Reliable and safe maps for automated driving
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>4</td>
</tr>
<tr>
<td>Abstract</td>
<td>4</td>
</tr>
<tr>
<td>Highly reliable maps: use cases</td>
<td>4</td>
</tr>
<tr>
<td>3.1 Sensor range extension</td>
<td>5</td>
</tr>
<tr>
<td>3.2 Support when sensors work inadequately</td>
<td>6</td>
</tr>
<tr>
<td>3.3 Location-based information unavailable from sensors</td>
<td>6</td>
</tr>
<tr>
<td>3.4 Vehicle localization</td>
<td>6</td>
</tr>
<tr>
<td>Interrelationships between safety areas</td>
<td>7</td>
</tr>
<tr>
<td>Derivation of safety requirements for maps</td>
<td>7</td>
</tr>
<tr>
<td>5.1 Iteration 1: Main function SOTIF</td>
<td>8</td>
</tr>
<tr>
<td>5.2 Iteration 2: Main function safety in use</td>
<td>9</td>
</tr>
<tr>
<td>5.3 Iteration 3: Technical safety requirements SOTIF</td>
<td>10</td>
</tr>
<tr>
<td>5.4 Iteration 4: Availability of the main function due to safety requirements</td>
<td>10</td>
</tr>
<tr>
<td>Differences between the map and reality</td>
<td>11</td>
</tr>
<tr>
<td>6.1 Minimization, quantification and mitigation of map inaccuracies</td>
<td>12</td>
</tr>
<tr>
<td>6.2 Map data error prevention and detection</td>
<td>13</td>
</tr>
<tr>
<td>6.2.1 Quantification and mitigation</td>
<td>12</td>
</tr>
<tr>
<td>6.2.2 Minimization</td>
<td>13</td>
</tr>
<tr>
<td>6.2.3 Map transmission</td>
<td>13</td>
</tr>
<tr>
<td>6.2.1.1 Data collection</td>
<td>14</td>
</tr>
<tr>
<td>6.2.2.1 Human errors</td>
<td>15</td>
</tr>
<tr>
<td>6.2.2.2 Software/tool errors</td>
<td>15</td>
</tr>
<tr>
<td>6.2.2.3 Process errors</td>
<td>16</td>
</tr>
<tr>
<td>6.2.2.4 Cybersecurity</td>
<td>16</td>
</tr>
<tr>
<td>6.2.3 Map transmission</td>
<td>16</td>
</tr>
<tr>
<td>6.2.4 In-vehicle errors</td>
<td>16</td>
</tr>
</tbody>
</table>
6.3 Anticipation and detection of reality changes .................................................................17
  6.3.1 Anticipation of reality changes by means of information from road building authorities........17
  6.3.2 Anticipation of reality changes by the use of crowdsourcing to detect preparation ............18
  6.3.3 Detection of reality changes by the use of measurement vehicles .....................................18
  6.3.4 Detecting reality changes through crowdsourcing .......................................................19
6.4 Detection and mitigation of map update interruptions ..................................................19
  6.4.1 Interruption in map transmission ..................................................................................19
  6.4.2 Interruption in map production ....................................................................................20
  6.4.3 Interruption in map data collection ..............................................................................20
6.5 Detection and mitigation of deviations .......................................................................20
  6.5.1 Detection ..................................................................................................................20
  6.5.2 Mitigation ..................................................................................................................20

7 Remaining challenges .....................................................................................................20

8 Appendix ........................................................................................................................21
  8.1 SAE automation levels .................................................................................................21
  8.2 Abbreviations ...............................................................................................................22
  8.3 References ....................................................................................................................22

Legal disclaimer
Company-confidential and proprietary information
ALL RIGHTS RESERVED. No part of this publication may be copied in any form, by photocopy, microfilm, retrieval system, or by any other means now known or hereafter invented without the prior written permission of Elektrobit Automotive GmbH and Baidu, Inc.
1 Preface

Using map data in automated driving applications raises the questions: Which applications require it? Can it be used for safety-related functions? In what ways can highly reliable maps be made?

