# Functional Decomposition of Automated Driving Systems for the Classification and Evaluation of Perceptual Threats

Robin Philipp*, Fabian Schuldt* and Falk Howar†

**Abstract:** This contribution investigates dependability threats to automated driving systems pertaining to the environment perception. The identification of factors that can lead to safety-relevant system failures is essential for assuring safety of automated driving systems. We establish a comprehensive taxonomy for the classification of perceptual threats based on a functional decomposition of automated driving systems. Moreover, we use an exemplary lane keeping assistance system to describe different types of threats by using the taxonomy. The proposed taxonomy enables the opportunity for future work on a safety validation concept for perception components.

**Keywords:** Automated Driving Systems, Dependability, Functional Decomposition, Perception

## 1 Introduction

Safety validation of automated driving systems is a challenge that needs to be met for the introduction of self driving vehicles on public roads. However, safety validation concepts for higher[1] automation of vehicles are yet to be developed. One approach that is already present in other domains and currently researched for automated driving systems is the method of functional decomposition [2]. Instead of verifying the complex system as a whole, the verification of less complex single components is examined. Shifting from vehicle level verification to component level verification offers the advantage to apply more specific verification methods for different components. The verification process therefore gains more manageability and flexibility. However, a downside to a decomposition-based verification is that threats have to be accounted for separately, which are not safety-relevant for a single component, but can become safety-critical when propagating along the following components.

Regarding an automated driving system the verification of the perception component is challenging and therefore of special interest. The perception component must guarantee detection of all relevant objects with a certain quality in a fixed time interval to ensure

*Robin Philipp and Fabian Schuldt are with Volkswagen Group Innovation, Wolfsburg, Germany (robin.philipp@volkswagen.de).

†Falk Howar is a Professor at the Chair for Software Engineering, Technische Unversität Dortmund, Germany.

[1]An automated driving system with level 3 or higher as defined by the SAE [1]

safe behavior of the self driving vehicle in every possible scenario [3]. This requirement, however, is still too vague to be tested considering that there is an infinite amount of possible scenarios that can happen. In order to formulate meaningful requirements for environmental perception of an automated driving system it is essential to identify possible threats for a perception component, where they can potentially originate from and what influence they can have on the whole system performance. Moreover the identification of possible threats can enable a better understanding of dependability threats a perception component should handle itself, which threats should be handled by subsequent processing and which threats should not occur.

In this work, we establish a taxonomy for perceptual threats to automated driving systems. We characterize perceptual threats by functionally decomposing environmental perception components into its constituent processing parts. The resulting interfaces of the decomposed parts can then be used to derive potential dependability threats.

## 2 Related Work

In the following contributions related to functional decomposition and regarding dependability threats in general and specifically caused by the perception component are introduced.

Amersbach et al. [4] functionally decompose automated driving systems into six layers based on the human driving task for the definition of particular test cases. The decomposition layers are information access, information reception, information processing, situational understanding, behavioral decision, and action. The proposed decomposition is not further distinguished into more layers to be applicable for various automated driving systems. However, to define requirements for the perception component there is a need for the definition of dependability threats based on a more specific decomposition of the environmental perception and the subsequent processing into an environmental model. Therefore, in this work we focus on the information processing layer by decomposing it and identifying corresponding dependability threats. While the contribution by Amersbach et al. [4] lacks a more detailed decomposition of the task of perceiving the environment, Rosenberger et al. [5] take a closer look into the information processing layer and functionally decompose a lidar sensor system. They define differently abstract interfaces along the lidar data processing chain: the raw scan of the lidar sensor, the resulting point cloud and an object list which contains geometric and physical attributes. These interfaces are then used for a more detailed comparison of real and synthetically generated lidar measurement data using different metrics for different interfaces. A similar approach for the differently abstract representations of sensor data is also considered in this work.

A contribution that deals with the identification of perceptual uncertainty is proposed by Hanke et al. [6]. They examine the construction of a statistical sensor model for the virtual test of automated driving systems. To provide more realistic testing conditions they investigate the integration of lossy perception process characteristics into sensor models. To do so, they define the output interface of the model to consist of several model units where each of these units deals with one specific perception error. However, their work primarily focuses on objects and does not distinguish between different processing steps of sensor data. Another contribution for the classification of perceptual uncertainty is made by Dietmayer [3]. He describes the task of machine perception for automated driv-

ing and distinguishes its uncertainty into three uncertainty domains: state uncertainty, existence uncertainty and class uncertainty. State uncertainty deals with uncertainty regarding state variables such as position, kinematic or size of detected objects. Existence uncertainty refers to the uncertainty whether an object that was perceived actually exists. Class uncertainty describes the uncertainty concerning the semantic classification of detected objects. In this work we combine the classification of perception threats and where they can occur along the processing chain by considering differently abstract representations of sensor data. However, due to the different components processing the sensor data and therefore several potential causes for dependability threats arising, there is a need to differentiate these threats. A general approach to classify dependability threats is conducted by Avižienis et al. [7]. They establish basic concepts for the dependability of computing and communicating systems and distinguish threats to dependability into faults, errors and failures and define them subsequently. While faults are causes to errors, errors can propagate and eventually lead to a failure of a subsystem. Moreover, the characteristics of faults, errors and failures are discussed and different measurements to handle dependability threats are addressed. We adapt the definitions of Avižienis et al. to the perception component of automated driving systems.

