

Application of SOTIF for the assessment of HMIs

TNO 2025 R11118 – 19 September 2025

Application of SOTIF for the assessment of HMIs

Author(s)	C.J. van der Ploeg, H.H.S.N. Subraveti, J.H. Hogema, S. Gaggari
Classification report	TNO Public
Number of pages	69 (excl. front and back cover)
Number of appendices	3

All rights reserved

No part of this publication may be reproduced and/or published by print, photoprint, microfilm or any other means without the previous written consent of TNO.

©2025 TNO

Contents

Contents	3
1 Abbreviations.....	4
2 Terminology	5
3 Introduction.....	6
3.1 Background	6
3.2 Scope	6
3.3 Approach.....	6
3.4 Introduction of the Report.....	7
4 Mode Confusion.....	8
4.1 Causes of mode confusion.....	8
4.2 Measuring mode confusion	10
4.3 Safety analysis of human-machine interactions	11
4.4 Real world examples of mode confusion.....	12
4.5 Conclusions	13
5 Introduction to SOTIF and functional safety assessment.....	14
5.1 ISO 21448: Safety Of The Intended Functionality	15
5.2 ISO 26262: Functional Safety and its relation to SOTIF	17
6 Methodology Design	19
6.1 Introduction.....	19
6.2 Proposed Methodology	21
7 Methodology application	26
7.1 Pre-testing.....	27
7.2 Formulating the Test Matrix.....	36
7.3 Testing	37
8 Conclusion.....	44
8.1 Summary and conclusions of the report	44
8.2 Discussion	44
References.....	49
Appendices	
Appendix A: BMW Manual Excerpt	52
Appendix B: Testing Matrix	62
Appendix C: Testing vehicle settings	66

1 Abbreviations

ACC	Adaptive Cruise Control
ADAS	Advanced Driver Assistance Systems
ADM	Automated Driving Mode
ADM+	Automated Driving Mode Plus
ADS	Automated Driving System
AEB	Automated Emergency Braking
ALKS	Automated Lane Keeping System
AV	Automated Vehicles
DCAS	Driver Control Assistance Systems
HMI	Human Machine Interface
HMM	Hidden Markov Model
HUD	Heads-Up Display
MCQ	Mode Confusion Questionnaire
MRM	Minimal Risk Manoeuvre
ODD	Operational Design Domain
OR	Operational Requirements
PP	Personal Pilot
SA	Situational Awareness
SAE	Society of Automotive Engineers
SOTIF	Safety Of The Intended Functionality
TOR	Take-Over Request
UNECE	United Nations Economic Commission for Europe
VRU	Vulnerable Road User

2 Terminology

Definition 1: Action. *Single act or behaviour that is executed by any actor in a scene (Def. 5) [1].*

Definition 2: Safety of the intended functionality. *The absence of unreasonable risk due to a hazard caused by functional insufficiencies (Def. 3) [1].*

Definition 3: Functional insufficiency. *A functional insufficiency can be defined on system-level or component-level in the following ways:*

- *The insufficiency of a specification of the intended functionality at the vehicle level*
- *The insufficiency of a specification of electric and/or electronic (E/E) elements in the system [1].*
- *A performance insufficiency in the implementation of electric and/or electronic (E/E) elements in the system [1].*

Definition 4: Scenario. *A description of the temporal relationship between several scenes (Def. 5) in a sequence of scenes, with goals and values within a specified situation, influenced by actions (Def. 1) and events [1].*

Definition 5: Scene. *Snapshot of the environment including the scenery, dynamic elements, and all actors' and observers' self-representations, and the relationships among those entities*

Definition 6: Triggering condition. *Specific condition of a scenario (Def. 4) that serves as an initiator for a subsequent system reaction contributing to either a hazardous behaviour or an inability to prevent or detect and mitigate a reasonably foreseeable indirect misuse (Def. 7).*

Definition 7: Misuse. *Usage in a way not intended by the manufacturer or the service provider*

Definition 8: Abuse. *The use of a vehicle by a driver incapable of ensuring the driving task in case of need.*

3 Introduction

3.1 Background

The Ministry of Infrastructure and Water Management in The Netherlands is considering the possibility of adding Human Factors aspects (HF) to the type approval process of passenger cars and commercial transport (cars, buses and trucks) that are equipped with driver assistance systems or automated vehicle systems. In these systems, the interaction with the driver plays a critical role with regards to the safe usage of these systems. Therefore, an evaluation of these interaction processes between the vehicle and driver are under consideration to become a part of the type-approval process.

Safety Of The Intended Functionality (SOTIF) is a standard that enables the analysis of a system for possible functional insufficiencies during its normal functioning. SOTIF is about making sure a system is safe even when it's working as designed. Sometimes, a system can still cause danger not because something broke, but because it wasn't designed to handle certain situations well enough. For example, a self-driving car might not recognize a pedestrian in unusual lighting, not because the sensors failed, but because the developer of the software didn't expect that situation to occur, and hence did not design the system to function in such a situation. SOTIF looks at those kinds of risks. This is different from functional safety, which is about what happens when something in the system actually breaks or stops working. Therefore, this is a complementary approach that is considered important in the development of automated driving systems and is also used extensively within the industry. The analysis aims to identify and prevent potential inadequacies in the system or opportunities for misuse by the user.

The Ministry raised the question of whether and how the SOTIF approach can be used to evaluate the quality of interaction processes between the vehicle and the user, in the context of automated driving systems. Pursuant to this, Rijkswaterstaat requested TNO to undertake a research project to further investigate the possibilities of such an approach.

3.2 Scope

In order to scope the research and provide a concrete use case for the application of the methodology, mode confusion in the case of vehicle automation was chosen as the phenomenon of interest. This decision was made to align the results with a previous SWOV study on the topic [2], which studied mode confusion in automated vehicles without the application of SOTIF. This would provide an objective point of reference that can be used to assess the applicability of the SOTIF framework in this context.

