# FAULT TREE-BASED DERIVATION OF SAFETY REQUIREMENTS FOR AUTOMATED DRIVING ON THE EXAMPLE OF COOPERATIVE VALET PARKING

**Valerij Schönemann, Hermann Winner**
Institute of Automotive Engineering ,Technische Universität Darmstadt
Darmstadt, Germany

**Thomas Glock, Eric Sax**
Research and Engineering Center, FZI Research Center for Information Technology
Karlsruhe, Germany

**Bert Boeddeker, Sebastian vom Dorff**
Research and Engineering Center, DENSO AUTOMOTIVE Deutschland GmbH
Eching, Germany

**Geert Verhaeg[1], Fabrizio Tronci[2], Gustavo G. Padilla[3]**
TNO[1], Magneti Marelli[2], Hella Aglaia Mobile Vision[3]
Netherlands[1], Italy[2], Germany[3]

Paper Number 19-0099

## ABSTRACT

Developing safe vehicle automation systems is crucial for the commercialization of automated driving. One of the major challenges for the release of fully automated driving is functional safety. Automated driving systems explode in complexity due to an infinite number of occurring scenarios. Thereby, the derivation of safety requirements for complex automated driving functions lacks a categorization to tackle the completeness issue. This work presents a structure for a fault tree-based approach to derive safety requirements from safety goals systematically in compliance with the international standard of functional safety for road vehicles known as ISO 26262. The investigation of the state of the art reveals that a functional safety concept for fully automated valet parking (AVP) has not yet been targeted. The methodology is therefore applied on the example of automated valet parking to elaborate a safety concept which was not yet investigated.

Beforehand, the AVP system was split into a manageable amount of relevant functional scenarios to decrease complexity. For each scenario, a Hazard Analysis and Risk Assessment (HARA) was performed. A set of safety goals was elaborated. The approach utilizes a fault tree-based Sense-Plan-Act architecture to achieve a large coverage of possibly derivable safety requirements from safety goals. The sense phase contains the acquisition of sensor data and leads to three uncertainty domains: state, existence, and class uncertainty. The plan segment includes the situation comprehension and action planning. Thereby, the transportation mission can be split into five tasks. The act block represents the execution of the planned trajectory. Longitudinal and lateral vehicle dynamics such as steering, shifting, accelerating, and braking are performed. A violation of a safety goal occurs if at least one of the failure events in the sense-, plan-, and act-phase is present. The methodology is suitable for safety goals which follow the specified Sense-Plan-Act pattern.

## INTRODUCTION

The globally leading cause of death among people aged 15-29 in the year 2012 are road traffic accidents [1]. 94 % of crashes can be tied back to human error [2]. In 2015, the United Nations agreed to global goals for sustainable development. The goal “good health and well-being” concerns road safety in which the number of global deaths and injuries from road traffic accidents shall be halved by 2020. Safe automated systems that intervene in case of a proximate accident and release the driver from the responsibility are required. Thereby, functional safety is one of the major challenges for the release of automated driving [3]. An automated driving function shall be harmless in all operating states. The system shall identify hazards and reach a safe location in which the vehicle is no hazard for other participants. The international standard for functional safety ISO 26262 specifies a systematic procedure for designing functionally safe electrical and electronic systems [4]. ISO 26262 and international standards for other domains are derived from the IEC 61508 [5].

Automated systems from different domains have a common denominator: exploding complexity. A nearly infinite number of possible scenarios has to be tested. The European Union (EU) project ENABLE-S3 focuses on the reduction of today’s cost-intensive verification and validation process to establish efficient methods for the commercialization of automated cyber-physical systems. Different approaches have to be targeted in order to cope with the increasing complexity regarding the development of safe automated systems.

A major challenge is to develop a functionally safe distributed system in which independent subsystems share responsibility for the automation task. Such a distributed system is fully Automated Valet Parking (AVP). AVP is realized through cooperation between the automated vehicle and a Parking Area Management system (PAM). The automated vehicle operates driverless and is classified as level 4 of SAE International's taxonomy of driving automation [6]. The use case provides an automated parking procedure. In previous work, a scenario-based methodology for functional safety according to ISO 26262 was presented and applied on the safety analysis of AVP [7]. The following pre-conditions were assumed for AVP:

1. Parking management system and automated vehicle manage the driving task in cooperation.
2. The handing over and requesting back procedure of the automated vehicle to/ from the PAM is instructed via a terminal (human-machine interface, HMI).
3. Manually and automatically operated vehicles are allowed to enter the parking garage.
4. Pedestrians, animals, obstacles, etc. sojourn in the car park.
5. Drivers and passengers have to leave the automated vehicle before AVP is activated.
6. Parking construction prevents dangers caused by running engines.

The described constraints served as an input to break down the system's functional behavior into scenarios. Thereby, the AVP system was split into a manageable amount of relevant functional scenarios to decrease complexity. For each scenario, a Hazard Analysis and Risk Assessment (HARA) is performed. As a result, a more complete set of safety goals was elaborated as indicated in Table 1.

This work is structured as follows: Section 2 contains the related work of functional safety. Section 3 illustrates a structure for a fault-tree-based approach to derive functional safety requirements for automated driving. Thereafter, the presented methodology is applied using the example of fully automated valet parking. Section 4 shows the elaborated safety requirements from safety goals for AVP. Section 5 summarizes the results of the safety requirements and gives a brief outlook for developing a safety concept.