While there are various contributions towards functional decomposition and categorization of perceptual threats and uncertainties, there is no known comprehensive taxonomy for the classification of threats to and from the perception component while also considering differently abstract levels of perception data in regards to the functional system architecture of automated driving systems.

# 3 Research Questions

**Research Question 1** *How can dependability threats to automated driving systems pertaining to perception components be characterized?*

For the establishment of a comprehensive taxonomy regarding dependability threats to and from perception components, we functionally decompose an automated driving system into components with well-defined tasks to receive precise interfaces. For that matter we extend existing approaches to functional decomposition (cf. [4], [5]) by respecting the individual steps of the perceptual processing chain of automated driving systems (cf. [8, p.47]). Moreover, we adapt the taxonomy for dependability threats by Avižienis et al. [7] (fault, error, failure) for the perception component of automated driving systems.

**Research Question 2** *What types of perception errors do exist and how can they be classified?*

When considering the task of perceiving the environment and processing different sensor data, there are several possibilities for the occurrence of errors from the raw scan of the environment up to the generated environmental model. Moreover, not every error or uncertainty has to be relevant for the automated driving system safely performing its driving task. Based on the functional decomposition, which is part of the first research question, we derive possible errors of perception components in this contribution. Furthermore, our proposed taxonomy for the classification of dependability threats to the perception component is evaluated by an exemplary lane keeping assistance system based on a camera.

# 4 Methodology

Robot systems are often distinguished into *Sense*, *Plan* and *Act* components. Adapted to a self driving vehicle, *Sense* includes the task of perceiving the surroundings and generating a model of the environment. *Plan* subsumes interpreting and predicting of future behavior of surrounding traffic participants based on the environmental model and then choosing a trajectory to be driven. *Act* stands for executing the planned trajectory by steering and accelerating or braking while also performing actions like indicating lane changes. This cycle is repeated for every scene[2]. A more detailed decomposition of automated driving systems is conducted by Amersbach et al. [4]. Figure 1 shows the decomposition layers of Amersbach et al. [4] mapped onto *Sense*, *Plan* and *Act* components.

Due to automated driving functions being highly complex systems consisting of various components, it is essential to identify the factors that can lead to safety-relevant system failures. In this section we propose a taxonomy for the classification of dependability threats to automated driving systems while focusing on the perception component. For that, we stick closely to the concept of faults, errors and failures introduced by Avižienis et al. [7] while also considering the differently abstract levels of sensor data representing the environment.

Avižienis et al. [7] define a fault as cause of an error. They distinguish between internal and external faults of a system. When a fault causes an error, it is active, otherwise it is dormant. An error is part of the total state of the system. When one or multiple errors cause the delivered service of the system to deviate from correct service, a failure occurs.

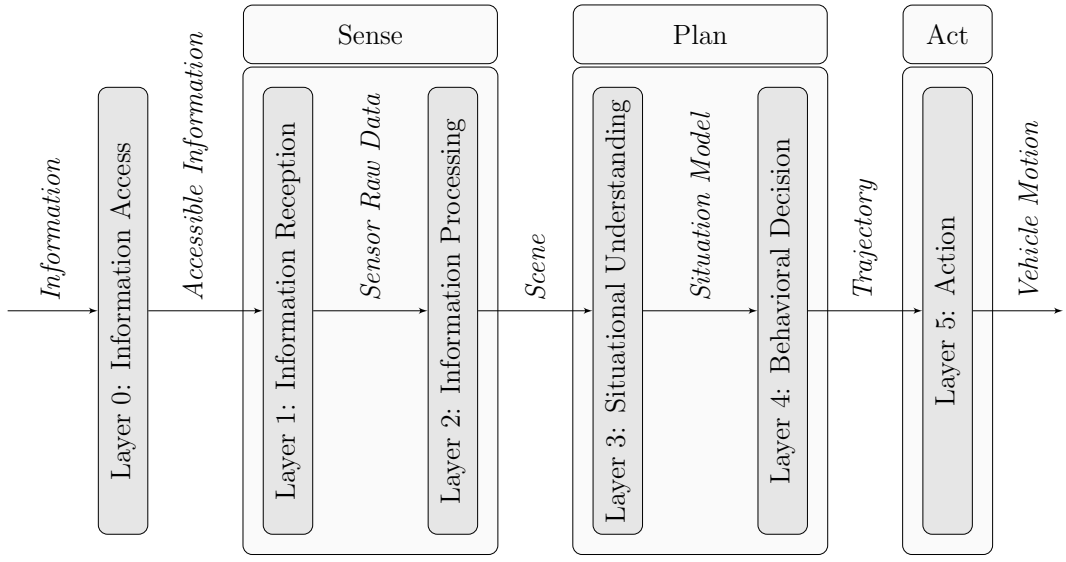


Figure 1: Functional decomposition by Amersbach et al. [4] mapped onto the *Sense-Plan-Act*-Paradigm