This document examines these questions, describes some technical implementation approaches, and indicates the unsolved problems.

2 Abstract

- Automated driving functions can utilize highly reliable map data
- Map suppliers’ tools and processes need reviewing and improvement to achieve the required data integrity
- Map quality metadata is required for HAD applications
- Map suppliers and road building authorities must cooperate to keep map data current
- Some safety aspects require further discussion (e.g., backend system protection methods, map quality metadata)
- Important aspects need standardization (e.g., SOTIF acceptable risk level, backend system safety requirements)

3 Highly reliable maps: use cases

At the moment, different application scenarios can be projected for highly reliable maps:

<table>
<thead>
<tr>
<th>Application</th>
<th>Sensor range extension</th>
<th>Support for insufficient sensor performance</th>
<th>Location based information that can not be derived from sensors</th>
<th>Localization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example</td>
<td>Takeover request in time before end of automated driving area</td>
<td>Bad weather (snow, ice, fog), country-specific signs, physical hacking</td>
<td>Road clearance for automated driving by car manufacturer, country specific rules</td>
<td>GPS map matching, landmarks</td>
</tr>
<tr>
<td>Challenges</td>
<td>1) Data quality: Precision, up-to-date-ness, completeness, correctness of the map data</td>
<td>2) Integrity: Functionality and security for backend and data transmission</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 2: Highly reliable map applications
Maps do not replace sensors, which supply data about dynamic processes in the vehicle's environment, e.g., the actions of pedestrians, cyclists, and other vehicles.

Reliance on a map for specific information means only that sensors cannot provide the information with the required quality; the vehicle still needs sensors. For example: a camera cannot read an obscured sign, but the data can be retrieved from a map. Conversely, a map cannot deliver information about the distance to other cars.

According to ISO 26262, map systems cannot be used to decompose safety requirements in conjunction with sensor systems if only one of the systems provides the necessary information with the required quality, excluding hardware or software failure.

A map system can thus only be used here either to rectify physical/algorithmic sensor system inadequacies or for decomposition.

Safety related applications usually only require a subset of the map attributes to be highly reliable rather than the entire map. These attributes are called reliable map attributes (RMA). Section 5 of this white paper gives an example of how to derive the detailed RMA list for a given application.

3.1 Sensor range extension

Predicting situations

Map information can extend sensor range through advance identification of potential hazard situations. The automated driving function can match or improve on an average driver’s skills, e.g., by adjusting speed when speed limit signs are obscured, or braking before reaching an obstacle.

Requesting driver takeover well before HAD route ends

HAD systems are currently only good enough for use in specific areas (e.g., highways).

In HAD mode, drivers generally do not monitor vehicle function and environmental conditions and are unaware of functional restrictions. They are not therefore expected to identify in advance where HAD mode should end, or to take immediate control of the vehicle when prompted (time is needed for reaction and situational awareness).

When sensors detect the HAD route end point, insufficient time may remain to transfer control to the driver. Hazards and discomfort may result if emergency braking is needed, which is even more likely if sensors cannot detect the end of the HAD route (e.g., signs obscured).

The system can compute the end of the HAD route from map data, and alert the driver in good time.

Steering to a safe stop

If the driver fails to take over, emergency in-lane braking is avoidable if, e.g., a hard shoulder is available. A map can indicate if and where there is one.

The vehicle safety concept can also include this as the response to a safety-related component failure or driver medical emergency.
3.2 Support when sensors work inadequately

Bad weather/obscured signs
The weather (e.g., snow, ice, fog) affects environmental sensors. Map information can help classify a sign when it is partially or entirely obscured.

Improving recognition through multiple detections
 Appropriately computed data from multiple vehicles lets the system detect objects more reliably than a single sensor.

3.3 Location-based information unavailable from sensors

HAD route permission
Legal permission for HAD is not and is unlikely to be signposted. This information can only be obtained from maps.