3.3 Approach

The project was divided into three large sections, as follows:

1. Literature research
 - a) Mode confusion

b) SOTIF

2. Methodology Design: Designing an approach for the application of SOTIF for analysis of human-automated vehicle interaction for preventing mode confusion.
3. Testing and analysis.

3.4 Introduction of the Report

This report presents the outcomes of this study. Chapter 4 provides an introduction to Mode Confusion, and covers the various forms of mode confusion and ways of modelling and evaluating this. Chapter 5 explores the SOTIF framework, and defines the scope of the analyses that can be carried out with it. It also provides a contrast to the Functional Safety standard, and discusses the complementarity of the two approaches. Chapter 6 combines the outcomes of the two prior chapters, and converges to a proposed methodology that is developed within this project. Finally, Chapter 8 documents the results of the pilot tests conducted within the project, and a discussion on the applicability of SOTIF for the purpose of analysing human-automated vehicle interaction, as well as open questions thereof.

4 Mode Confusion

Automated driving is commonly classified under the six SAE levels [3], with particular focus on Level 2 (partial driving automation) and Level 3 (conditional driving automation) in current consumer vehicles. In Level 2 (L2) vehicles, the system supports both lateral (steering) and longitudinal (speed) aspects of driving simultaneously, but the driver is required to continuously monitor the environment and be ready to take control at any moment. The driver is expected to remain engaged, actively monitoring the system performance and road conditions. In the case of Level 3 (L3) vehicles, the system handles all aspects of driving within a specific operational design domain (ODD). However, if conditions fall outside of that domain, the system will not operate and issue a takeover request (TOR) to the driver. Although the driver can disengage from the driving task (e.g., by engaging in non-driving-related tasks), they must be prepared to take control when alerted by the system. This shift in responsibility between different automation levels means that the driver must always remain aware about which system is currently in use and its capabilities and limitations to maintain safe driving. With an increasing number of vehicles with Advanced Driver Assistance Systems/Driver Control Assistance Systems/Automated Driving Systems (ADAS/DCAS/ADS) along with an increasing number of different systems within one vehicle, there is a real possibility of mode confusion.

Historically, mode confusion was first studied in the context of aviation. In the cockpit, pilots rely on multiple automated systems (e.g., flight directors, flight management systems) that have various modes such as climb, cruise, or approach. Confusion arises when the pilot's mental model of these systems does not match the system's actual state. Mental model is the internal representation of how the ADS works, what it can do, its limitations, and how it behaves under various conditions [4]. For example, if a pilot assumes that the autopilot is managing the aircraft's altitude when, in fact, it has switched to a different mode due to changing conditions, critical discrepancies can occur that jeopardize flight safety. Mode confusion is a phenomenon that has been well documented in the aviation, robotics and automated vehicles industry [5]. With the increasing adoption of automated driving technologies — particularly in L2 and L3 vehicles — similar issues have begun to surface on the road. Mode confusion in automated vehicles (AVs) occurs when drivers misunderstand or are unaware of the system's current operational mode, leading to inappropriate trust, slow responses, or over reliance on automation leading to potential hazards. Therefore, it is important to understand mode confusion in the context of automated driving. In this section, a detailed description of the causes of mode confusion is presented along with different methods of measuring mode confusion. This is followed by a literature review on safety analysis of human-machine interactions and the section is concluded with examples of mode confusion as observed in real-world studies.

4.1 Causes of mode confusion

Based on the definition in [6], mode confusion refers to a mismatch between a user's mental model of a system and reality. It can be caused by the following three factors:

- Incorrect perception of system behaviour
- Incorrect knowledge of system functioning

- Incorrect interpretation of the safety implications of system functioning

4.1.1 Incorrect perception of system behaviour

Incorrect perception of system behaviour means that the user is not able to correctly interpret how a system is acting or is going to act in a given situation. An example of this is when a driver believes that the automated driving system (ADS) has detected a vulnerable road user (VRU) because of a visual or auditory cue from the human machine interface (HMI), but the system has actually not detected that specific VRU. Another example can be when a driver thinks that an adaptive cruise control (ACC) system is slowing down the vehicle for traffic ahead as the car decelerates, but the slowing is due to an incline and not an ACC engagement. This can have major implications such as an over-reliance on the system, as the driver assumes the ADS is capable of handling a situation when it is not and increased risk of delayed or inappropriate driver interventions.

4.1.2 Incorrect knowledge of system functioning

Incorrect knowledge of system functioning refers to the incomplete or inaccurate understanding of an user on how the system operates including the capabilities and limitations of the system. Examples of this type of mode confusion include - a driver believing that an automated emergency braking (AEB) system detects all types of obstacles, but the system only detects vehicles and not smaller objects like VRUs or animals or a driver assuming that an ADS is capable of detecting objects in all weather conditions when, in reality, heavy rain impairs the system's sensors (poor understanding of ODD). This can have severe safety implications. Incorrect knowledge of system functioning can lead to misuse or disuse of the system and high expectations on the system to perform tasks it is not designed to handle, potentially resulting in critical safety events.

4.1.3 Incorrect interpretation of the safety implications of system functioning

This type of mode confusion occurs when the user fails to recognize the risks or safety implications inherent in how the system operates. If a driver assumes that they can rely on a DCAS system and take their eyes off the road, not realizing the system cannot handle complex traffic merges, they fail to intervene when necessary, exacerbating potential hazards. Similarly, when a driver does not understand that an ADAS requires hands-on supervision because the system could disengage unexpectedly, they may take inappropriate actions due to poor understanding of the safety implications. This can promote unsafe behaviour during system operation and an underestimation of the responsibility of the driver in monitoring the system.

These three factors often interact with each other, thus compounding risks. A driver with incorrect knowledge of system functioning may misinterpret the system's cues, leading to an incorrect perception of system.