We assume that errors can occur in every step of processing environmental sensor data. Therefore we have to look at the data each component provides to the following

[2]We adopt the definitions of scene and scenario by Ulbrich et al. [9]

component. The raw scan of the surrounding environment is processed into a model of the surrounding environment and therefore exists in differently abstract levels during the processing. Considering the functional system architecture of automated driving functions [8, p.47] on the lowest level, there is a raw scan of the environment consisting of the data generated by the different sensors. Based on that different features like objects, traffic signs or road markings are detected. On the highest level all features are merged into a scene - a representation model of the environment. Figure 2 illustrates the processing of environmental sensor data and summarizes where the dependability threats, which are introduced in the following, can occur.

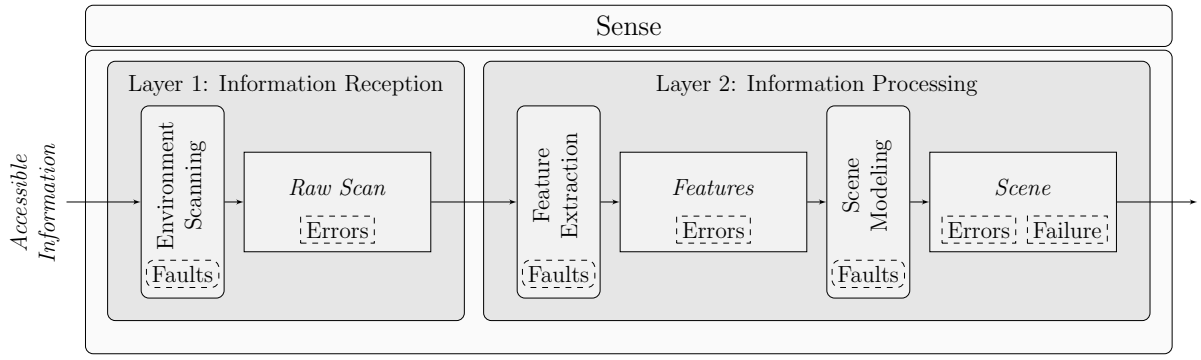


Figure 2: Processing chain of the perception component and potential occurrences of dependability threats relating to the *Sense* component as a system

## 4.1 Fault

Referring to our taxonomy, a fault is the cause of a perception error. Considering that there are different types of perception errors, there are also different types of faults to the perception component subsequently. On the one hand, errors that are propagating along the processing chain can be seen as faults to the resulting errors. On the other hand, each processing step of sensor data can contain its own faults (cf. Figure 2). When creating a raw scan of the environment, there are two types of faults: external faults and internal faults. External faults are disturbance variables like environmental conditions which can obscure the accessible information. Internal faults are either linked to the hardware, e.g. a systematic measurement error of a sensor, or are anchored in the software, e.g. a flawed point cloud generation out of received lidar beams. Faults to the processing of the raw scan into features are e.g. bugs in the object segmentation based on point clouds or images. When generating a scene, faults are either errors on feature level or present because of flaws in the scene modeling. An exemplary fault on this level is e.g. a incorrect lane matching algorithm for perceived vehicles.

## 4.2 Error

Each of the different representations of the environment can be inaccurate and therefore be subject to errors (cf. Figure 2). Examples for errors in these differently abstract representations are e.g. a blurred camera image on raw scan level, an object that is seen which is not existent on feature level and a correctly perceived traffic light that is,

however, linked to an incorrect lane on scene level. According to Avižienis et al. [7], many errors do not affect the system's external state.

### 4.3 Failure

According to Avižienis et al. [7] a system failure occurs when the delivered service deviates from correct service. In terms of the environmental perception, the question arises what correct service of the perception component of an automated driving system comprises. According to Dietmayer [3], correct service is delivered by a perception component when all relevant objects are detected with a certain quality within a fixed time interval. Moreover, the objects have to be correctly assigned to the traffic infrastructure. Hence, the delivered service deviates from correct service when either not all relevant objects are seen or when there is a mismatch in the modeled scene. In this case, the automated driving system would not be able to evaluate the situation appropriately anymore and therefore not be capable of performing its driving task safely enough.