Manufacturer’s performance-based HAD route approval
Vehicle manufacturers may close certain route segments to HAD for a particular vehicle type or configuration although HAD may be legally permitted in general on that route segment, e.g., if the vehicle system’s performance is inadequate for safe operation there.

National regulations
The vehicle must “know” its location to apply national regulations, e.g., left-/right-hand traffic. Sensors can detect frontier signs when the vehicle is driven across a border. If it is transported to another country, e.g., by rail, its location can be retrieved from a map using satellite position data.

3.4 Vehicle localization
Localization is required for HAD functions. This can be achieved by map matching. The system determines the position on the map by matching the vehicle’s absolute position identified by satellite navigation and its previous motion profile to road geometries in the map.

Depending on the automation level and required functionalities, different localization accuracy is required.

A level 3 highway pilot function without automatic lane changes is only to be activated on highways. The system should be able to determine whether the vehicle is on the correct road. The “road type” information is provided by the HD map.

To ensure lane-precise localization, higher lateral localization accuracy may be needed for a level 3 highway pilot function with automatic lane changes. This may require lane marking information from the HD map.
4 Interrelationships between safety areas

Many different areas must be considered with regard to automotive safety. The three areas most relevant in the context of reliable maps are:

- **Functional safety (according to ISO 26262)**
  - Relates to hardware and software in the car
  - Mitigation of risks to due to HW/SW not working according to specification
  - Does not include “nominal performance” necessary for safe operation

- **SOTIF (safety of the intended functionality)**
  - Relates to functions in the car
  - Addresses the “nominal performance” necessary for safe operation

- **Safety in use**
  - Prevention of intentional or unintentional misuse
  - Prevention of mental overload and distraction

5 Derivation of safety requirements for maps

There is currently no standardized procedure that integrates all the safety areas relevant to the design of a system for a highly automated driving function (e.g. Highway Pilot, HWP). This chapter describes an approach that can be used to do this.

The proposed approach uses iterative design to reduce the complexity of the procedure. The development part of the ISO 26262 safety lifecycle is run through at least partially in each iteration.
In each iteration, the analysis results are used to improve the design of the functions and system. As well as functional safety analyses, safety in use, SOTIF and availability analyses are also used.

The following subsections describe some of the iterations for an example highway pilot (HWP) functionality.

### 5.1 Iteration 1: Main function SOTIF

In the first iteration in this example, a SOTIF analysis is performed for the current system design immediately after the hazard analysis and risk assessment (HARA). The analysis results reveal that pedestrian detection is not good enough to allow the car to drive autonomously in a city scenario.

The ISO 26262 HARA method is used to describe and evaluate the resulting risk. The hazardous situation described is that of a pedestrian crossing the street being hit by the car that is driving autonomously in a city.

This defines a safety goal, namely that the highway pilot function will only be active on highways.

It is assumed that the technical safety concept defines that the driver’s manual will state that the highway pilot must not be engaged off-highway. There will also be safety requirements that state that the HWP will only be activated if desired by the user (=> reliability of the HWP on/off switch).
5.2 Iteration 2: Main function safety in use

Iteration 1 assumes that drivers always know when they are driving on a highway and will never try to activate the HWP if they are not.

In iteration 2, a safety in use analysis may show that this assumption is not true, i.e. that drivers often try to mis-use the function or they erroneously think that they are on a highway when they activate it.

In other words, the driver cannot be trusted.

Hence, this defines a functional safety requirement that the driver can only activate the HWP when the system detects that the car is on a highway.

Some form of localization (e.g. GNSS with motion sensors) is necessary for this requirement. The information about whether or not the current road is a highway is taken from a map.
5.3 Iteration 3: Technical safety requirements SOTIF

The next iteration analyzes whether the nominal performance of the GNSS, sensors and map are sufficient to guarantee correct road type identification in all cases and situations.

There may be locations that will always show errors. For example, GNSS position uncertainty may mean that the system erroneously localizes the car on a highway when it is in fact on a highway ramp or on a road that is very close to a highway.

This potentially hazardous situation can be eliminated with a new safety requirement: The HWP can only be active if there are no ramps or other roads close to the current position (within the circle of position uncertainty).