***Table 1.***
***Safety Goals for Automated Valet Parking [7]***

| ID | Safety Goal | ASIL |
|---|---|---|
| SG01 | Unintended activation of the valet parking function outside of the PAM-controlled parking area shall be prevented. | D |
| SG02 | The integrity of the communication between the PAM and the vehicle shall be ensured. | D |
| SG03 | The system shall prevent a collision between automated vehicles and persons. | C |
| SG04 | The vehicle shall not start moving during embarkment and disembarkment. | C |
| SG05 | The system shall prevent collisions with other vehicles. | B |
| SG06 | The system shall notify a human supervisor in case of a collision or fire. | B |
| SG07 | The system shall ensure that the vehicle stays within the (statically defined) drivable area during AVP. | B |
| SG08 | The valet parking function shall be disabled if people are inside the vehicle. | A |
| SG09 | The system shall prevent collision of automated vehicles with objects. | A |

## RELATED WORK

A major challenge for the release of automated driving is the issue of testing. Up to now, only the international standard ISO 26262 illustrates a systematic process for developing functionally safe electrical and electronic systems in the automotive domain. Neither a standard, nor a methodology is specified to elaborate a safety concept specifically for automated driving. However, functional safety as well as a corresponding methodology for developing a safety concept for such complex systems is crucial for the release of automated driving [8].

Alexander et al. [9] combined several existing approaches to develop a methodology for deriving safety requirements for autonomous systems. The authors describe the derivation of safety requirements as a three-stage process. In the first step, harmful events are determined (hazard identification). Causes of the hazards are explored (hazard analysis) and finally safety requirements can be derived from causes. The system is seen as a combination of operators (Combined Autonomous Systems, CAS) in which hazards may occur. High-level capabilities of CAS are determined and hierarchically decomposed in lower level capabilities until these can be analyzed for safety (Hall-May [9]). The authors consider autonomous systems in general. Autonomous systems from other domains will lead to different safety requirements e.g. by comparing automated systems in the health domain with automated driving functions.

The fault tree analysis is a deductive approach starting with a top undesired event and is suggested in the ISO 26262 beside a Failure Modes and Effects Analysis (FMEA) and Hazard and Operability study (HAZOP) for safety analysis. FTA is also used in the nuclear power and aerospace sector. Failure events can be identified by considering Boolean logic. The main advantage of a FTA is that it displays interactions between events in a graphical format [11]. The interaction cannot be seen from a FMEA. A FMEA is more suitable for an inductive failure analysis of components and subsystems. Furthermore, the FTA should contain all failure modes of a FMEA.

Lambert applied a qualitative FTA on a car starting system [12]. Thereby, the applier has to identify the failure modes that cause the top event. Starting from the top undesired event that the car does not start, the author shows a logical progression of undesired events connected via AND and OR logic. However, a vast number of undesired events may occur with increasing system complexity. The elaboration of a FTA for automated driving systems without providing any structure is challenging.

Stolte et al. [13] derived safety goals and functional safety requirements of actuation systems for automated driving by applying a system theory-based methodology. The authors used a System-Theoretic Process Analysis (STPA) to identify unsafe control actions and its causes which serve as an input for a HARA. Furthermore, safety requirements are derived from a control structure and corresponding unsafe control actions. The authors do not determine safety requirements for perception or planning modules of automated vehicles. The trajectory input was assumed to be correct and only actuation systems of automated vehicles were analyzed.

The national project PEGASUS [14] applies a scenario-based approach to reduce driving test distances for a statistical approval of highly automated driving. It is assumed that the majority of the driven mileage is uncritical and only critical scenarios are required to be investigated. Amersbach and Winner [15] proposed a six-layer decomposition of the automated driving function. The six layers are Information Access, Information Reception, Information Processing, Situational Understanding, Behavioral Decision, and Action. A matrix to allocate fail criteria to functional layers and relevant scenarios is built. Fail criteria are identified by using a FTA. Redundant fail criteria that are “subsets or intersecting sets of each other” are combined and thus the testing effort is reduced. Test cases and environments are derived from fail criteria for the use of safety approval. However, the authors propose a different approach and do not relate to the ISO 26262 standard. The interaction of different subsystems is not targeted.

Furthermore, there is still a risk of a violation of a safety goal without any malfunction. It is therefore required to consider the safety of the intended function (SOTIF). A sub-working group was built within ISO 26262 to specify when a target function behaves safely. The results are present in the ISO/WD PAS 21448. This work aims to cover critical scenarios, which are not only a result of malfunction, but also the safety of the intended functionality.

Reschka et al. [16] investigated safety concepts for automated driving without driver monitoring. The analysis leads to high-level safety mechanisms to handle potential hazards for AVP systems. More specific safety requirements are not presented. Bosch and Daimler [17] released the first prototype for infrastructure- based AVP in a mixed traffic parking garage. However, further specification concerning the safety are missing. Chirca et al. [18] and Schwesinger et al. [19] provide mainly a technical description of an AVP service in which safety is not of major focus.