This study uses three factors causing mode confusion stated above to understand mode confusion. While the focus is on exploring these causal relationships, prior research has used similar factors as the basis for classifying mode confusion into different types. Our approach does not aim to categorize mode confusion, but rather to investigate the conditions under which it arises. Mode confusion results from a lack of mode awareness. Monk (1986) [7] proposed two types of mode awareness - Type 1 which refers to the general awareness of differ-

ent automation modes and their functionalities and Type 2 which refers to the knowledge of the current active automation mode. Similar definitions have been adopted in studies such as [8] and [9].

4.2 Measuring mode confusion

Quantifying and measuring mode confusion is critical for developing effective mitigation strategies. Several methods have been proposed to assess the degree of mode confusion in automated vehicles.

4.2.1 Subjective Measures

One common approach to measure mode confusion involves self-report measures, where drivers complete surveys or questionnaires after experiencing simulated or real-world driving scenarios. Questionnaires and surveys ask drivers to rate their understanding of the system's current mode, the clarity of the HMI, and their confidence in the system's operation [10]. These subjective measures help gauge the driver's mental model and the potential for confusion. Subjective measures can capture the user experiences and are easily scalable but suffer from misinterpretation of the surveys and subjectivity in the ratings.

4.2.2 Performance-Based Measures

Another method involves analysing driver performance during mode transitions. Simulation studies can measure reaction times and error rates when drivers are required to take over control from the automation. For example, if a driver consistently takes too long to respond during a transition from an automated mode to manual mode, this can be an indicator of mode confusion [11]. These performance-based metrics provide data that can be used to compare different HMI designs and automation strategies. Performance-based measures can provide measurable data but may be difficult to isolate the responses to exact causes. Delayed responses may result from other factors apart from mode confusion such as fatigue or inattention.

4.2.3 Physiological Measures

Physiological data, such as eye-tracking, ECG-derived measures such as heart rate variability, and galvanic skin response, offer additional insights into driver state during automated driving. When drivers are confused about the mode of operation, their physiological signals may indicate increased cognitive load or stress. Researchers have used such measures to validate self-reported data and performance metrics, creating a more comprehensive picture of mode confusion in Automated Vehicles (AVs) [12]. These measures can provide data on cognitive load and attention but require specific instruments which also may be obtrusive and interfere with the natural behaviour.

4.2.4 Task-Related Assessments

Task-related assessments involve embedding secondary tasks into the driving simulation [13]. The assumption is that if a driver is confused about the automation's mode, their ability to manage secondary tasks (such as interacting with the infotainment system) may deteriorate. This degradation in performance serves as an indirect measure of the cognitive impact of mode confusion. By correlating secondary task performance with mode transition events, researchers can further understand the operational impact of confusion on driving safety.

Secondary tasks are typically used in workload assessment. It does not prove mode confusion but can be used as an indirect measure for mode confusion. These assessments can be used to isolate mode confusion in controlled environments and can differentiate between the severity of mode confusion but methods such as freeze-probe or other task-related assessments may interrupt the task flow affecting user behaviour.

4.2.5 Hybrid Assessments

Kurpiers et al., (2020) [9] proposed a new method that combines subjective and objective information to take into account all major aspects of mode awareness (see Fig. 4.1). They divide mode awareness into two pillars - the knowledge pillar and the behaviour pillar. The knowledge pillar constitutes of a measurement of the participant's mental model. A questionnaire was developed for the mental model consisting of five parts which test the user's knowledge about driver assistance systems through subjective ratings and objective evaluation. The behaviour pillar looks into factors such as eye glance data, gaze tracking and driving data for more objective and performance-based measures. Hybrid assessments can capture different dimensions of mode confusion and help confirm findings across different data types reducing dependency on any single method's limitations. However, these can be time consuming and not easily scalable.

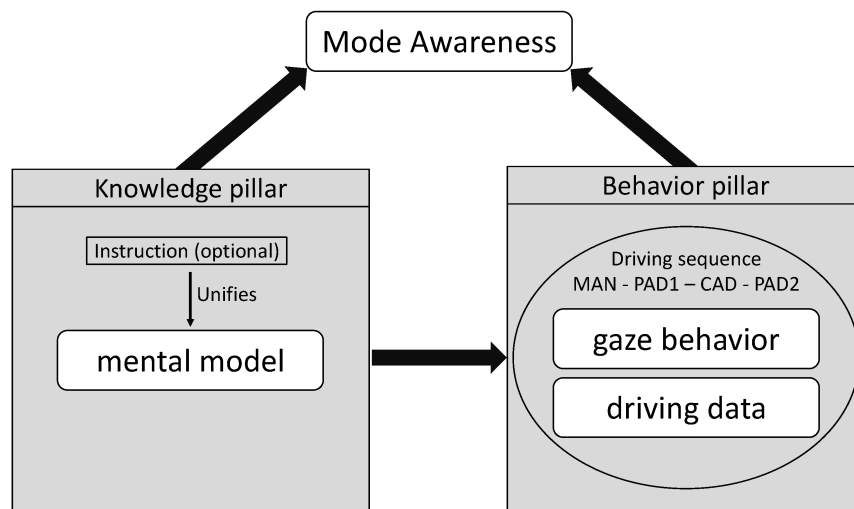


Figure 4.1: Hybrid measurement of mode awareness which is subdivided into a knowledge and a behaviour pillar. Here, MAN is manual mode, PAD1 and PAD2 are Partially Automated Driving modes and CAD is Conditionally Automated Driving.

Each of the methods to measure mode confusion listed above have its own strengths and weaknesses. However, no single method fully captures the complexity of mode confusion. In general, it remains a challenging phenomenon to measure reliably, often requiring a combination of techniques to obtain a thorough understanding.

4.3 Safety analysis of human-machine interactions

This section offers a brief overview of the literature on safety analysis of human-machine interactions in the context of automated driving. It is important to highlight that the focus of this overview is on the methodological approaches employed across various studies

rather than on their specific outcomes. Given the diversity of approaches, evaluation criteria, and implementation settings, summarizing results into a unified set of conclusions would risk oversimplifying the insights each study offers. Instead, this review aims to highlight the range of conceptual and methodological frameworks used to explore the topic of human-machine interactions.