## 5 Classification of Perception Error Types

In the following, both errors on raw scan level and on feature level are examined. To that end, raw data errors for the sensor technologies camera, Lidar and Radar are briefly discussed. Consecutively, we will derive errors on feature level by individually considering the single parts that make up the environment. While doing so, we are also referring to commonly used approaches on how this accessible information is included into the scene modeling.

### 5.1 Raw Scan

Errors on raw scan level are anchored in the raw data[3] generated by the deployed sensors. Due to the fact that different types of sensors generate different kinds of raw data, it is not possible to define common errors on this level of environmental representation which are applicable for every type of sensor. Instead the raw data of the different sensor types has to be looked at separately. Raw data generated by a camera are in general images consisting of pixels. Image noise due to the level of illumination or image distortions caused by effects like rolling shutter are therefore examples for camera raw data errors, as well as whole missing image sections (e.g. missing traffic signs due to flickering when capturing a variable-message sign over time). A Lidar sensor emits laser beams into the environment and measures their echoes. For each laser beam, a measured distance is recorded and, depending on the sensor implementation, other values like intensity or echo-puls-width are also obtained. Therefore, the raw data of a lidar consists of tuples of measured values. [5] Uncertainties in these measurement tuples due to noise, non-measured echoes or broken down channels can be considered as lidar raw data errors. According to Holder et al. [10] raw data of a radar is defined as the range-doppler-beam spectrum at the interface after the spectral analysis of the sensor readings and before the subsequent post-processing, which typically starts with a thresholding. Common distortions that occur in these raw data are defined as artifacts by Holder et al. [10]. While these artifacts obscure the

[3]We adopt the definition of raw data by Holder et al. [10].

accessible information, they can be seen as errors. Causes of such artifacts are e.g. mirror reflections, aliasing or electronic noise in the sensor [10].

## 5.2 Features

Errors on feature level are dependent from the different features that are considered for the scene modeling. For the definition of errors on this level it does not matter based on which kind of raw data the feature was extracted. Errors regarding features can be derived by looking at the elements which the environment consists of. Subsequently, we first decompose the environment into its parts. According to Ulbrich et al. [9] the environment consists of movable objects and the scenery. The scenery is then split up into the lane network, vertical elevation, stationary elements and environment conditions. Lanes and conflict areas belong to the lane network. Stationary elements are among other things obstacles, curbs, traffic signs and traffic lights. Figure 3 illustrates the decomposed elements of the environment.

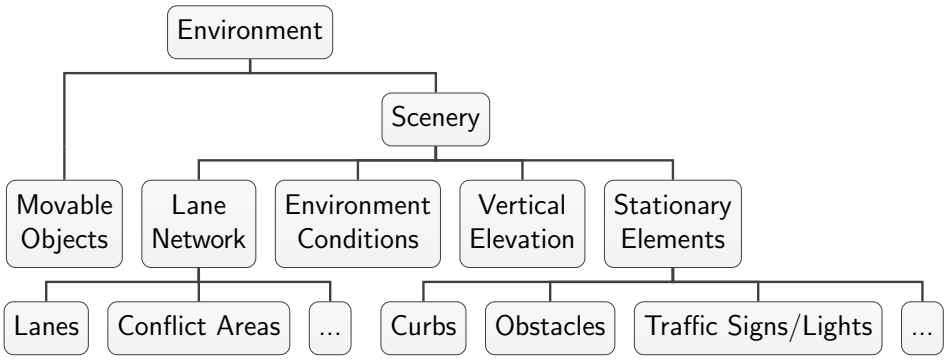


Figure 3: Elements of the environment according to Ulbrich et al. [9]

One part of the environmental perception is to detect existing movable objects. Whenever an object is not detected an object is missed by the environmental perception. A non-existing movable object, that is detected, is called a phantom object. Both of these cases can increase the risk during automated driving. But even when an existing object is perceived, there is an uncertainty that comes with every measurement. Ideally a movable object is represented by one bounding box instead of multiple ones. Regarding static non-continuous attributes of movable objects, like the classification, it is trivial to define that any deviation from the real classification is an error. However, concerning attributes that are continuous (e.g. dimensions) and attributes that are additionally dynamic and therefore can change over time (e.g. position and kinematics), it is not obvious when an uncertainty could propagate into a safety relevant error. This depends on the relevance of the perceived objects to the driving task as well as the robustness of the automated driving system. Possible errors regarding movable objects are summarized in Figure 4.

