## 2.2.2 Elements

Fail-safe and fail-degraded capabilities are implemented by the elements described in detail below. The general capability regarding cybersecurity as described in Section 2.1.4 has to be considered for each element. However, the specific cybersecurity measures are not described in each element, as this depends on the overall cybersecurity architecture.

### 2.2.2.1 ENVIRONMENT PERCEPTION SENSORS

The environment perception sensors cluster should capture all relevant external information to create a world model. Entities to detect are, but are not limited to, infrastructure defining the allowed area of driving, (vulnerable) road users, obstacles, traffic signs and acoustic signals.

Sensor types: As of today, a single sensor is not capable of simultaneously providing reliable and precise detection, classifications, measurements, and robustness to adverse conditions. Therefore, a multimodal approach is required to cover the detectability of relevant entities. In more detail, a combination of the following technologies shall provide suitable coverage for the given specific product:

**CAMERA**
Sensor with the highest extractable information content as sensor captures visible cues similar to human perception. Main sensor for object/feature type classification. Limited precision in range determination, high sensitivity to weather conditions.

**LIDAR**
High-precision measurement of structured and unstructured elements. Medium sensitivity to environment conditions.

**RADAR**
High-precision detection and measurement of moving objects with appropriate reflectivity in radar operation range, high robustness against weather conditions.

**ULTRASONIC**
Well-established near-field sensor capable of detecting closest distances to reflecting entities.

**MICROPHONES**
Public traffic uses acoustic signals to prevent crashes and regulate traffic, e.g. on railway intersections. Thus, devices capturing acoustic signals are required for automation levels where the systems need to react to these.

Sensor sets need to be capable of detecting sensing degradation, such as sensor blindness, de-calibration or misalignments. Possible methods for this could be based on sensor-specific measures or cross-sensor comparisons and calibration methods.

#### SENSOR ARRANGEMENT

The design of the sensor cluster needs to cover the ODD of the respective functionality. For example, a sensor cluster designed for a system on highways needs to cover ranges and precision levels that are different to those of urban scenarios. The detectability of external entities strongly depends on the material these are made of. This publication considers a combination of at least two, if not three, different measurement technologies to implement susceptibility of the sensor cluster to all relevant elements in the real world. This approach further enables the simultaneous capturing of the majority of elements with at least two different measurement technologies. Subsequent processing steps are thus enabled to provide detection rates superior to individual sensor detection rates.

However, errors and perception failure may still occur even when an iterative design approach is followed and ISO 26262 recommendations are complied with. In the unlikely event of severe sensor degradation or E/E faults, the sensor arrangement needs to be laid out such that it enables the safe capturing of relevant elements in degraded mode until the safe state is reached.

### 2.2.2.2 A-PRIORI PERCEPTION SENSORS

### 2.2.2.2.1 HD MAP

#### HD MAP AS A RELIABLE SENSOR

An in-vehicle map has never played a safety-related role as it could do in automated driving. For a relatively long period of time, the capabilities of onboard sensors alone will be insufficient to meet the high reliability, availability and safety requirements of the automated vehicle system in certain situations. A HD map is therefore necessary as a reliable off-board sensor containing carefully processed a-priori information to “detect” features that are not easily detectable by on-board sensors or to provide a redundant source of information for on-board sensors, including location-based ODD determination, environment modeling in adverse conditions and precise semantic understandings in complex driving situations. In situations where on-board sensors cannot reliably detect features, the HD map can be utilized as a more reliable redundant source of information.

### RELIABLE MAP ATTRIBUTES AND HOW TO IDENTIFY RMA SETS

Multiple map attributes are utilized in location-based ODD determination, such as lane markings, road markings, traffic signs, light poles, guardrails or artificial markers. However, some attributes are not always "reliable" to detect due to reasons including occlusion, abrasion or frequent changes. Therefore, reliable map attributes (RMAs) should be detected correctly in safety-relevant use cases, so that collectively they can meet the low location-based ODD determination false positive rate requirement.