The safety analysis of interactions between humans and ADS is a critical area of research, which aims to ensure that these systems operate safely with human users. This analysis encompasses various factors, including human-machine interaction, system reliability, and the effectiveness of safety protocols. The safety analysis of human-machine interactions in automated driving looks into interaction sequences (visualized via sequence diagrams), closely examining control transitions, and ensuring drivers build accurate mental models. Interaction sequences in human-machine interactions refer to the step-by-step flow of actions and responses between a human and a system while performing a certain task. Sequence diagrams can be used to visually represent this flow of actions and responses between humans and ADS. Using interaction sequences to analyse human-machine interactions can help identify and mitigate potential interaction failures. Warg et al., (2020) [14] proposed a method to find safety issues in human-machine interactions. The study developed interaction sequences between human and ADS as a variant of sequence diagrams. These sequence diagrams served as an input to a cause-consequence analysis with the purpose of finding potential interaction faults that may lead to failures. The study emphasized the need for common terminology across the different domains such as human factors and systems engineering for better identification of faults in system design. This can help make improvements towards creating a safe HMI and interaction sequence for safe transitions. Janssen et al., (2019) [15] proposed a hidden Markov model (HMM) to describe the uncertainty about the combination of automation mode and human beliefs, and the transitions between them. Transitions refer to the process of shifting control authority between the human and the ADS. Transitions are especially significant during take-over events when the vehicle must move from automated mode to manual control or vice versa. Lu and De Winter (2015) [16] provided a rigorous review of the essentials of human-machine interaction in automated driving, focusing on control authority transitions. Ensuring that the system provides adequate notice (often through multi-modal alerts) so that drivers have enough time to regain control is of prime importance. The HMI should communicate the current state and impending transitions clearly to prevent mode confusion. Human response times can vary, and analysing how different scenarios (such as distractions or out-of-the-loop phenomena like reduced situation awareness) affect the transition process is necessary. For safe interaction, it is crucial that the driver's mental model closely aligns with the ADS' actual functionality. Misunderstandings can lead to over-reliance or distrust. HMIs that provide a clear, timely, and consistent feedback about the system's status and intentions help create and maintain better mental models. Training and repeated exposure also help drivers build more accurate mental models, which enhances situation awareness and overall safety [17]. It is also important to emphasize that mode confusion in automated driving is a construct, similar to concepts like workload or distraction. Identifying mode confusion in practice can be challenging because its observable effects — such as delayed reactions or inappropriate responses — can also result from other factors like high workload or distraction. As a result, it is often difficult to isolate mode confusion as a unique cause, since it overlaps with other cognitive demands placed on the driver.

4.4 Real world examples of mode confusion

Several on-road studies have been conducted to study the problem of mode confusion. Endsley (2017) [18] conducted a naturalistic driving study on the autonomy features in the Tesla

Model S. The author recorded her experiences over a 6-month period, including assessments of situational awareness (SA) and problems with the autonomy. The study found issues regarding driver training, mental model development, mode confusion, and unexpected mode interactions. Mode confusion was the most frequent problem encountered. This confusion was attributed to the fact that the lever controlling the ACC and autosteer functions was located directly below the turn signal lever leading the car to speed up on several occasions when the intention was to change lanes, necessitating an intervention. Autosteer is a Tesla feature that helps the car stay centred in a lane, based on lane markings and other vehicles. Banks et al., (2018) [19] reported similar findings with drivers frequently assuming that the system was in one mode when it was actually in another. A major concern highlighted by this study was that the occurrence of mode confusions remained high despite the drivers being alert and well-motivated to remain in control of the vehicle. Wilson et al., (2020) [20] also conducted an on-road study with the Tesla Model S to examine driver trust and mode confusion. Similar to earlier studies, several incidences of mode confusion were recorded, where participants believed the vehicle was in Level-2 automation, but was in fact either in adaptive cruise control (without lateral control; Level 1) or manual driving (Level 0). The study also remarked that the drivers rather than noticing the mismatch in their understanding through the vehicle's HMI, were often prompted by the researchers conducting the study regarding mode confusion, or by noticing cues from the vehicle's unexpected behaviour. The study also included anecdotes from the participants regarding mode confusion such as:

P9, male, aged 51 "I noticed that uh... while my foot wasn't on the accelerator I still had my hands on the wheel, and I noticed having to command the vehicle to follow the lane, and therefore I realized that it wasn't steering itself, and then I realized that the dash didn't have the large blue icon [automation symbol], which suggested that AutoPilot wasn't fully in."

These studies collectively highlight the issue of mode confusion, showcasing its critical impact on safety and traffic dynamics. While none of the cases of mode confusion in these studies lead to hazards, these studies pointed to the problems mode confusion can potentially create. Addressing mode confusion is not only essential for mitigating risks but also for enhancing the overall driving experience, making it a vital area for continued investigation.

4.5 Conclusions

The emergence of mode confusion in L2 and L3 automated vehicles poses a significant challenge for both designers and type-approval authorities. As the industry moves toward higher levels of automation, ensuring that drivers maintain an accurate understanding of system status will be crucial for safety. Ongoing research is needed to refine the measurement techniques and develop standardized mitigation strategies that can be integrated into future vehicle designs. Collaboration between academia, industry, and regulatory bodies will be essential to develop guidelines that address mode confusion in a holistic manner. Mode confusion can have serious implications where the transition between automated and manual control is critical. As the technology evolves, continued research and interdisciplinary collaboration will be paramount to ensure that AVs not only offer enhanced convenience but also maintain the highest safety standards.