The state of the art reveals that a structure for breaking down highly complex and self-driving automation systems is missing. This work aims to overcome the lack of a recipe for deriving safety requirements from safety goals. This work presents a methodology how such a specification can be achieved by deriving safety requirements for automated driving systematically in compliance with the international standard ISO 26262. The approach utilizes a fault tree-based technique to achieve a large coverage of possibly derivable safety requirements. The issue of completeness is targeted qualitatively by applying a deductive

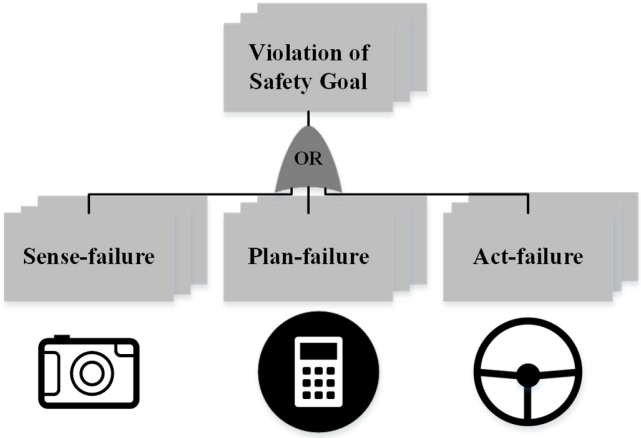


***Figure 1. The violation of a safety goal occurs if at least one of the failure events in the sense-, plan-, and act-phase is present.***

method. The methodology is applied on cooperative valet parking for which a safety concept is still missing in the state of the art.

## METHODOLOGY

The methodology presented in this work provides a path to systematically derive safety requirements from safety goals. A fault tree-based approach is proposed to ensure a more complete set of safety requirements. Sequential robot control architectures are known as Sense-Plan-Act or Sense-Model-Plan-Act architectures. Thereby, the signal processing steps of the sensor data acquisition, the environment modeling, the planning, and finally the actions are executed sequentially. Sequential architecture elements serve for achieving a long-term goal, e.g. the execution of a driving mission [20]. In the following the terms Sense, Plan, Act and the corresponding breakdown into segments are introduced. Figure 1 indicates the safety analysis of a Safety Goal's violation.

*Sense*: The Sense phase contains the acquisition of sensor data and modelling of the environment. According to Dietmayer et al. [21] detecting static and dynamic objects and physically measuring them as precisely as possible, leads to three uncertainty domains visualized in Figure 2:

- State uncertainty: Represents the measuring errors of physical measured variables, especially the object's dimensions (length, width, height), the object's pose and the object's velocity.
- Existence uncertainty: Outlines the uncertainty whether an object captured by the sensors and mapped into the representation actually exists. This concerns mainly false positives and false negatives. For example, emergency braking should only be executed in case of a high existence probability.
- Class uncertainty: Describes uncertainty of the capability to classify the object's membership in order to predict the object's behavior. Type of object might be for example pedestrians, bicyclists, trucks, or cars. The degree of granularity is dependent on the use case.

*Plan*: The Plan segment includes the situation comprehension and action planning. The transportation mission can be split into five tasks which are partly computed by today's navigation systems. These five steps are given in Figure 3:

- Mission Planning: In the first step, a mission has to be planned from the current location to the destination.
- Route Planning: A route has to be determined in order to get to the destination.
- Behavior Planning: Selects a sequence of maneuvers by considering other traffic participants, traffic rules and restrictions.
- Maneuver Planning: Maneuvers such as lane changes have to be executed.
- Trajectory Planning: A trajectory has to be calculated to perform necessary maneuvers.

Timing constraints for the start and end of each maneuver and the calculation of the maneuver trajectory have to be specified.

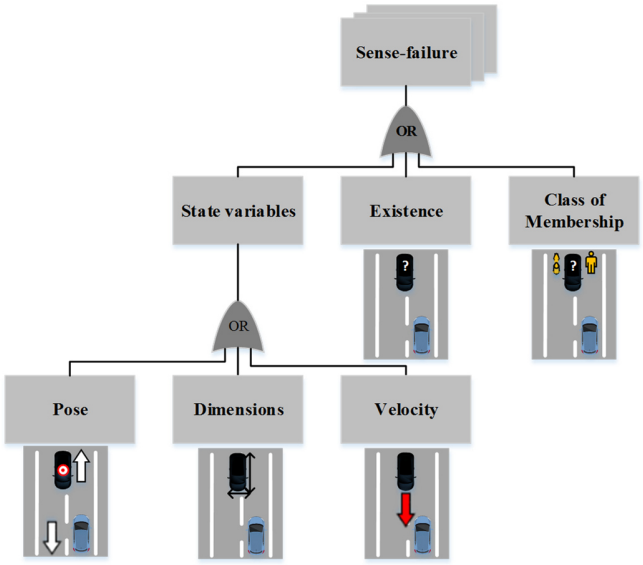


***Figure 2. According to Dietmayer [17] an uncertainty in the sense phase occurs if the object's state variables such as the object's pose, the object's dimensions, and the object's velocity are not measured with sufficient precision or if the object's existence or its class of membership are uncertain.***

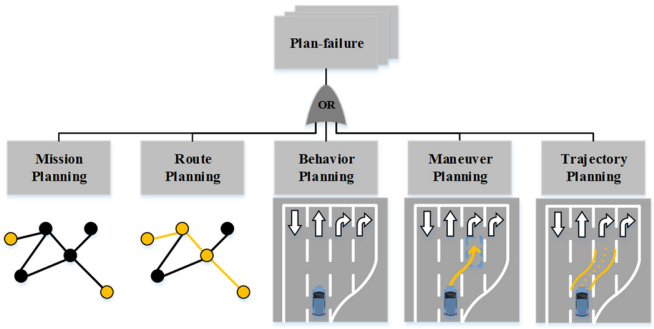


***Figure 3. According to Lotz [22] the driving mission can be split into mission planning, route planning, behavior planning, maneuver planning, and trajectory planning. For maneuver and trajectory planning, timing constraints for calculation and execution are crucial.***

*Act*: The Act block represents the execution of the planned trajectory. The following vehicle control inputs are required for performing longitudinal and lateral vehicle dynamics: Steering, shifting, accelerating, and braking. A complete electrification of actuators is mandatory. This is realized by today's X-by-Wire concepts: Throttle-by-Wire, Brake-by-Wire, Shift-by-Wire, and Steer-by-Wire [19]. Thereby, either the targeted steering, shifting, acceleration, and braking parameters are not plausible for the executed maneuver in terms of range and time or corresponding vehicle components are corrupted. The breakdown of possible Act-failures is illustrated in Figure 4.