5.4 Iteration 4: Availability of the main function due to safety requirements
At this point, the system design already appears to be quite safe as long as it functions according to specification. However, has availability been sacrificed for the sake of safety?

An availability calculation may show that, especially near cities, there may be many ramps and parallel secondary roads, so that the driver may not be able to use the HWP at all because of the strict safety requirements.

Of course, safety requirements must not be relaxed to improve availability. An alternative here may be to add another functionality: Use a camera to detect the number of lanes and the type of lane marking on the current road, and compare the results with the highways, ramps or parallel secondary roads within the circle of localization uncertainty. If, for example, the number of lanes matches the mapped highway but not the parallel road, it is certain that the car is on the highway and the HWP can be activated. This increases the availability of the HWP.

The above analysis is an example of how to derive the map safety requirement. It shows that the safety requirement depends on the OEM and HAD provider system design.

6 Differences between the map and reality

Differences between the map and reality that can introduce errors in HAD applications are a different type of fault to those described in ISO 26262. The table below compares the faults due to differences between the map and reality with the ISO26262 fault types.

<table>
<thead>
<tr>
<th>Map data does not match with reality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time of deviation origination</td>
</tr>
<tr>
<td>Before SOP</td>
</tr>
<tr>
<td>During car production</td>
</tr>
<tr>
<td>After car production</td>
</tr>
<tr>
<td>Similar to systematic faults</td>
</tr>
<tr>
<td>Similar to systematic faults</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

The map will differ from reality in the case of:

- Map inaccuracy
- Map data errors
- Reality changes
- Map update delays
- Localization errors (not considered in this white paper)
To reduce risk, it is possible to:

- Minimize, quantify and mitigate map inaccuracy
- Prevent, detect and remove map data errors
- Anticipate and detect reality changes
- Minimize, detect and mitigate map update delays
- Detect and mitigate deviations

These approaches are described in the following sections.

6.1 Minimization, quantification and mitigation of map inaccuracies

6.1.1 Quantification and mitigation

Map data does not need to be extremely accurate for hazards to be avoided. The functions that use it only need to know its actual accuracy so that this is considered in critical decisions.

One feasible approach is to quantify the map inaccuracy, and add this information to the map as metadata. Functions that use the map data can then also take the map inaccuracy into account.

If the map accuracy is too low for safety-critical decisions to be based on the map data, the functions may request a switch to a safe state.

If this approach is followed, the correctness of the map accuracy metadata rather than the map accuracy itself is safety relevant.

Example:
The “driver can activate HAD” decision is based on map information (road type and road geometry) and GPS position data:

Case 1:
- Vehicle is on a rural highway
- No parallel roads or entrance/exit ramps within 100m
- Satellite position accuracy is better than 1m (GNSS receiver data)
- Maximum road geometry deviation is less than 5m (map quality metadata)
- On-board sensors indicate that the vehicle is traveling at highway speed
- Satellite position and road geometry inaccuracy ranges overlap
- Direction of travel and road orientation correspond
- The road type on the map is “Highway”
  Conclusion: The vehicle is on a highway.

Case 2:
- Vehicle is on an urban highway
- A parallel country road is 8m away
- Satellite position accuracy is 10m
- Road geometry accuracy is 5m
- Satellite position inaccuracy overlaps both roads
- Direction of travel suits both roads
- Highway local speed limit is 100 km/h; speed plausible for both roads
- Highway signs not visible
  Conclusion: The vehicle is not definitely on a highway, system prohibits HAD.
6.1.2 Minimization
If map data inaccuracy in itself is not safety critical, why is it good to reduce the inaccuracy? A reduction in inaccuracy increases the availability of the functions that use the map data.

For example, when the map data is used for a highway pilot function, it may not be possible to activate the function or the function may often switch off if the map data is not accurate enough.

It may therefore make sense to improve the map data accuracy depending on the requirements of such functions.

6.2 Map data error prevention and detection
Map data errors can occur in

- data collection
- map production
- transmission, or
- in the vehicle.