5 Introduction to SOTIF and functional safety assessment

As vehicle automation advances and accountability for driving tasks gradually transfers to the vehicle, the necessity for transformed safety assessment methods for these vehicles evolves accordingly. In SAE Level 0-2 vehicles, the responsibility of the driving task lies with the human driver. Complementary to the passive safety of the vehicle, the primary obligation of vehicle manufacturers with these level 0-2 functionalities is centered on ensuring the safety of the vehicle's electrical and electronic (E/E) systems. The principal aim of this safety is to minimize or ideally prevent the severity of harm, decrease the chances of a harmful situation arising, and guarantee that even when a fault appears, the human driver remains capable of controlling the situation. From SAE Level 3 onwards, the vehicle assumes partial or even full control over the driving task, shifting responsibility for any insufficiencies in system performance away from the human driver. As a result, norms and standards have evolved to evaluate not just the functional safety of a vehicle but also the safety of its intended functionality. An integral component of assessing vehicle functionalities for safety involves developing a safety case. In this process, the OEM demonstrates the safety of its vehicle functionalities by constructing safety arguments following the cited standards. This chapter delves into each type of safety assessment and demonstrates how these methods complement each other.

First, we explore the relationship between each safety norm and the three-circle behavioural model illustrated in Fig. 5.1 [21]. Here, behaviour refers to the interaction between a system and its environment, where the system usually includes the driver of the vehicle (when applicable). The required (or ideal) behaviour signifies what is necessary for a system to be deemed valid and safe. The specified behaviour defines what the system designer considers to be safe and valid behaviour, translating requirements into practice. Lastly, the implemented behaviour represents the actual performance of the system, which may differ from the required and specified behaviours in various ways.

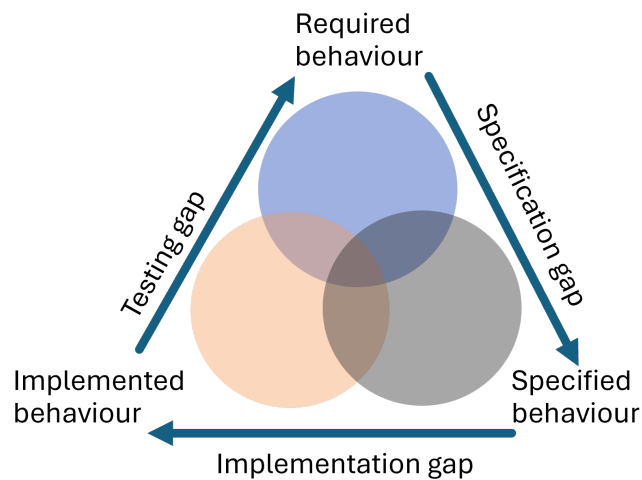


Figure 5.1: Three-circle behavioural model for comparing SOTIF and functional safety [21, Figure 2].

As discussed in [21], the construction of a safety argument essentially involves a series of deductive steps. During this process, assumptions might be introduced, either explicitly or implicitly. It is possible for these assumptions to be erroneous in certain contexts, rendering the entire chain of deduction unsound. This issue is known in the literature as a *deduction gap*. In Fig. 5.1, three specific deduction gaps are identified. The first is the specification gap, which is a deductive discrepancy where the defined behaviour does not match the required behaviour. This often occurs when there is a misunderstanding about the intended functionality or the context in which it operates. The second gap, the implementation gap, arises when the actual implementation deviates from the specification. This usually happens when designers misinterpret the specifications, perhaps because the function operates in a context different from the one outlined. Lastly, the testing gap is present when the implemented behaviour is not completely verified to align with the required behaviour. This gap frequently exists because the required behaviour is often detailed in a very specific operational design domain, making it extremely difficult to test or verify the system across all these various scenarios. It must be noted that, when looking at the three-circle behavioural model, the best case would be when the three circles fully intersect (as such eliminating all deductive gaps).

5.1 ISO 21448: Safety Of The Intended Functionality

The main objective of the ISO 21448 SOTIF [1] standard is to describe the activities and rationale used to ensure that the risk level, associated with all identified SOTIF-related hazardous events, is sufficiently low. Here, SOTIF-related hazardous events are defined as hazardous events as a result of functional insufficiencies (Def. 3). Such functional insufficiencies are not necessarily always active in a system, and are actuated by so-called triggering conditions (Def. 6). Such triggering conditions can be due to external factors, related to the environment in which the vehicle is driving, or internal factors, related to the inner workings of the vehicle. Below we give two examples of functional insufficiencies due to an external and internal factor.

- *Functional insufficiency triggered by external factor:* A vision-based object detection system is no longer able to detect objects (*functional insufficiency*) when the contrast

between such an object and the environment is too low, due to, e.g., heavy fog (*triggering condition*).

- *Functional insufficiency triggered by internal factor*: An AEB system results in a false positive braking action (*functional insufficiency*) while driving in a corner and seeing an object in front which, in fact, was not standing on the road (*triggering condition*).

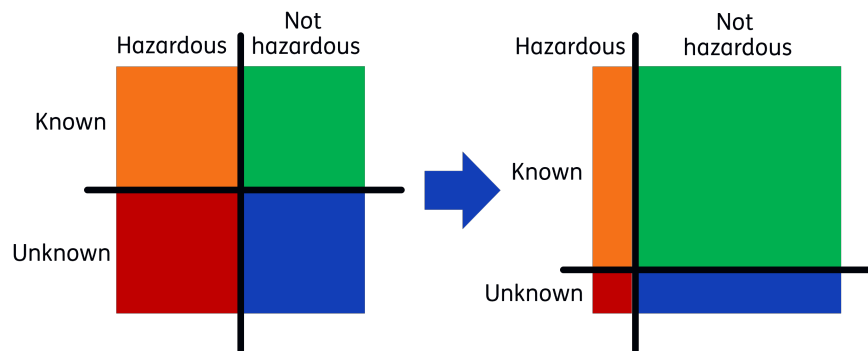


Figure 5.2: The essence of what SOTIF tries to achieve: to minimize the hazardous unknown scenarios, and mitigate the hazardous known scenarios.