Traffic signs and lights are mandatory for managing traffic flow. For an automated driving system to abide by the road traffic regulations, traffic signs and lights need to be correctly captured, matched to their corresponding lanes and considered in the path planning. Regarding the definition of perceptual errors related to traffic signs, we differentiate between missed traffic signs, phantom traffic signs and correctly perceived traffic signs, which are, however, afflicted with uncertainties. Because traffic signs are static

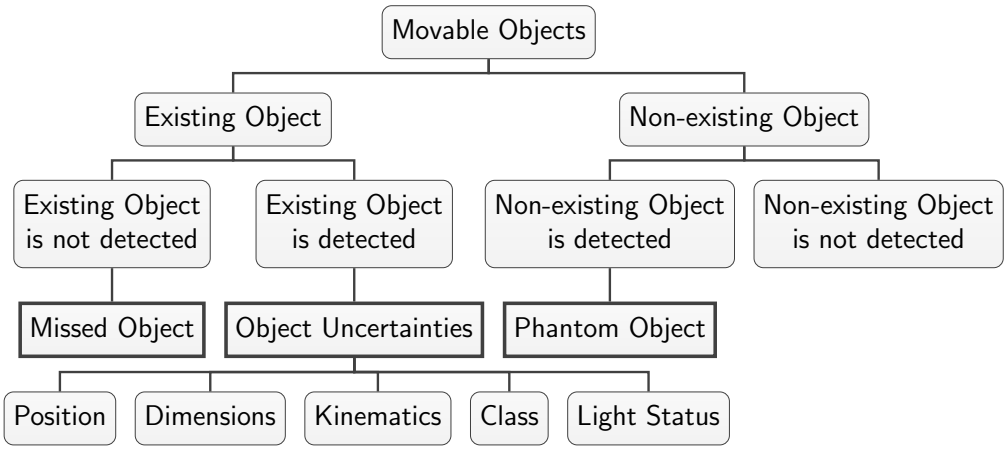


Figure 4: Errors regarding movable objects

(unlike movable objects), it is easier to define when an uncertainty might propagate into a safety relevant error. The position of the traffic sign needs to be captured accurately enough to be correctly matched to its corresponding lane. For the interpretation of the traffic sign both the class (e.g. a speed limit) and the value (e.g. $80\,\mathrm{km\,h^{-1}}$) have to be recorded correctly. While the value of most traffic signs does not change over time, traffic lights and variable-message signs are dynamic elements and therefore do not exclude changes regarding their value (e.g. a traffic light changing from green to yellow). Figure 5 summarizes the introduced errors.

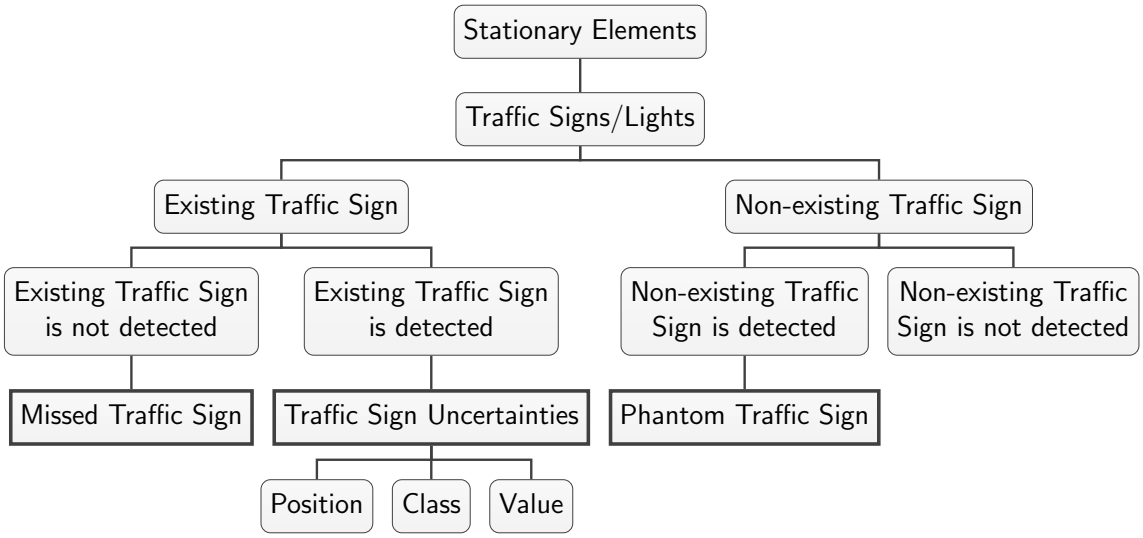


Figure 5: Errors regarding traffic signs

Lanes are defined by lane markings which imply the lane boundaries. In urban areas lane boundaries are additionally represented by curbs. Multiple lane marking segments form a continuous lane marking. For the automated driving system to construct these continuous lane boundaries, the lane marking segments need to be captured by the environmental perception. Moreover, overlapping lanes form conflict areas. We define overlooked lane marking segments as missed lane marking segments and detections of non-existing lane marking segments as phantom lane marking segments. Detected lane

marking segments can be uncertain in regards to their exact position and characteristics (e.g. curvature) and their class (e.g. solid, dashed, curbs), which also includes the color for lane markings (usually white or yellow). The class attribute is mandatory to know whether a lane boundary can legally be crossed and hence needs to be considered by the path planning. Any deviation from the real class can subsequently be considered as an error. Position and characteristics of lane marking segments are continuous values and need to be accurate enough to create a precise lane network. As soon as the lane network cannot be clearly derived by the detected segments, the uncertainty can be interpreted as safety-critical. Errors regarding lane marking segments are summarized in Figure 6.