The presented structure can be further broken down into use case-specific safety requirements. The safety requirements can be derived systematically by covering a more complete set of safety requirements due to the application of a deductive fault tree-based approach. The methodology is not suitable for all derived safety goals since for example C2X-communication does not follow the specified Sense-Plan-Act pattern.

## DERIVATION OF SAFETY REQUIREMENTS

In the following, the elaborated methodology is applied to the safety goal "SG03: *The automated driving system shall prevent a collision between automated vehicles and persons*". Furthermore, the derivation is similar for SG05 and SG09 only with a different ASIL inheritance for derived safety requirements and decomposition to architectural elements.

The division in sense, plan, and act leads to the following high-level Functional Safety Requirements (FSR):

- FSR3.1: The system shall detect objects in its required sensor perception area
- FSR3.2: The system shall not plan a harmful trajectory
- FSR3.3: The vehicle shall prevent unintended control actions

Each high-level FSR will be further broken down into low-level FSR.

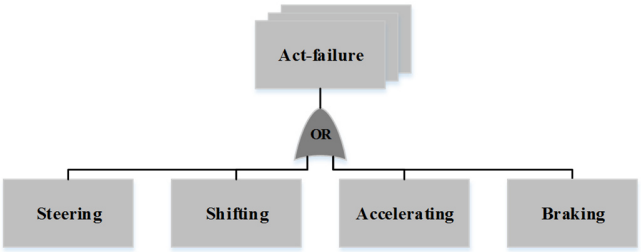


*Figure 4. Steering, shifting, accelerating, and braking are primitives that are required for vehicle control mechanisms.*

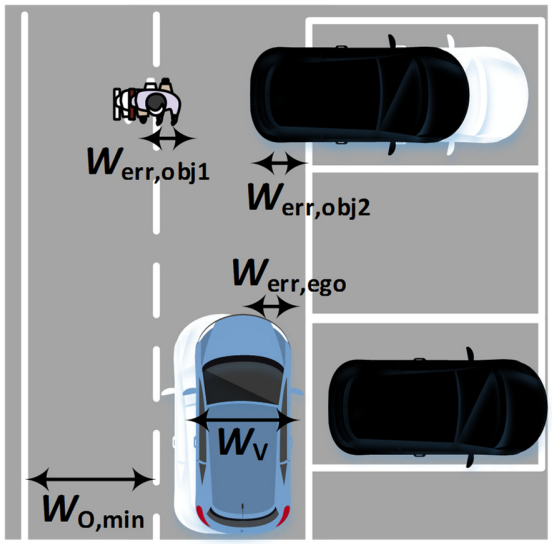


*Figure 5. Maximum accepted total error of size determination and object localization is given by the narrowest part in the operational domain and measurement inaccuracies*

## A. Sense

Since no standard exists specifically for safety requirements of automated driving, other regulations have to be considered as a basis. State uncertainty is represented by the functional safety requirement FSR3.1.1 - FSR3.1.3 of Table 3. and corresponding derived functional safety requirements. The system has to detect the object's position by localizing it. The precision of localization is given by the narrowest part of the operational design domain $W_{\mathrm{O,min}}$, the vehicle width $W_{\mathrm{V}}$, and corresponding measurement inaccuracies $W_{\mathrm{err}}$ which may appear on both sides in worst-case. Figure 5 indicates an ego-vehicle driving straight and approaching two objects. Beside the ego-vehicle's localization error $W_{\mathrm{err,ego}}$, the object's localization errors $W_{\mathrm{err,obj}}$ are present. The ego-vehicle assesses a collision-free area due to localization errors, but in reality the ego-vehicle would collide with a traffic participant. The total accepted localization error $W_{\mathrm{err,total}}$ is given by

$$W_{\mathrm{err,total}} \leq W_{\mathrm{err,ego}} + W_{\mathrm{err,obj}} = \frac{W_{\mathrm{O,min}}}{2} - \frac{W_{\mathrm{V}}}{2} \quad \text{(Equation 1)}$$

$$W_{\mathrm{err,obj}} \leq \frac{W_{\mathrm{O,min}} - W_{\mathrm{V}}}{4} \quad \text{for } W_{\mathrm{err,ego}} = W_{\mathrm{err,obj}} \text{ (infrastructure-based)}$$