RMAs should have the following properties:

- Fused with on-board sensor inputs, a combination of RMAs should be a sufficient condition to infer that the automated vehicle is reaching the boundary of the ODD.
- RMAs should be reliably detectable by onboard sensors within the ODD.
- RMAs should be observed with a relatively low real-world rate of change, so that the RMA failure rate can be controlled to an acceptable risk level.
- The quality and freshness of RMAs should be verifiable within an acceptable time delay.

As stated above, only a subset of all map attributes is related to safety. The method for abstracting the complete list of RMAs is project-specific (these include but are not limited to the development examples outlined in Section 1.2).

### RMA FAILURE MODES AND CORRESPONDING MEASURES

Due to its nature of being offline but not processed in real time, a HD map has the advantage of being less probabilistic compared to onboard sensors. However, this also results in the limitations of a HD map when employed in safety-related use cases. RMA failure occurs due to deviations between the map and reality, possibly arising from:

- Errors introduced during source data collection, map creation and distribution processes
- Errors introduced due to real-world changes, which can further be classified as:
  - INTENDED CHANGES: Typically by a local road authority (e.g. planned road construction)
  - UNINTENDED CHANGES: Typically due to external forces or normal wear (e.g. a piece of guardrail is damaged in a collision and not recovered before the next road maintenance)
  - MALICIOUS CHANGES: Typically due to an unauthorized/malicious action (e.g. unauthorized removal of a speed limit sign)

The above errors should be addressed appropriately to ensure that the automated driving system is able to reach an accepted risk level. Failures relating to procedural deficiency can be avoided by a quality assurance system including but not limited to those articulated in established map quality standards (e.g. ISO 19157, ISO/TS 19158, TS 16949). Failures relating to planned road changes can be avoided by incorporating road change plans from a road authority into the map updating process. Meanwhile, as indispensable public information, road construction and maintenance plans should be fully transparent and easily accessible by all map providers. Errors as a result of real-world changes are difficult to monitor and control, thus they should be carefully analyzed. Changes of RMAs can be divided into two categories based on the impact that they have for the use case of an automated vehicle system:

**MINOR CHANGES**

do not impede or exceed the specification tolerance for the given RMA-associated functionalities in safety-relevant use cases (e.g. dents in guardrails or lane markings with small parts missing)

**MAJOR CHANGES**

significantly reduce the detection rate and exceed the specification tolerance for the given RMA and may lead to localization errors (e.g. missing guardrails for a certain distance due to a severe crash)

Therefore, failures of RMAs due to major changes should primarily have an impact on the failure rate of location-based ODD determination. Several measures can be implemented to mitigate random failures. First, RMAs should be carefully chosen so that the possibilities of unplanned major changes are limited and can be statistically proven. Second, an effective mechanism for map updating or maintenance is critically important. A map updating or maintenance platform that comprises sensor data collected from multiple inputs, including but not limited to survey car fleets, massively deployed intelligent vehicles (e.g. vehicles with the ability to collect sensor data), high resolution satellite images and/or road infrastructures with surveillance sensors, can effectively detect the random road changes and lower the risk of random RMA failures.

**OTHER SAFETY CONSIDERATIONS:**

Map modification after initial creation is a mandatory map processing step in certain regions of the world. (NPC, 2017). Safety-relevant content should not lose reliability as a result of these measures. A sound safety analysis and eventual measures are required to continue to enable the use of maps in the vehicle.

Furthermore, malicious changes to map content need to be prevented. As a HD map is an off-board sensor, cybersecurity should be considered from creation through to storage and distribution. This is discussed in greater detail in Section 2.1.5.

#### 2.2.2.2.2 GNSS

Absolute GNSS position contributes to the automated vehicle system safety. Consequently, not only accurate but also trustful absolute GNSS positions are required for location-based ODD determination. A time window of GNSS position validity with integrity should be defined, as various levels of accuracy, integrity and availability will be in place while the automated vehicle is in operation. Continuity metric is no longer the main parameter of GNSS-based positioning with integrity.

A higher availability of GNSS-based positioning can be achieved by implementing multi-frequency and multi-constellation GNSS antennas and receivers, which is a prerequisite for interoperability and compatibility between GNSS constellations and radio frequency signals.