The main objective of a SOTIF analysis for a system functionality/subfunctionality can be visualized as in Fig. 5.2. Here, the left-hand side represents the starting point of the SOTIF analysis, where usually there is some prior knowledge on some hazardous and non-hazardous scenarios, but definitely not an exhaustive list. It is then the main goal to:

1. perform a risk acceptance evaluation of known hazardous scenarios, based on the analysis of intended functionality
2. reduce the probability of known hazardous scenarios to an acceptable level through functional modification,
3. reduce the probability of the unknown scenarios causing potentially hazardous behaviour to an acceptable level through an adequate verification and validation strategy.

When considering the part a human driver plays in an automated vehicle, SOTIF addresses the potentially harmful consequences associated with a driver through the classification of misuse. This is further divided into direct and indirect misuse. Direct misuse involves the improper use of a feature that might lead to the generation of hazardous behaviour within the system, thereby acting as a possible triggering condition. An example here could be: activating a highway functionality in an urban setting, in which the vehicle does not detect and react to, e.g. vulnerable road users, resulting in a hazardous scenario. Indirect misuse, on the other hand, does not directly pertain to a triggering condition but may diminish controllability or heighten harm when hazardous behaviour takes place. An example here could be that the driver is inattentive when attention is required, causing a reduction in controllability when a hazardous situation occurs.

Since SOTIF primarily covers reasonably foreseeable misuse, that is, unintended but in a predictable way, abuse (Def. 8) is out of scope in SOTIF due to its unpredictable nature (there is no way to place accurate statistics on abuse in that sense).

5.2 ISO 26262: Functional Safety and its relation to SOTIF

The ISO 26262 [22] standard addresses the functional safety aspect of automated vehicles by concentrating on minimizing the unreasonable risks that arise from failures in electrical and electronic (E/E) systems. In contrast, the SOTIF standard (ISO 21448 [1]) specifically targets the elimination of unreasonable risks resulting from functional insufficiencies. Annex 2 from the SOTIF standard [1] and [21] clarifies the exact position of the standard together with ISO 26262. The first mean of comparison is through Fig. 5.1.

Although ISO 26262 deliberately excludes safety concerns that arise during the correct (nominal) behaviour of the system, SOTIF specifically addresses those risks, especially when the intended behaviour of the system is not safe enough for certain situations. ISO 26262 focuses on hazards caused by system or hardware failures, whereas SOTIF assumes the system is working as intended, but may still be unsafe due to limitations in design or understanding of the environment. However, SOTIF can also consider how a system responds to failures, particularly when that response introduces new safety concerns. To closely align the implemented behaviour with the specified behaviour, both the ISO 26262 and SOTIF standards are applicable. For more intricate systems, such as ADAS or AD systems, ISO 26262 presents challenges as it cannot fully encapsulate the complexities of the real world, leading to the inevitability of "unknown hazardous scenarios" and the inability to comprehensively validate many system facets. Thus, SOTIF becomes more appropriate for significantly aiding in the validation of the implemented behaviour.

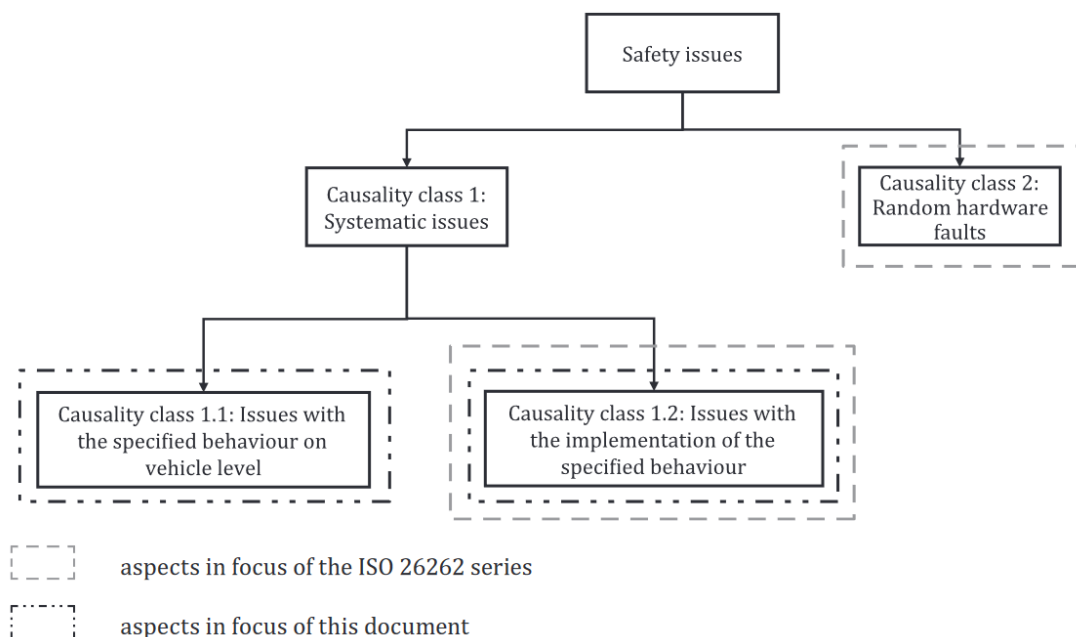


Figure 5.3: Safety issues grouped in causality-classes [1, Figure A.18].

Safety issues can be grouped according to causality. Fig. 5.3 distinguishes between class 1 and class 2 causalities of safety issues. In class 1, the safety issue has a causally decomposable root cause and, in addition, is consistent and repeatable. In class 2, safety issues occur sporadically and may lack a direct causal link. Importantly, class 2 is fully addressed by ISO 26262. Within class 1, further subdivisions exist. Subclass 1.1 concerns issues tied to

specified behaviour at the vehicle level, which are explained as insufficiencies in vehicle-level specifications and are explicitly covered by SOTIF. Subclass 1.2 involves issues with the implementation of such behaviour, involving both standards and potentially arising from performance shortcomings, specification insufficiencies at the element level, and various design and implementation issues. This area overlaps in both standards: ISO 26262 targets issues related to potential E/E system failures, including subsystems, components, or other elements, while SOTIF addresses performance insufficiencies and specification gaps impacting intended functionality, where situational awareness is crucial for safety.