Considering Germany's road construction regulation and Germany's traffic regulation, a minimum lane width $W_{\mathrm{L,min}} = 2.75$ m [25][26] and a maximum vehicle width of $W_{\mathrm{V,max}} = 2.50$ m [27] can be found. The overall error of size determination and object localization for $W_{\mathrm{err,ego}} = W_{\mathrm{err,obj}}$ shall be less than $W_{\mathrm{err,total}} = (W_{\mathrm{L,min}} - W_{\mathrm{V,max}})/2 = 12.5$ cm and $W_{\mathrm{err,obj}} \leq 6.25$ cm. However, for AVP systems a parking lot width of $W_{\mathrm{P,min}} = 2.75$ m is not profitable for the operator and a minimum parking lot width of Germany's parking garage regulation $W_{\mathrm{P,min}} = 2.30$ m [26] could be considered by not allowing to enter oversized vehicles. In that case, a look on the European's average passenger car size of 2016 could be done [24]. Adding a safety margin of 10 cm for withdrawn car mirrors on each side, we end up with an average vehicle width of around $W_{\mathrm{V,avg}} = 2$ m and therefore an overall error of size determination and object localization of less than $W_{\mathrm{err,total}} \leq (W_{\mathrm{P,min}} - W_{\mathrm{V,avg}})/2 = 15$ cm and $W_{\mathrm{err,obj}} \leq 7.5$ cm.

The object can only be detected if it appears in the system's sensor perception area. Safety-relevant areas of interest for collision avoidance can be specified dependent on the dynamic driving parameters of the engaged traffic participants such as velocities, timing constraints and deceleration capabilities. A definition of an area, in which the perception of objects for collision avoidance is mandatory, has to be given. Furthermore, maneuvers that can occur in the defined operational domain as illustrated in Figure 6 have to be identified. The superposition of the maneuver-based stopping distances shows that the overall safety zone is created by the ego-vehicle's and the object's travelled envelopes given by their widths and stopping distances [28].

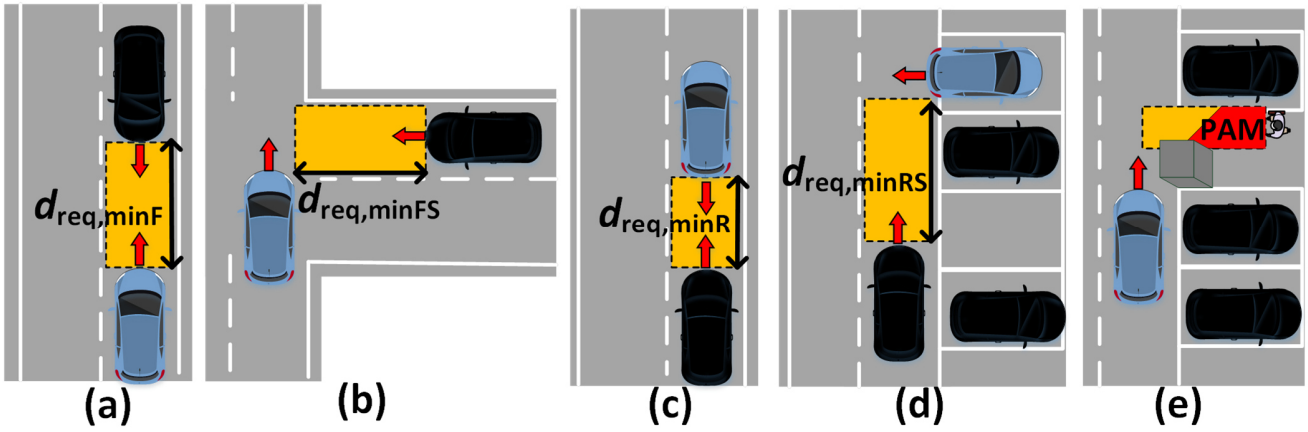


***Figure 6. Identified maneuvers that lead to a minimum required sensor perception area: (a) driving straight with potential frontal collision between an automated and manually driven vehicle and both vehicles are braking, (b) intersection crossing and approaching collision partner, (c) driving in reverse with potential rear collision and both vehicles braking, (d) leaving the parking spot in reverse, (e) covered object and required infrastructure support.***

The worst-case concerning the stopping distance is defined as a frontal collision of an automated and manually operated vehicle driving with $v_{\max}$ and both vehicles are braking. It is assumed that both vehicles react at the same time. The minimum required sensor range $d_{\text{req}}$ is theoretically given by the stopping distance until frontal collision and can be calculated according to

$$d_{\text{req,min}} \geq \left(v_{\text{ego}} + v_{\text{obj}}\right) \cdot \left(\mathrm{t}_{\text{B,lag}} + t_{\text{R,ad}}\right) + v_{\text{obj}} \cdot \left(t_{\text{R,md}} - t_{\text{R,ad}}\right) + \frac{v_{\text{ego}}^2 + v_{\text{obj}}^2}{2 \cdot D_{\min}} + d_{\text{tol}} \qquad \text{(Equation 2)}$$

Thereby, the worst-case constraints are defined as presented in Table 2. Considering rather conservative values of a nearly dry road surface and a resulting minimum deceleration of $D_{\min} = 8\ \mathrm{m/s^2}$, a free running time $\mathrm{t}_{\text{B,lag}} + t_{\text{R,ad}} = 0.5$ s, worst-case driver reaction time $t_{\text{R,md}} = 1.5$ s and $d_{\text{tol}} = 0.5$ m, we get $d_{\text{req,minF}} \geq 27.51$ m. A worst case for a rear collision is a collision at a maximum allowed reverse velocity of the ego-vehicle $v_{\text{ego}} = v_{\text{maxR}}$, an object forward velocity of $v_{\text{obj}} = v_{\text{maxF}}$, and braking of both vehicles. From this, a required sensor range of $d_{\text{req,minR}} \geq 20.88$ m can be calculated. Finally, a worst case for the perception distance to the side is given by crossing an intersection at a maximum allowed intersection crossing velocity of $v_{\text{obj}} = v_{\text{maxI}}$

$$d_{\text{req,minFS}} = d_{\text{req,minRS}} \geq v_{\text{obj}} \cdot \left(t_{\text{B,lag}} + t_{\text{R,obj}}\right) + \frac{v_{\text{obj}}^2}{2 \cdot D_{\min}} + d_{\text{tol}} \qquad \text{(Equation 3)}$$