GNSS sensor functionality relies on the direct visibility of satellites. Consequently, GNSS-based positioning cannot have high continuity and availability due to environmental obstructions such as bridges or tunnels. In good GNSS conditions, position accuracy with high integrity, detection of loss of lock and fast convergence times after GNSS outages are therefore substantial for an automated driving system. Reaching accuracies and integrity performance metrics simultaneously is enabled by GNSS receivers that can utilize data received from an adequate number of satellites (e.g. 10 or more satellites) and additional data from correction services. These services need to implement fast processing, frequent updates and dedicated correction sets to support a best possible GNSS positioning algorithm.

A further aspect to cover is the assessment of new signals with respect to interferences in ARNS/RNSS bands or other interferers or jammers that could harm GNSS positioning performance. Integrity can be given only if spoofing is addressed at the GNSS component level.

#### 2.2.2.3 V2X

V2X may provide valuable information to the automated driving system. However, safety and security aspects should be considered to ensure a proper integrity. In addition, the automated driving system should operate safely in conditions where V2X is not available.

An example for this could be providing redundancy for the detection of traffic signal state that else could be detected only by camera. There is currently no redundant method for detecting traffic signal states without additional communication from the infrastructure.

#### 2.2.2.4 SENSOR FUSION

There is a variety of sensor fusion algorithms, each of which requires individual analysis with respect to hardware or software error robustness or input data error sensitivity, for instance. Thus, a carefully selected approach incorporating inductive, deductive and data-driven iterative design procedures, for example, should be followed.

Generally, input checks that determine the plausibility of individual sensor data, fusing multiple weighted input sources, and accumulating sensor data are possible strategies. Hardware and software diversity for the implementation of functionalities with the highest required error robustness should be considered.

While individual sensors can provide information about their current detection capabilities and range, sensor fusion can add substantial value in determining the current horizon of full sensor cluster perception, which may help to monitor the actual sensor performance. Regarded as a cross-referencing mechanism, sensor fusion can enable the detection of individual sensor limitations that are not detectable by the individual sensor itself.

### 2.2.2.5 INTERPRETATION AND PREDICTION

Prediction is an essential element for the realization of an automated driving system. The automated vehicle should behave almost like a manually driven vehicle, so that its behavior is predictable to other participants and does not disturb the traffic flow. Actual traffic is based on knowledge, rules and experience and how (vulnerable) road users will usually act next. To adapt this behavior for the automated vehicle, the vehicle needs a prediction based on a reliable interpretation of the situation.

Interpreting the current environment enables the prediction of other (vulnerable) road users. It is not possible to base safety on probabilistic calculations without measurable or common properties. Human road users in particular can make irrational decisions. On the other hand, if a function is provided that is always planning for the worst-case scenario, it may include actuations which provide risks to the overall system in other ways that are unacceptable for the goal of attaining the capabilities.

A solution may consider a combination of the following properties:

- Predict only a short time into the future. The likelihood of an accurate prediction is indirectly related to the time between the current state and the point in time it refers to (i.e. the further the predicted state is in the future, the less likely it is that the prediction is correct).
- Rely on physics where possible, using dynamic models of (vulnerable) road users that form the basis of motion prediction. For example, a vehicle driving in front of the automated vehicle will not stop in zero time on its own. Thus, a classification of relevant objects is a necessary input to be able to discriminate between various models.
- Predictable drive planning should consider the compliance of other (vulnerable) road users with traffic rules to a valid extent. For example, the automated vehicle should cross intersections with green traffic lights without stopping, relying on other (vulnerable) road users to follow the rule of stopping at red lights. In addition to this, foreseeable non-compliant behavior to traffic rules (e.g. pedestrians crossing red lights in urban areas) needs to be taken into account, supported by defensive drive planning.
- Situation predication to further increase the likelihood of (vulnerable) road user prediction being correct. For example, the future behavior of other (vulnerable) road users when driving in a traffic jam differs greatly to their behavior in flowing traffic.

The Interpretation and Prediction system should understand not only the worst-case behavior of other (vulnerable) road users, but their worst-case reasonable behavior. This allows the Interpretation and Prediction system to make reasonable and physically possible assumptions about other (vulnerable) road users. The automated driving system should make a naturalistic assumption, just as humans do, about the reasonable behavior of others. These assumptions need to be adaptable to local requirements so that they meet locally different „driving cultures“.