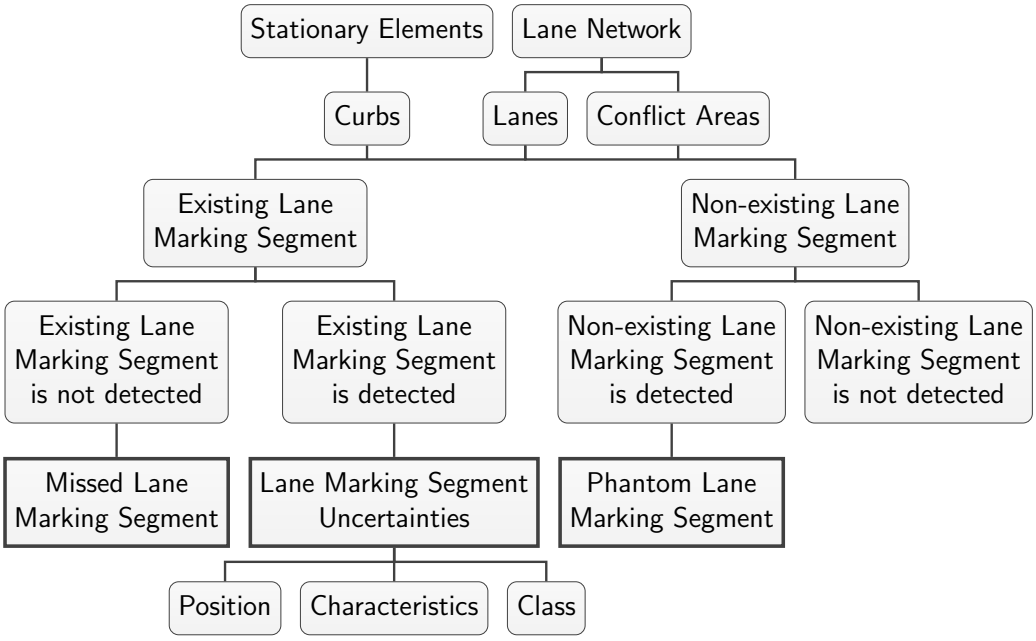


Figure 6: Errors regarding the lane network

One approach to capture vertical elevation is by estimating the ground plane. This information is not only important for path planning, but can also be used to improve quality of object detection [11]. Regarding a point in the environment, it either belongs to the ground plane or not. Subsequently, errors regarding ground mark classification are either overlooked ground marks or misleadingly classified ground marks (cf. Figure 7).

The integration of surrounding obstacles and not accessible areas into the path planning of a robot system is often implemented by creating an occupancy grid. For the creation of an occupancy grid, the environment is divided into grid cells. Afterwards, for each grid cell it is determined whether the cell is occupied or not. Hence, possible errors regarding the occupancy grid are either occupied cells which are classified as not occupied (overlooked obstacle) or not-occupied cells which are misleadingly classified as occupied (not-existing obstacle) (cf. Figure 8).