We end up with a required sensor perception range of $d_{\text{req,minFS}} = d_{\text{req,minRS}} \geq 19$ m. The required sensor perception area to the rear side is actually largest if the vehicle leaves the parking spot backwards. However, since the required sensor perception area to the front is mandatory in many specific situations, the required sensor perception area to the rear side $d_{\text{req,minRS}}$ can be significantly reduced if only reverse parking and forward leaving of the parking bay is allowed. Considering a parking spot length of $L_{\text{P,min}} = 5$ m [26], we can approximate $d_{\text{req,minRS}} \geq L_{\text{P,min}} = 5$ m. Objects that lie within the ego-vehicle's required sensor perception area and are covered, have to be detected by top-mounted sensors of the infrastructure. The elaborated safety zone should adjust its size according to the present velocities in the sensor perception area. The overall required horizontal FoV of 180° in the front and to the rear is required to detect moving objects in the frontal/ rear vehicle area. Elaborated functional safety requirements are shown in Table 3.

***Table 2.***
***Pre-defined Constraints for Automated Valet Parking [28]***

| ID | Description | Value |
|---|---|---|
| C01 | Maximum allowed velocities: in forward $v_{\mathrm{max,f}}$, in reverse $v_{\mathrm{max,r}}$, at intersections $v_{\mathrm{max,i}}$ | $v_{\mathrm{maxF}} = 30\ \mathrm{km/h}$<br>$v_{\mathrm{maxR}} = 10\,\mathrm{km/h}$<br>$v_{\mathrm{maxI}} = 10\,\mathrm{km/h}$ |
| C02 | Worst-case expected time delays: system response time from the plausibility check until initiating the brakes $t_{\mathrm{R,ad}}$, driver reaction time $t_{\mathrm{R,md}}$, lag time of the brake $t_{\mathrm{B,lag}}$ given by the response time of the brake $t_{\mathrm{R,b}}$ and the time until buildup of deceleration $t_{\mathrm{B,b}}$ | $t_{\mathrm{R,ad}} = 0.3$ s<br>$t_{\mathrm{R,md}} = 1.5$ s<br>$t_{\mathrm{B,lag}} \approx t_{\mathrm{R,b}} + \frac{t_{\mathrm{B,b}}}{2}$<br>[1]$t_{\mathrm{B,lag}} = 0.2$ s |
| C03 | Minimum expected deceleration $D_{\mathrm{min}} = \mu_{\mathrm{min}} \cdot g$ for object- and ego-vehicle | $D_{\mathrm{min}} = 8\ \frac{\mathrm{m}^2}{\mathrm{s}}$ |
| C04 | Safety margin $d_{\mathrm{tol}}$ | $d_{\mathrm{tol}} = 0.5$ m |

1) Breuer and Bill, 2008

***Table 3.***
***Derivation of FSR3.1: "The system shall detect objects in its sensor perception area."***

| ID | Functional Safety Requirement |
|---|---|
| FSR3.1.1 | The system shall detect the object's state variables sufficiently accurate. |
| FSR3.1.1.1 | The system shall localize the object's pose $p_{\mathrm{obj.}}$ The error for size determination and object localization shall be less than $W_{\mathrm{err,obj}}$. |
| FSR3.1.1.1.1 | The system shall detect objects in a 180° front and rear horizontal and sufficiently high vertical field of view. |
| FSR3.1.1.1.2 | The system shall detect the object's pose $p_{\mathrm{obj}}$ in its minimum required sensor range $d_{\mathrm{req,minF}}$, $d_{\mathrm{req,minFS}}$, $d_{\mathrm{req,minR}}$, and $d_{\mathrm{req,minRS}}$. |
| FSR3.1.1.2 | The system shall determine the object's dimensions length $l_{\mathrm{obj}}$, width $w_{\mathrm{obj}}$, height $h_{\mathrm{obj}}$ in its minimum required sensor range. The error for size determination and object localization shall be less than $W_{\mathrm{err,obj}}$. |
| FSR3.1.1.3 | The system shall determine the object's velocity $v_{\mathrm{obj}}$ in its minimum required sensor range. |
| FSR3.1.1.4 | The system shall detect objects under all possible environment conditions in the PAM area. |
| FSR3.1.1.5 | The system shall diagnose broken/ covered or misplaced sensors. |
| FSR3.1.1.6 | The system shall detect objects that are covered from the vehicle's view in its minimum required sensor perception area. |
| FSR3.1.2 | The system shall have an ASIL-dependent false positive and false negative rate. |
| FSR3.1.3 | The system's object classification shall not lead to harmful situational interpretation. |

**B. Plan**

The navigation to a specified destination starts with mission planning. The vehicle's position and the destination's position are required for mission planning. Based on the current and the destination's position, todays graph-based search algorithms for road networks determine a route. The computed route shall be composed of up-to-date, accessible, connected road segments that shall be driven in compliance with traffic regulations. The functional safety requirements are equally valid for the lane assignment. Maneuvers such as lane changes are required to reach the destination. The maneuver and the corresponding trajectory shall be feasible, collision-free, and calculated within hard real-time constraints. Thereby, hard real-time is defined as "a missing system response deadline leads to a collision". Start and end of the maneuver have to be defined depending on the maneuver and environmental constraints. Derived functional safety requirements are presented in Table 4.