Figure 7: Areas where map data errors can occur
### 6.2.1 Data collection

The following map data errors can occur in data collection:

- **Object/attribute non-detection** (false negative)
- **Object/attribute false detection** (false positive)
- **Misclassification** (thematic accuracy)

All these error types can be caused by insufficient sensor performance. Human error can in particular also cause non-detection, false detection or misclassification errors.

The initial data collection is best done by the map supplier’s measurement vehicles, as their better sensors and computing power ensure high accuracy and low false detection/misclassification rates.
6.2.2 Map production

The main sources of map data errors in map production are:

- Human errors
- Software/tool errors
- Process errors

6.2.2.1 Human errors

Human errors can be caused by e.g.:

- Insufficient training
- Over/under-challenging
- Inattentiveness
- Intent/sabotage
- Fatigue/illness
- New situations

Measures to reduce the above have not been standardized for the automotive industry, but procedures from other industries involving safety critical human activities can be applied. A human error prevention guideline, trainings and regular adherence checks can help to reduce the probability of human errors.

6.2.2.2 Software/tool errors

ISO 26262 covers in-vehicle hardware/software, but Part 8, “Confidence in the use of software tools” may apply if backend software is considered as a set of tools. ISO 26262, Part 8, includes a 5-step tool risk assessment and protection method derivation procedure:

1) Assess the safety goal violation impact (“Tool Impact”, TI 1-2)
   TI1: No violation possible
   TI2: Violation possible
2) Assess the tool error detection/correction probability of subsequent measures (“Tool Detection”, TD 1-3)
   TD1: High
   TD2: Medium
   TD3: Otherwise
3) Determine the Tool Confidence Level (TCL 1-3, see Table 3). TCL1 always results from TI1 or TD1
4) Select the appropriate table (TCL2 => Table 5, TCL3 => Table 4)
5) Extract methods according to the safety goal ASIL:
   + "Recommended"
   ++ "Highly recommended"

Aviation standard DO-330 describes even more detailed procedures regarding tool confidence evaluation.
6.2.2.3 Process errors
Because some situations are not covered, errors may occur even though the tools and humans involved do what the process requires.

Using a process FMEA can help to identify and evaluate process related issues.

6.2.2.4 Cybersecurity
Existing security standards such as J30161 or ISO 21434 can be applied here. It is insufficient to only assess the security measures for technical systems. It is also necessary to e.g. restrict access to the map provider’s facilities, and the relevant staff must be trained to follow important rules (e.g. no unknown USB stick to be plugged into a computer).

6.2.3 Map transmission
When the map data is transmitted, it may be changed

- Unintentionally due to HW/SW errors
- Intentionally by third parties (cybersecurity).

End-to-end protection mechanisms (checksum, message counter, as built into e.g. AUTOSAR) can detect/correct unintentional transmission errors. End-to-end security encryption covers unintentional errors and intentional tampering. Existing security standards (like J30161 or ISO 21434) can also be applied here.

6.2.4 In-vehicle errors
Map data may also be corrupted due to hardware or software errors in the car.

ISO 26262 already covers how to avoid and handle in-vehicle system errors. This is therefore not discussed further in this white paper.
6.3 Anticipation and detection of reality changes

Even if a map is perfectly correct and is not changed at this moment in time, it can be incorrect in the next instant if the reality changes. A map is always only a snapshot, a model that represents reality at a certain point in time.

Some things in reality change more often than others, e.g., traffic light modifications are rare compared to changes in signs or markers. If the changes affect the characteristics that are used for safety related applications, the map must be updated as quickly as possible.

It is not possible to detect changes in reality in real time, but it is possible to anticipate planned changes. For all other types of reality changes, it is necessary to detect the differences between the map and reality, and mitigate the risk by means of immediate action.

Reality changes can be categorized as:

- Unintentional changes (e.g. lane markings destroyed by bad weather)
- Planned changes (e.g. a new ramp is built)
- Intentional but unplanned changes (e.g. traffic diverted due to an accident)
- Malicious changes (e.g. traffic signs vandalized)

The map can be a more reliable sensor than the vehicle’s on board environment sensor in the case of the first and fourth types of reality change described above.