### 2.2.2.6 LOCALIZATION

An automated driving system must reliably know its location as precisely as required depending on the system design. Different approaches can be applied when determining an automated driving vehicle's position on a HD map, including:

**GNSS-BASED LOCALIZATION**

This approach consists of GNSS, odometry and correction services to achieve precise global coordinates, and matching GNSS measurements to an HD map to obtain a relative position on the map.

**ENVIRONMENT-PERCEPTION-SENSOR-BASED LOCALIZATION**

Based on a rough global coordinate obtained by GNSS and odometry, this approach matches real-world features (such as natural or artificial landmarks) or point clouds detected by Environment Perception Sensors with respective features or point clouds on an HD map to localize the automated driving system on the map.

Both localization approaches are subject to errors caused by performance limitations of the sensors involved, or sensor processing chains (or by real failures in either of these), or by multiple elements involved in the procession.

Localization needs to be implemented such that is robust against at least single, simple and timebound sensor performance issues. This is necessary due to the nature of the sensors (e.g. limitations of GNSS in tunnels, light conditions affecting vision sensors, etc.). Therefore, a sound safety analysis of involved inputs with relevant failure modes, performance limitations, availabilities, and respective effects on the position estimation needs to be carried out. As a single localization approach may not be sufficient for all relevant situations of an automated driving system, a redundant system incorporating both of the above localization approaches to provide seamless localization with the required integrity can increase localization performance.

### 2.2.2.7 ADS MODE MANAGER

The ADS Mode Manager has to fulfill the task of safely changing between manual and different automated driving modes. For the activation of an automated driving mode, this means obtaining all information to check whether all prerequisites such as the ODD are fulfilled (e.g. whether the automated vehicle is on the correct road type, check the weather conditions, etc.). Required information can be transferred from a backend to the vehicle, directly measured, calculated or derived from statistics.

There are many reasons for requesting that the automated driving system be deactivated. These include requests from the vehicle operator or from a monitor, or as a result of leaving the ODD or a monitor being unavailable. If such a request or reason is perceived, the relevant MRC should be targeted (see Section 2.1.7).

Reasons for changing modes may be triggered based on the vehicle state, user state determination or monitors. For example, a deactivation request arising from the vehicle state may be a fuel gauge, tire pressure or other vehicle systems. Examples arising from the user state include the belt status or vehicle operator attention. Based on the information from one or more monitors, the ADS Mode Manager has to decide whether to change to a degraded mode or issue an MRM to reach an MRC. However, these examples are strongly linked to the specific automated driving system.

Checking whether the automated vehicle is inside or outside of the ODD is a complicated task, because an ODD definition covers a widespread set of requirements. Being able to sense all of them is crucial for activation and deactivation. Table 5 lists all combinations of errors that may occur in the event of erroneous detection:

**Determining the Vehicle's Location**

| | | Reality | |
|---|---|---|---|
| | | Vehicle within ODD | Vehicle outside ODD |
| System Output | Vehicle within ODD | True Positive (TP) | False Positive (FP) |
| | Vehicle outside ODD | False Negative (FN) | True Negative (TN) |

*Table 5: Determining the Vehicle's Location*

Only the false positive combination is safety-related. The system erroneously detects being inside the ODD when in reality the vehicle is outside of the ODD. The behavior and consequences of automated driving operation outside of the ODD are by definition not safe enough. Therefore, appropriate safety measures are required to ensure the safe detection of ODD areas and limits. Being inside the ODD but detecting being outside will result only in deactivation, which is carried out in a safe manner.

### 2.2.2.8 EGOMOTION

Egomotion describes the actual state of the car in terms of yaw rate, longitudinal acceleration, lateral acceleration and more. Further values describing the vehicle state may include vehicle speed or slip angle. Some of the data can directly be measured using an inertial measurement unit, wheel ticks or derived from other sensors such as cameras. Other Egomotion data cannot be read directly and so can be estimated with the aid of other sensors using mathematical models, for example. Because Egomotion is an input for several other elements, it should be fail-degraded to fulfill the capabilities. There are numerous ways to achieve this, so implementations will vary considerably.