*Table 4.*
*Derivation of FSR3.2: "The system shall not plan a harmful trajectory."*

| ID | Functional Safety Requirement |
|---|---|
| FSR3.2.1 | The system shall plan a safe mission. |
| FSR3.2.1.1 | The system shall localize its pose $p_{\mathrm{obj}}$. The error for size determination and localization shall be less than $W_{\mathrm{err,ego}}$. |
| FSR3.2.1.2 | The system shall localize the destination's position. The error for size determination and localization shall be less than $W_{\mathrm{err,obj}}$. |
| FSR3.2.2 | The system shall plan routes on up-to-date, accessible, connected road segments in compliance with traffic regulations. |
| FSR3.2.3 | The system shall assign maneuvers on up-to-date, accessible drivable area in compliance with traffic regulations. |
| FSR3.2.4 | The system shall compute a feasible, collision-free maneuver within hard real-time constraints (= missing deadline leads to a collision). |
| FSR3.2.5 | The system shall plan a collision-free trajectory. |

### C. Act

Act-failures are not further broken down since an investigation is already done in [13] and state of the art. For the sake of completeness, functional safety requirements are illustrated exemplary in Table 5.

*Table 5.*
*Derivation of FSR3.3: "The vehicle shall prevent unintended control actions."*

| ID | Functional Safety Requirement |
|---|---|
| FSR3.3.1 | The system shall detect corrupted or uncalibrated actuators and breakdown of necessary vehicle components. |
| FSR3.3.2 | The system shall prevent unintended steering. |
| FSR3.3.3 | The system shall prevent unintended shifting. |
| FSR3.3.4 | The system shall prevent unintended accelerating. |
| FSR3.3.5 | The system shall prevent unintended braking. |

Finally, a safety engineer has to control whether a functional safety requirement is not yet covered by another safety goal and should inherit the corresponding safety goal's Automotive Safety Integrity Level (ASIL). The functional safety requirements for the remaining safety goals are shown in Table 6. in the appendix.

## CONCLUSION AND OUTLOOK

The state of the art has revealed challenges for automated driving in terms of functional safety. Beside malfunctions, the safety of the intended functionality has to be considered. The derivation of safety requirements for complex automated driving functions leads to the completeness issue. An approach is proposed to derive functional safety requirements in compliance with ISO 26262 according to a deductive fault tree-based methodology for automated driving functions. Functional safety requirements can be derived systematically to target the completeness issue qualitatively. The technique is applied on elaborated safety goals for automated valet parking. Functional safety requirements are derived for all elaborated safety goals. A minimum required sensor perception area could be specified for AVP in which the object's parameters such as pose, dimensions, velocity, existence and class are required to be known. The maximum accepted total error of size determination and object localization could be identified. In future work, functional safety requirements should be assigned to functional blocks of the valet parking system architecture. Thereby, the distribution of functionalities between the automated vehicle and the parking area management system will be targeted and additional test cases will be derived for functional safety requirements to validate the safety concept of automated valet parking.

**ACKNOWLEDGEMENT**
This project has received funding from the ECSEL Joint Undertaking under grant agreement No 692455. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Denmark, Germany, Finland, Czech Republic, Italy, Spain, Portugal, Poland, Ireland, Belgium, France, Netherlands, United Kingdom, Slovakia, Norway.

**REFERENCES**

[1] World Health Organization, "Global status report on road safety 2015," World Health Organization, 2015.

[2] S. Singh, "Critical reasons for crashes investigated in the national motor vehicle crash causation survey," No. DOT HS 812 115, 2015.

[3] W. Wachenfeld and H. Winner, "The Release of Autonomous Vehicles," in Autonomous Driving: Technical, Legal and Social Aspects, M. Maurer, J. C. Gerdes, B. Lenz, and H. Winner, Eds.: Springer, 2016, pp. 425–449.

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

[5] International Electrotechnical Commission, "Functional safety of electrical/electronic/programmable electronic safety related systems," IEC 61508, 2000.

[6] SAE, "Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles," Society of Automotive

[7] V. Schönemann and H. Winner et al.," Scenario-based Functional Safety for Automated Driving on the Example of Valet Parking," in IEEE Future Information and Communication Conference, Singapore, 2018.

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

[9] R. Alexander, N. Herbert, and T. Kelly, "Deriving safety requirements for autonomous systems," in 4th SEAS DTC Technical Conference, 2009.

[10] M. Hall-May, "Ensuring Safety of Systems of Systems—A Policy-based Approach," PhD Thesis, University of York, 2007.

[11] H. Ross, "Functional Safety for Road Vehicles: New Challenges and Solutions for E-mobility and Automated Driving," Springer Verlag, pp. 115 – 119, 2016.

[12] H. Lambert, "Use of fault tree analysis for automotive reliability and safety analysis," Lawrence Livermore National Lab., CA (US), 2003.

[13] T. Stolte, G. Bagschik and M. Maurer, "Safety goals and functional safety requirements for actuation systems of automated vehicles," 19th IEEE Intelligent Transportation Systems (ITSC), 2016.

[14] German Aerospace Center (DLR), "PEGASUS RESEARCH PROJECT," [Online] Available: http://pegasus-projekt.info/en/home, accessed: March 28th 2018.