<table>
<thead>
<tr>
<th>Type</th>
<th>Change type</th>
<th>Reality change</th>
<th>Example</th>
<th>Counter Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Reality change</td>
<td></td>
<td>Deviation detection + mitigation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unintended</td>
<td>E.g. snow on traffic sign</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Planned</td>
<td>E.g. new ramp built</td>
<td>Reality change anticipation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Intended unplanned</td>
<td>E.g. traffic redirection due to accident</td>
<td>Deviation detection + mitigation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Malicious</td>
<td>E.g. traffic sign manipulation</td>
<td>Deviation detection + mitigation</td>
</tr>
</tbody>
</table>

Figure 3: Possibilities for the anticipation of different reality change types

6.3.1 Anticipation of reality changes by means of information from road building authorities

Random, unpredictable road changes such as earthquake damage or landslips are rare, and sensors will often detect them, allowing emergency braking.

Virtually all reality changes regarding static characteristics result from planned construction measures.

Providing map suppliers with the relevant information early on allows them to plan re-mapping, measure the changes before final approval, and publish the updated maps when the change is completed.

Road building authorities should therefore share information about planned, ongoing, and completed construction projects with map providers. Incentives to encourage this are:

- Financial: The map supplier pays for the information.
- Political: The government requests the authority to pass on the data to ensure that the country benefits fully from vehicle automation.
- Goods-related: The map supplier provides information about e.g., road conditions or use in exchange for the information, enabling the authority to improve planning.

This method is considered to be necessary.
6.3.2 Anticipation of reality changes by the use of crowdsourcing to detect preparation

It will take years to get all road building authorities to agree, provide their data, and harmonize their systems’ technical interfaces, and some may never comply due to political barriers.

To overcome this, the following approach is recommended to avoid hazards and minimize the use of measurement vehicles:

- Crowdsourcing identifies and reports change sites that are not on the map
- Map supplier lowers the confidence level of the affected map attributes
- Map supplier prepares update from completion date and changed appearance data from site operator
- If real time completion date data is unavailable, map supplier waits until crowd data indicates completion (e.g., roadworks signs removed)
- If needed, a measurement vehicle verifies completion as planned
- Map supplier publishes updated map and raises confidence levels after confirmation received.

This method is considered to be necessary.

6.3.3 Detection of reality changes by the use of measurement vehicles

Regularly moving along all routes to identify changes is inadvisable as the residual error rate would be unacceptably high even if very many vehicles were used. For example:

Assuming that:

- 1% of vehicles on the road are measurement vehicles (unlikely)
- 10% of vehicles on the road drive in automated mode
- Reality changes are random or unpredictable
- The reality change would immediately cause an accident to a vehicle in automated mode if not reflected in the map
- The map perfectly represents reality until the change occurs

Then:

- The probability of an accident (first vehicle at the changed location is in automated mode) is 10% (unacceptably high)
- 5 automated vehicles will arrive at the location (potential accidents) before the first measurement vehicle arrives
  - The change is still not mapped and vehicles will not have the updated map immediately, so numerous vehicles will be exposed to the hazard.

This method is considered as a possible add-on, but is not sufficient on its own.
6.3.4 Detecting reality changes through crowdsourcing
In the above example, the probability of an automated vehicle being the first to reach the critical location is only 10%, so even if all the automated vehicles on the road provide their data online, crowdsourcing is not sufficient. This method is considered as a possible add-on, but is not sufficient on its own.

6.4 Detection and mitigation of map update interruptions
A map is like a sensor with a very high latency time. Information from the map is always “old” at the time that it is used. As discussed in section 6.5 below, detection and mitigation of deviations is necessary so that the vehicle’s functions can safely handle any differences between the map and reality. Nevertheless, safety is increased when the latest map data is always available in the car, especially when the data can only be obtained from the map and cannot be perceived by sensors.