### 2.2.2.9 DRIVE PLANNING

Creating a driving policy that can drive in a collision-free manner without compromising comfort or traffic flow is a challenge in automated driving. A promising solution lies in defining formal rules, such as the examples of a theoretical approach (Shalev-Schwartz, Shammah, & Shashua, 2018) and hierarchical sets of rules (Censi, et al., 2019). These theoretical rules must still be applied to the complexities of real-world mixed traffic, and the resulting evaluation of the effect on traffic must still take place.

These formal rules may include, but are not limited to, the following examples. They should be followed during implementation for all drive modes.

#### EXPLICIT TRAFFIC RULES

- Conform to all applicable traffic rules within the ODD that the automated vehicle is operating in, taking regional differences in traffic rules into special consideration. Roads, signaling elements and other examples of infrastructure are the physical embodiment of the explicit traffic rules, e.g. a STOP sign or double solid lane marking.

#### IMPLICIT TRAFFIC RULES

- Maintain a safe longitudinal and lateral distance from other objects to avoid collision.
- Right of way is given, not taken. Following the safety-first principle, non-compliance of other (vulnerable) road users with traffic rules should be expected and dealt with defensively.
- Be cautious in areas where other (vulnerable) road users may be occluded. If information from Interpretation and Prediction, the ODD, or other sources indicates that there is a potential for occluded objects, the automated vehicle should be prepared for the possible sudden appearance of other vulnerable road users such as pedestrians.
- If it is possible to perform a legal and safety-assured maneuver to evade a potentially unsafe situation, then the automated vehicle should do so.
- If it is not possible to evade an unsafe situation without prioritizing traffic rules, then it may be possible for the automated vehicle to prioritize traffic rules while making a safety-assured maneuver.

Formal models can facilitate traceability between driving decisions (down to the level of specific software or hardware pieces) and these rules. The process of formalizing the specific parameters to be used within these rules and their associated hierarchies is a delicate balance. Uncertainty could be reduced if a set of rules, their parameters and their hierarchy are agreed on in advance. It should be noted that safe driving is inherently based on assumptions about other (vulnerable) road users (e.g. maximum deceleration). This is particularly important for occlusion scenarios. On the other hand, driving too defensively may confuse other (vulnerable) road users and could lead to a safety incident.

Such rules can be further described within the context of a set of specifically defined constructs:

- A DANGEROUS SITUATION is a state of the automated vehicle such that there exists the possibility of a collision, e.g. the safe longitudinal or safe lateral distance has been violated. This could be caused by the automated vehicle itself, another (vulnerable) road user or due to a change in the environment.
- The DANGEROUS TIME is all the time(s) in which the automated vehicle is in a dangerous situation.
- The DANGER THRESHOLD is the moment in time immediately before the automated vehicle enters a dangerous situation.
- A PROPER RESPONSE is the reaction the automated vehicle should perform to escape a dangerous situation and return to a safe state.

The idea is that if the automated vehicle implements a proper response to a dangerous situation at the danger threshold, then the automated vehicle should not cause collisions on the basis of its own actions and should often be able to avoid collisions caused by others who were not driving safely.

#### 2.2.2.10 TRAFFIC RULES

Traffic rules are an important part of the behavior of any vehicle on the road. All automated vehicles should comply with the traffic rules in the ODDs that they operate in. However, not all traffic rules are created equal. Some traffic rules are explicit, such as the meaning or purpose of a STOP sign or speed limit. Other traffic rules, however, are open to interpretation. For instance, California's Basic Speed Law states that the vehicle should not drive faster than is safer for current conditions (CA Vehicle Code, 1959). However, "safer for current conditions" is not explicitly defined and so could be subject to interpretation. For these subjective traffic rules, a uniform machine-interpretable definition of the expected behavior (e.g. by providing updated parameters to use in a formal safety model such as the one in the Drive Planning element would reduce interpretation uncertainty).