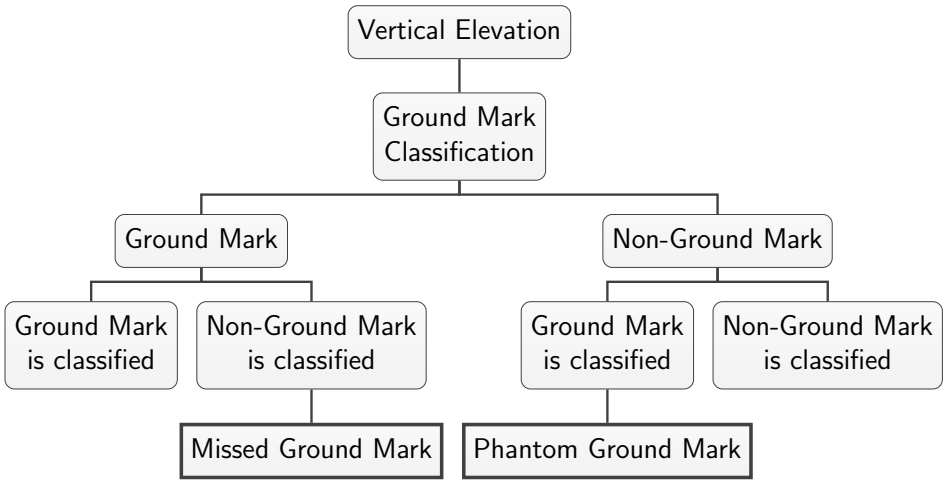


Figure 7: Errors regarding ground mark classification

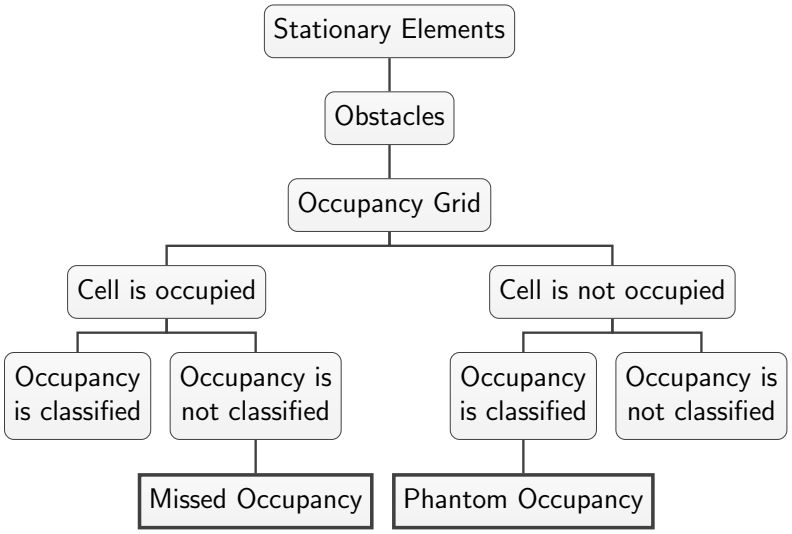


Figure 8: Errors regarding occupancy

# 6 Case Example: Lane Keeping Assistance System

To show the applicability of the presented taxonomy, we consider a lane keeping assistance system as case example and its handling of exemplary dependability threats in a hypothetical scenario. Task of the considered assistance system is to detect lane marking segments in a camera image, model them to lanes and subsequently assist the driver with lateral control of the vehicle to keep the lane. Figure 9 shows the functional architecture of the *Sense* component of the exemplary system and one possible hazard, which is analyzed in the following.

We now consider for the system to run into a scenario where the correct service cannot be maintained without making adjustments. While the camera captures lane marking segments, we assume a low hanging sun to blind the camera for a short time and therefore cause overexposed images. That results in *Errors* in the raw data because the image misses parts of the environment and therefore does not represent all of the accessible information. Extraction of lane marking segments based on these images leads to *Missed Lane Marking*

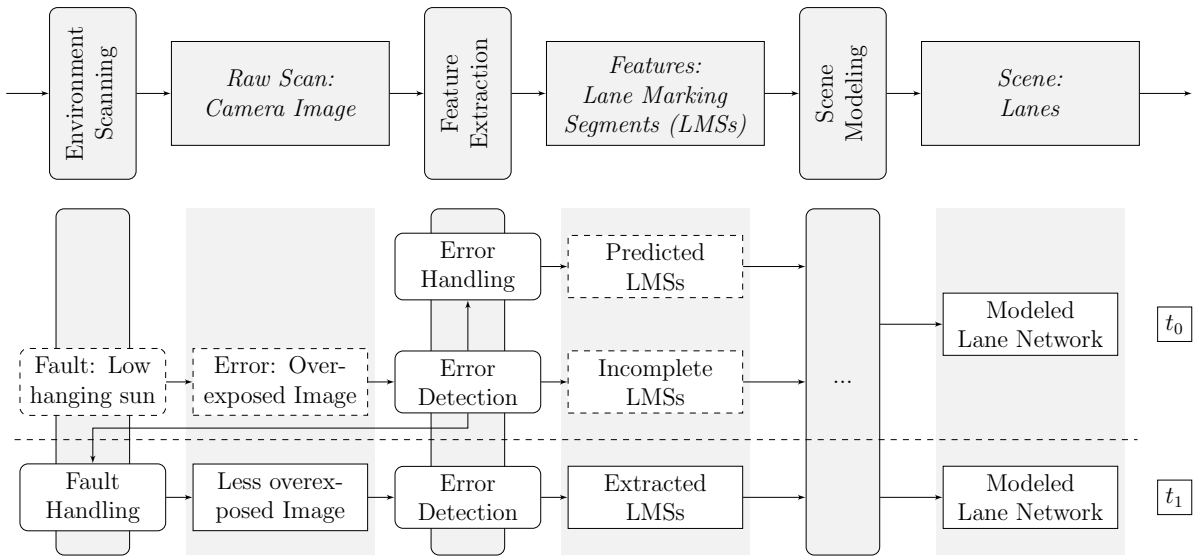


Figure 9: Case Example: Handling of exemplary dependability threats for a Lane Keeping Assistance System

*Segments* and therefore an incomplete set of lane marking segments. To deal with these false negative errors, the hypothetical system contains a component for *Error Detection*, which can trigger *Fault Handling* of the environment scanning to avoid *Errors* in the images of upcoming iterations and trigger *Error Handling* to cope with defective images for the current iteration. According to Avižienis et al. [7], the combination of *Fault Handling* and *Error Handling* form *System Recovery*.