6.4.1 Interruption in map transmission
Only the map data for the near surroundings and along the path of the car is usually relevant at any given time rather than all of the map data. One possible approach is to download partial map updates from the server before they become relevant for the vehicle (e.g. map data along a planned path or the most probable path determined by an electronic horizon).

The vehicle can request the server if any new version of a certain part of the map is available and download the new version if there is one. Otherwise, the version already stored in the car can be used.

What happens if the server is unavailable or the download fails, e.g. due to a bad mobile data connection? In this case, the car functions can attempt to resume the download for a certain period of time. If the data cannot be downloaded before it is needed, the function that uses the data can switch to a safe state, e.g. degrade the functionality or initiate a driver takeover request.

If this approach is followed, only the correctness of the version information for each map part and not the availability of a mobile data connection is safety critical.
6.4.2 Interruption in map production
If the map provider’s production process is completely down, all the map parts can still be buffered in cloud storage. The map will still appear to be correct from the perspective of the car. Because the map part versions in the cloud do not change, there is no apparent need to download new map part versions. The maps become more and more out of date from minute to minute.

This situation must be avoided. For example, either the map provider or the car itself can receive a regular alive counter signal from a “map provider watchdog” and block the use of the map if this signal is no longer received.

6.4.3 Interruption in map data collection
The same is true for the collection of map data. If certain information is no longer available (e.g. update from road building authorities), map users must be informed that the map attributes based on the information are possibly out of date.

6.5 Detection and mitigation of deviations

6.5.1 Detection
Detection and mitigation of deviations “in the car” is the last line of defense. It can help in cases where other measures (such as map error prevention or anticipation of reality changes) have failed or where there are no other possible measures (e.g. in the case of traffic sign manipulation).

To be able to detect a deviation in the car, the relevant map characteristic (e.g. an attribute) must also be perceivable by the car’s sensors. For example, a deviation in the map attribute “autonomous driving allowed on this road” cannot be detected in the car if there are no special signs that indicate this information in reality.

6.5.2 Mitigation
If a deviation has been detected in the car, the resulting risk must be mitigated by immediate reactions, e.g.:

- Assumption of the worst case: If the map shows a speed limit of 80 km/h and the sensors see a speed limit of 30 km/h, it is assumed that 30 km/h is true. Of course, this must not result in an emergency brake maneuver that could increase the risk of a rear collision.
- Driver takeover request
- Minimum risk maneuver (e.g. stop the car in an emergency lane)

7 Remaining challenges
This white paper has attempted to discuss each aspect of maps that can affect the safety of applications that use them. However, many challenges still remain. Map providers, HAD providers, automated vehicle producers, and road authorities need to work together to find the solutions.

Multiple aspects with regard to highly reliable maps still need clarification. These include:

- Human error prevention guidelines must be developed for map making.
- Effective analysis methods for safety in use and SOTIF must be identified or developed.
- Communication between road building authorities and map makers must be established.
- Safety mechanisms to detect map data collection or map production interruptions must be specified and implemented.
- The different ASIL levels for qualitative safety measures need to be distinguished.
8 Appendix