[15] C. Amersbach and H. Winner, "Functional Decomposition - An Approach to Reduce the Approval Effort for Highly Automated Driving," in 8. Tagung Fahrerassistenz, 22.-23. November, München, 2017.

[16] A. Reschka, Safety Concept for Autonomous Vehicles, In *Autonomous Driving – Technical, Legal and Social Aspects*, pp. 473–496, Springer Nature, 2016

[17] Automotive World, 2018. Daimler and Bosch jointly premiere automated valet parking in China. From: www.automotiveworld.com/news-releases/daimlerand-bosch-jointly-premiere-automated-valet-parkingin-china/. Accessed: November 2018

[18] M. Chirca, R. Chapuis, and R. Lenain, "Autonomous Valet Parking System Architecture," IEEE International Conference on Intelligent Transportation Systems (ITSC), 2015.

[19] U. Schwesinger, M. Bürki, J. Timpner, S. Rottmann, L. Wolf, ... & L. Heng. Automated valet parking and charging for e-mobility. In Intelligent Vehicles Symposium (IV), pp. 157-164, 2016.

[20] J. Hertzberg, K. Lingemann and A. Nüchter, "Mobile Roboter: Eine Einführung aus Sicht der Informatik," Springer-Verlag, 2012.

[21] K. Dietmayer, "Predicting of machine perception for automated driving," in Autonomous Driving: Technical, Legal and Social Aspects, M. Maurer, J. C. Gerdes, B. Lenz, and H. Winner, Eds.: Springer, 2016, pp. 407-424.

[22] F. Lotz, „Entwicklung einer Referenzarchitektur für die assistierte und automatisierte Fahrzeugführung mit Fahrereinbindung", PhD thesis, Technische Universität Darmstadt, Darmstadt, Germany, 2017, pp. 85-87

[23] A. Cacilo et al. "Hochautomatisiertes Fahren auf Autobahnen–Industriepolitische Schlussfolgerungen" Stuttgart: Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO , 2015.

[24] International Council on Clean Transportation, "European Vehicle Market Statistics Pocketbook 2017/18." (2017).

[25] Arbeitsgruppe Straßenentwurf, "Richtlinien für die Anlage von Straßen (RAS), Teil Querschnitte (RAS-Q 96)," Forschungsgesellschaft für Straßen und Verkehrswesen, Bonn.(a)(b)(c)(d), 1996.

[26] Bundesministerium der Justiz und für Verbraucherschutz, „Anordnung über den Bau und Betrieb von Garagen (GarBBAnO)," 1990.

[27] Bundesministerium der Justiz und für Verbraucherschutz, "Straßenverkehrs-Zulassungs-Ordnung (StVZO), " 2012.

[28] V. Schönemann, M. Duschek, H. Winner, "Maneuver-based adaptive Safety Zone for infrastructure-supported Automated Valet Parking," 5th International Conference on Vehicle Technology and Intelligent Transport Systems (in publication), 2019.

**APPENDIX**

***Table 6.***
***Derivation of functional safety requirements for derived safety goals***

| ID | Safety Goal (SG)/ Functional Safety Requirement (FSR) | SG |
|---|---|---|
| SG01 | Unintended activation of the valet parking function outside of the PAM-controlled parking area shall be prevented. | |
| FSR1.1 | The system shall detect if the automated vehicle's position is located within the handover zone. | |
| FSR1.2 | The system shall detect if the automated vehicle is in standstill. | SG01 |
| FSR1.3 | The system shall have the ability to activate and deactivate the valet parking function. | |
| FSR1.4 | The system shall not activate the valet parking function without user permission. | |
| SG02 | The integrity of the communication between the PAM and the vehicle shall be ensured. | |
| FSR2.1 | The system shall control transmitted safety relevant information for authentication, identification, error correcting, and manipulation. Transmitted data shall be encrypted. | |
| FSR2.1.1 | The system shall add to transmitted safety relevant information a check sum, a signature, a time stamp, and an identifier. Transmitted data shall be encrypted. | SG02 |
| FSR2.1 | The system shall receive safety-relevant information in time. | |
| SG04 | The vehicle shall not start moving during embarkment and disembarkment. | |
| FSR4.1 | The system shall detect the embarkment and disembarkment of passengers with its sensors. | |
| FSR4.1.1 | The system shall detect persons in the handover and handback zones. | SG04 |
| FSR4.1.2 | The system shall detect if doors are closed. | |
| SG06 | The system shall notify a human supervisor in case of a collision or fire. | |
| FSR6.1 | The system shall detect collisions. | |
| FSR6.2 | The system shall detect fire in the parking garage. | |
| FSR6.2 | The system shall stop the valet parking service by applying an emergency brake of automated vehicles in case of a fire. | SG06 |
| FSR6.3 | The system shall notify a human supervisor via a Human Machine Interface. | |
| SG07 | The system shall ensure that the vehicle stays within the (statically defined) drivable area during AVP. | |
| FSR7.1 | The system shall detect if a digital map of the parking garage was transferred. | |
| FSR7.2 | The system shall place the automated vehicle's trajectories within the drivable area. | SG07 |
| FSR7.3 | The maximum distance error of the automated vehicle's lateral control with respect to the lane center shall not exceed $W_{\mathrm{err,ego}}$. | |
| SG08 | The valet parking function shall be disabled if people are inside the vehicle. | |
| FSR8.1 | The system shall detect whether people are inside the vehicle. | SG08 |