In this case example, *Error Handling* is implemented by *Compensation* (cf. [7]). The compensation comprises relying on predicted lane marking segments that were generated during feature extraction of earlier iterations (e.g. by using a Kalman-Filter). Both predicted and the set of incomplete lane marking segments are then provided to the subsequent lane modeling. Simultaneously to *Error Handling*, *Fault Handling* in the environment scanning is triggered. To cope with the low hanging sun and to avoid *Errors* in the camera images, camera settings are reconfigured (e.g. light shade and exposure time). Therefore, according to Avižienis et al. [7] *Fault Handling* in this case means *Reconfiguration*. This results in less overexposed camera images for upcoming iterations.

Based on the executed *System Recovery*, lane marking segment extraction and subsequent lane modeling can then be sufficiently precise again for the *Sense* component to deliver correct service without considering predicted lane marking segments of an earlier iteration.

# 7 Conclusion and Future Work

In this contribution a taxonomy for the characterization of dependability threats to perception components is established. For that, the task of environment perception is functionally decomposed and thus precise interfaces are created. Subsequently, the concept of faults, errors and failures is implemented to include causalities between the threats along the processing chain of environmental perception. For the classification of perceptual error

types, both the raw scan of the environment and extracted features are closer examined. Within the scope of this work, raw data of camera, Lidar and Radar is briefly discussed. For the definition of perceptual errors on feature level, possible errors are derived by splitting up the environment into its subsequent parts and considering in which aspects extracted features can be flawed. Since for the definition of these errors the components of the environment established by Ulbrich et al. [9] have been considered, we do not claim for our error classification to be exhaustive. The proposed taxonomy is supported by an exemplary case example.

Since our focus was deducting perceptual errors on feature level, future work should also address dependability threats on raw scan and scene level in more detail, especially regarding possible faults. Moreover, future work should deal with the influence of different kind of threats on the robustness of automated driving systems focusing on the *Sense* component. Acquiring information about how precise environmental perception must be is a key step for safe system design. Therefore, not only false negative and false positive errors, but also uncertainties of true positives should be investigated in more detail. Additionally the importance of surrounding objects has to be considered, since not every object is of relevance for the automated driving system. Subsequently, not every error is safety-relevant and thereby results in higher safety risks of automated driving system. Defining and also refining of safety requirements revolving around the environmental perception will be a key challenge to solve for the safety validation of automated driving systems.

# References


[1] *SJ3016: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*, Jun 2018.

[2] B. Lightsey, "Systems Engineering Fundamentals," Department of Defense - Systems Management College, Fort Belvoir, VA, USA, Tech. Rep., 2001.

[3] K. Dietmayer, *Predicting of Machine Perception for Automated Driving.* Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 407–424.

[4] C. Amersbach and H. Winner, "Functional decomposition: An approach to reduce the approval effort for highly automated driving," in *8. Tagung Fahrerassistenz.* München: Lehrstuhl für Fahrzeugtechnik mit TÜV SÜD Akademie, 2017.

[5] P. Rosenberger, M. Holder, S. Huch, H. Winner, T. Fleck, M. R. Zofka, J. M. Zöllner, T. D'hondt, and B. Wassermann, "Benchmarking and Functional Decomposition of Automotive Lidar Sensor Models," in *2019 IEEE Intelligent Vehicles Symposium (IV)*, Paris, France, 2019.

[6] T. Hanke, N. Hirsenkorn, B. Dehlink, A. Rauch, R. Rasshofer, and E. Biebl, "Classification of Sensor Errors for the Statistical Simulation of Environmental Perception in Automated Driving Systems," in *2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)*, Nov 2016, pp. 643–648.

[7] A. Avižienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 1, pp. 11–33, Jan 2004.

[8] F. Schuldt, "Ein Beitrag für den methodischen Test von automatisierten Fahrfunktionen mit Hilfe von virtuellen Umgebungen," Ph.D. dissertation, Technische Universität Braunschweig, 2017.

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

[10] M. F. Holder, C. Linnhoff, P. Rosenberger, C. Popp, and H. Winner, "Modeling and simulation of radar sensor artifacts for virtual testing of autonomous driving," in *Automatisiertes Fahren*. München: Lehrstuhl für Fahrzeugtechnik mit TÜV SÜD Akademie, 2019.

[11] J. Rieken, R. Matthaei, and M. Maurer, "Benefits of using explicit ground-plane information for grid-based urban environment modeling," in *2015 18th International Conference on Information Fusion (Fusion)*. IEEE, 2015, pp. 2049–2056.