#### 2.2.2.11 MOTION CONTROL

To implement the desired vehicle motion, precise actuator commands must be derived from the given trajectory that is the output of the Drive Planning element (see Section 2.2.2.9). Therefore, a motion controller is necessary for generating lateral and longitudinal commands. The respective closed control loops must be stable with sufficient reserve to compensate for dynamic changes in road conditions, the vehicle dynamics and while performing mode transitions. The generated actuator commands are then allocated to steering, braking and the powertrain.

### 2.2.2.12 MOTION ACTUATORS

The motion actuators for steering and braking systems and the powertrain form the primary ability to control the motion of the ego vehicle. For this reason, they are often referred to as primary actuators. With regards to the aforementioned fail-safe and fail-degraded capabilities, there are various approaches to achieving fail-operational performance goals. Depending on the item definition, different sets of maneuvers can be derived that still have to be actuated and accordingly require different fail-operational capabilities of the different primary actuator systems.

Lateral and longitudinal guidance as performed by the motion actuators have to fulfill the capabilities according to the item definition.

#### 2.2.2.12.1 STEERING SYSTEM

The aim of a steering system is to control the lateral movement of a vehicle. The steering system has to deal with a lot of interference, such as road undulation, crosswind or friction coefficient, which directly affects the intended lateral movement.

To fulfill the capabilities, particularly being able to fail degraded, there are now fail-operational EPS systems that have an additional independent electronic system. This can fail degraded while retaining enough performance to control lateral movement. These EPS systems are generally suitable to act as an element covering the requirements based on the capabilities. In addition to this, there are further solutions for covering the capabilities, e.g. rear-wheel steering or yawing by braking.

#### 2.2.2.12.2 BRAKING SYSTEM

The aim of a braking system is to control the longitudinal movement of a vehicle in terms of deceleration requested by motion control. As with manual driving, stability functions such as ABS and ESC are crucial prerequisites for ADS-controlled deceleration requests. However, the impact of the automated driving functionality to the brake functions should be considered.

#### 2.2.2.12.3 POWERTRAIN

The aim of the powertrain is to control the longitudinal movement of a vehicle in terms of acceleration. Compared to the other two steering system and braking system elements, this element may not need to be fail-degraded.

### 2.2.2.13 BODY CONTROL WITH SECONDARY ACTUATORS

The role of body control for automated driving is mainly to communicate planned driving maneuvers and to enable safe and lawful driving conditions (e.g. ensuring a clear view through the windshield or adequate control of the headlights). Therefore, components such as indicator lights, headlights and the windscreen wiper motor are often referred to as secondary actuators, as they do not directly influence the ego motion of the vehicle.

The following describes examples of potential impacts that should controlled by the automated driving system:

- External lights should illuminate with the correct intensity to ensure adequate visibility to surrounding (vulnerable) road users and to provide a bright illumination for optical sensors (e.g. a camera sensor). The automated driving system has to ensure this operation when in automated driving mode, as the driver may be performing other tasks.
- Warning or indicator lights should work correctly, as they may confuse (vulnerable) road users (e.g. by unintended activation or indication of wrong direction). Additional communication systems may be needed depending on the item definition.
- Windshields (and rear mirrors) should be kept clean during automated driving mode, as a safe takeover by the vehicle operator needs to be ensured by providing a clear view to the front and the rear. Thus, cleaning, air conditioning and heating systems should provide adequate operation during the automated driving mode.

Passive safety components (e.g. seat adjustment, seat belt pre-tensioners, airbags) are not considered in this publication. Nonetheless, the impact automated driving has on these components should be considered.

### 2.2.2.14 HUMAN-MACHINE INTERACTION

Human-machine interaction (HMI) is considered a crucial element for the safe operation of SAE L3, L4 or L5 vehicles. HMI provides the means of interaction between human and machine to exchange information and operations and is designed in a way that makes using the automated driving system clear and intuitive for users. Therefore, HMI can use visual cues, tactile feedback and acoustic cues to support the user with relevant information, and it can offer different types of interfaces to receive input from the user. HMI should be carefully designed to consider the psychological and cognitive traits and states of human beings with the goal of optimizing the human’s understanding of the task and situation and of reducing accidental misuse or incorrect operations.