Fortschrittberichte VDI : Reihe 12, Verkehrstechnik, Fahrzeugtechnik. Düsseldorf: VDI-Verl, 1996, vol. Nr. 299.