It is crucial to recognize that, as illustrated by these two figures and their explanations, ISO 26262 and SOTIF effectively enhance one another, making them suitable to serve independently as safety arguments for a product. Annex 2 of ISO 26262 outlines a procedure for harmonizing the safety arguments derived from adhering to both standards.

6 Methodology Design

6.1 Introduction

The previous chapters of the report describe the results of the literature study conducted on two parallel tracks:

- Mode confusion in automated vehicles; and
- Vehicle safety assessment using the SOTIF methodology.

This chapter describes the process adopted to combine the knowledge collected in the literature research towards a composite methodology that can be used to assess the quality of a human-machine interaction, in the case of an automated driving system.

6.1.1 Scope

The first step towards the design of such a process was to identify a delimited scope, purpose and intended user of the developed methodology, so as to be able to focus the analysis. The subsequent subsections further delineate the decisions taken in this direction.

6.1.1.1 Hazardous Situation

From a SOTIF point of view, the aim is to explore functional insufficiencies, how these are triggered by the system or the environment, and whether they can potentially lead to a hazardous situation. In the scope of this work, we do not consider the downstream analysis of how mode confusion could eventually lead to a hazardous situation. Instead, we treat mode confusion as the hazardous situation itself.

This decision raises the additional question of whether mode confusion can be treated as a hazardous situation by itself, or if mode confusion is a triggering condition, which leads to other hazardous situations. Since the SOTIF framework aims to evaluate a quantifiable risk rating for hazardous situations, this is a crucial difference from the methodology design point of view.

Although, as discussed in Section 4.4 it is established that the presence of mode confusion is not desirable from the safety case perspective, it can be argued that the presence of mode confusion by itself does not amount to a hazardous situation. Rather, mode confusion is likely to lead to another situation which amounts to a hazard. The following example can help illustrate this distinction:

While driving on a highway, a driver tries to enable an L2 hands-off system, by actuating a button on the steering wheel, but accidentally presses an adjacent button instead. The driver does not receive visible feedback from the vehicle HMI about the current automation state of the vehicle. Due to this, the driver believes that it has actuated the automated driving function and release control of the

steering wheel. The vehicle consequently drifts into an adjacent lane and collides with another vehicle.

In this case, the pressing of the wrong button is a *triggering condition*, supplemented by the absence of visual feedback to the driver (*functional insufficiency*) that lead to mode confusion. However, mode confusion also acts as a *triggering condition*, which, combined with the action of releasing control of the steering wheel, drifting towards an adjacent lane, as well as the presence of another vehicle in the adjacent lane lead to the collision (*the hazardous situation*).

In the absence of additional information on the vehicle environment, it is not feasible to arrive at a quantification of the risks during a safety assessment of this human-machine interaction. Therefore, in this project, it was chosen to restrict the analysis to the step of the occurrence of mode confusion, and to treat mode confusion as a triggering condition. The extension of the analysis to evaluating the resulting hazardous situations is considered out of scope of this project, and part of future research.

6.1.1.2 End-user

In order to ensure applicability from the Ministry of Infrastructure and Water Management's perspective, it was chosen to design a methodology from the perspective of the type approval authority, such as the RDW (*Dienst Wegverkeer*) in the Netherlands. This decision creates additional requirements for the methodology:

- The methodology uses the finished output of the interface, as fitted on the vehicle to be approved, as the starting point.
- Documentation utilised for the analysis should be reasonably available to the type approval authority (e.g. user manuals, documentation of the vehicle, etc.)
- Any additional documentation required to conduct the analysis, such as design documentation, should be specified within the outcome of the project such that it can be requested from the OEMs.

6.1.1.3 Resulting Research Question

In conclusion, the methodology developed in the project enables a type-approval authority to apply the SOTIF framework to assess human-machine interactions for automated driving, with the objective of avoiding mode confusion.

6.1.2 Approach

The methodology was designed by means of a series of semi-structured brainstorming sessions, designed to help combine the knowledge assimilated in the parallel literature research tracks, combining domain knowledge in the assessment of HMIs and mode confusion, with the SOTIF framework. In consecutive steps, the SOTIF approach was adapted to address the research question defined in Section 6.1.1.3.

The framework was validated using an on-paper exercise for the Mercedes-Benz EQS, with an L3 Drive Pilot [23] system, leading to further refinements of the methodology.

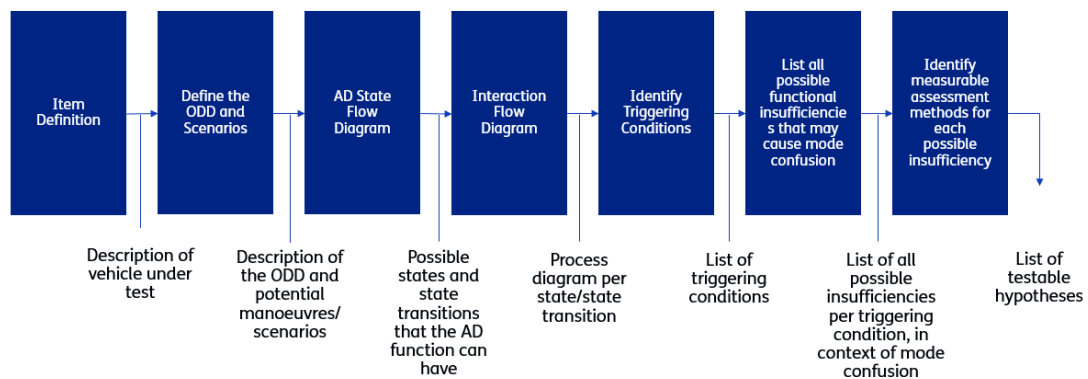


Figure 6.1: Proposed methodology for using the SOTIF framework to assess Human Machine Interfaces to avoid mode confusion. The blue boxes include the process steps and the text placed below each arrow indicates the expected outcomes/deliverables at each stage.