8.1 SAE automation levels

<table>
<thead>
<tr>
<th>SAE level</th>
<th>Name</th>
<th>Narrative Definition</th>
<th>Execution of Steering and Acceleration/Deceleration</th>
<th>Monitoring of Driving Environment</th>
<th>Fallback Performance of Dynamic Driving Task</th>
<th>System Capability (Driving Modes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No Automation</td>
<td>The full-time performance by the human driver of all aspects of the dynamic driving task, even when enhanced by warning or intervention systems</td>
<td>Human driver</td>
<td>Human driver</td>
<td>Human driver</td>
<td>n/a</td>
</tr>
<tr>
<td>1</td>
<td>Driver Assistance</td>
<td>The driving mode-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the human driver perform all remaining aspects of the dynamic driving task</td>
<td>Human driver and system</td>
<td>Human driver</td>
<td>Human driver</td>
<td>Some driving modes</td>
</tr>
<tr>
<td>2</td>
<td>Partial Automation</td>
<td>The driving mode-specific execution by one or more driver assistance systems of both steering and acceleration/deceleration using information about the driving environment and with the expectation that the human driver perform all remaining aspects of the dynamic driving task</td>
<td>System</td>
<td>Human driver</td>
<td>Human driver</td>
<td>Some driving modes</td>
</tr>
<tr>
<td>3</td>
<td>Conditional Automation</td>
<td>The driving mode-specific performance by an automated driving system of all aspects of the dynamic driving task with the expectation that the human driver will respond appropriately to a request to intervene</td>
<td>System</td>
<td>System</td>
<td>Human driver</td>
<td>Some driving modes</td>
</tr>
<tr>
<td>4</td>
<td>High Automation</td>
<td>The driving mode-specific performance by an automated driving system of all aspects of the dynamic driving task, even if a human driver does not respond appropriately to a request to intervene</td>
<td>System</td>
<td>System</td>
<td>System</td>
<td>Some driving modes</td>
</tr>
<tr>
<td>5</td>
<td>Full Automation</td>
<td>The full-time performance by an automated driving system of all aspects of the dynamic driving task under all roadway and environmental conditions that can be managed by a human driver</td>
<td>System</td>
<td>System</td>
<td>System</td>
<td>All driving modes</td>
</tr>
</tbody>
</table>

Figure 4: SAE automation levels, original table

Figure 5: SAE automation levels, simplified
8.2 Abbreviations

HAD  Highly automated driving
HARA  Hazard analysis and risk assessment
SOTIF  Safety of the intended functionality

8.3 References

[1] ISO/AWI PAS 21448 Road vehicles - Safety of the intended functionality
   Working document of the ISO TC 22/SC 32/WG 8
   (not yet released)

   2011 International Organization for Standardization

   2013 International Organization for Standardization

   2014 International Organization for Standardization

   2009 International Organization for Standardization

   2011 RTCA Inc.

   2016-01 SAE International
Author: Yali Wang

The Functional Safety Expert Yali Wang began his professional career in Cummins Inc, where she worked as an embedded software specialist. Since 2017, She joined Baidu Inc. and hold the position as head of system integration. She had rich experience in the field of ISO26262, SoTIF and other safety domain related to highly automated driving. She has been worked as functional safety specialist for several highly automated driving applications.

Author: Steffen Kuhn

Steffen Kuhn is Head of Elektrobit Consulting. He and his team advise companies on subjects like functional safety, agile development methods as well as architectures and strategies for the automotive sector. Mr. Kuhn developed his know-how through his 18 years of experience in technical consulting, management consulting, and software development. He is an expert in the fields of process improvement for compliance with (A)Spice/CMMI, functional safety, lean and agile development methods, and project management.
About Elektrobit (EB)
Elektrobit (EB) is an award-winning and visionary global supplier of embedded and connected software products and services for the automotive industry. A leader in automotive software with over 30 years serving the industry, EB’s software powers over 1 billion devices in more than 90 million vehicles and offers flexible, innovative solutions for connected car infrastructure, human machine interface (HMI) technologies, navigation, driver assistance, electronic control units (ECUs), and software engineering services. EB is a wholly owned subsidiary of Continental.

Elektrobit Automotive GmbH
Am Wolfsmantel 46
91058 Erlangen, Germany
Phone: +49 9131 7701 0
Fax: +49 9131 7701 6333
sales@elektrobit.com
www.elektrobit.com

About Baidu Apollo
Apollo Pilot is Baidu’s autonomous driving product targeting for mass production, which aims to provide the safest, most economical and comfortable driving service. Baidu integrates the technology and experience accumulated in the field of autonomous driving based on the study of Chinese users’ driving behaviors.

Apollo Pilot 是百度利用多年在自动驾驶领域沉淀的丰富技术，结合中国用户驾驶习惯打造的最适应中国国情的可量产自动驾驶产品，致力于提供最安全、经济、舒适的自动驾驶服务。