6.2 Proposed Methodology

The proposed methodology, as reported in Figure 6.1 is composed of several consecutive steps aimed at providing a structured approach to increase the coverage of various aspects of human-machine interaction.

The entire methodology is proposed to be conducted in two steps. First, an on-paper exercise is conducted, based on a detailed analysis of the owner's manual. Subsequently, an on-road test session is conducted to evaluate the critical and/or ambiguous states and transitions identified in the first phase. This step may also lead to some revisions of the analysis conducted in the first step.

The following subsections describe each step, and relevant tools/frameworks that can be used for this, in more detail.

6.2.1 Item Definition

This step aims to identify the vehicle under test, with an emphasis on the automation modes and the interfaces between the user and the vehicle. The following guiding questions can be used:

1. What automation features exist, and at what level of automation?
2. What interfaces exist:
 - a) In what form can the system provide information to the user?
 - b) In what form can the user actuate/react to the HMI?

6.2.2 ODD and Scenario Definition

For each Automated Driving System (ADS) on board, the specific conditions in which the system can (not) operate should be enumerated. This information can be collected from an analysis of the user manual from the vehicle OEM.

6.2.3 AD State Transition Diagram

Subsequently, a state transition diagram that covers the changes of states of the different functionalities of the ADS should be designed. This diagram describes the states or conditions that the machine (in this case, the ADAS/ADS) goes through its lifetime, in response to events.

Examples of this could include situations where the vehicle detects that it is in the ODD for a certain automated driving (assistance) feature and communicates this to the user, when the user actuates said ADS, and eventually, when the system is disabled by the user or by the vehicle when it detects the end of the ODD.

6.2.4 Interaction Flow Diagram

For each state flow identified in the previous step, an interaction flow diagram should be designed. An example of such an approach is shown in Figure 6.2¹. The aim of this diagram is to capture all the flows of information and inputs that may exist between the Automated Driving System (ADS), the Human Machine Interface (HMI) and the Human User (HU). Each block in the diagram represents a state or (internal/external) process at the ADS, HMI or HU, and each arrow represents the flow of a Stimulus (S) or Actions (A).

Note that the interaction flow diagram also captures a simplified mental model of the human user, through the Perception (P), Comprehension (C), Processing (PR) and Decision (D) blocks in the HU. These internal processes should also be considered in the analysis of the human-machine interaction, particularly for mode confusion.

6.2.5 Triggering conditions

Each arrow and state block within the interaction flow diagram represents a (desired) flow of information between the different actors in the interaction process. Therefore, each of these items, if not designed for adequately, could lead to insufficiencies in the human-machine interaction. Additionally, the intermediate flows within the HU represent the mental model and physical capabilities of the human. Therefore, a misalignment between this and the information flow, could also lead to insufficiencies in the system.

Therefore, each arrow and block within the interaction flow diagram could be considered as a source of potential triggering condition. For example, when a visual cue from a certain assistance system is perceived, but potentially interpreted incorrectly (i.e., interpreted as another assistance system, or perhaps a completely different functionality), this would be a functional insufficiency triggered by the fact that the system behaves differently from the drivers expectation, resulting in mode confusion.

6.2.6 Triggering Conditions to Potential Functional Insufficiencies

After identifying the possible triggering conditions, each triggering condition can be translated to potential functional insufficiencies. The following types of information flows can ex-

¹The interaction-flow diagram is crafted using the assessor's existing knowledge of the vehicle, such as information from the operating manual. After conducting tests, if it is discovered that the actual interaction flow differs from the diagram due to errors or unclear instructions in the manual, this discrepancy can be identified as a potential cause of mode confusion "Type II", which relates to incorrect understanding of how the system operates.

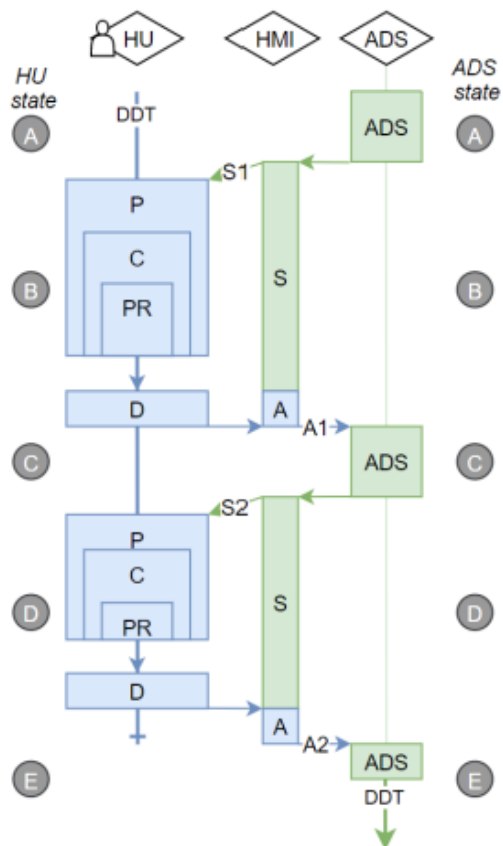


Figure 6.2: Example of an interaction flow diagram, taken from [14]. Here, ADS is the Automated Driving System, HMI is the Human Machine Interface, HU is the Human User, DDT is the dynamic driving task, P is the Perception, C is the Comprehension, PR is the Processing, S is a stimulus, A is the action and D is the Decision of the human.

ist:

1. From the HMI to the human user:
 - a) Visual
 - b) Auditory
 - c) Tactile/haptic
2. From the human user to the HMI:
 - a) Actuation of the pedals
 - b) Providing torque inputs on the steering wheel
 - c) Actuation of a lever/button
 - d) Gaze
 - e) Position of Hands
 - f) Voice command
 - g) Gesture

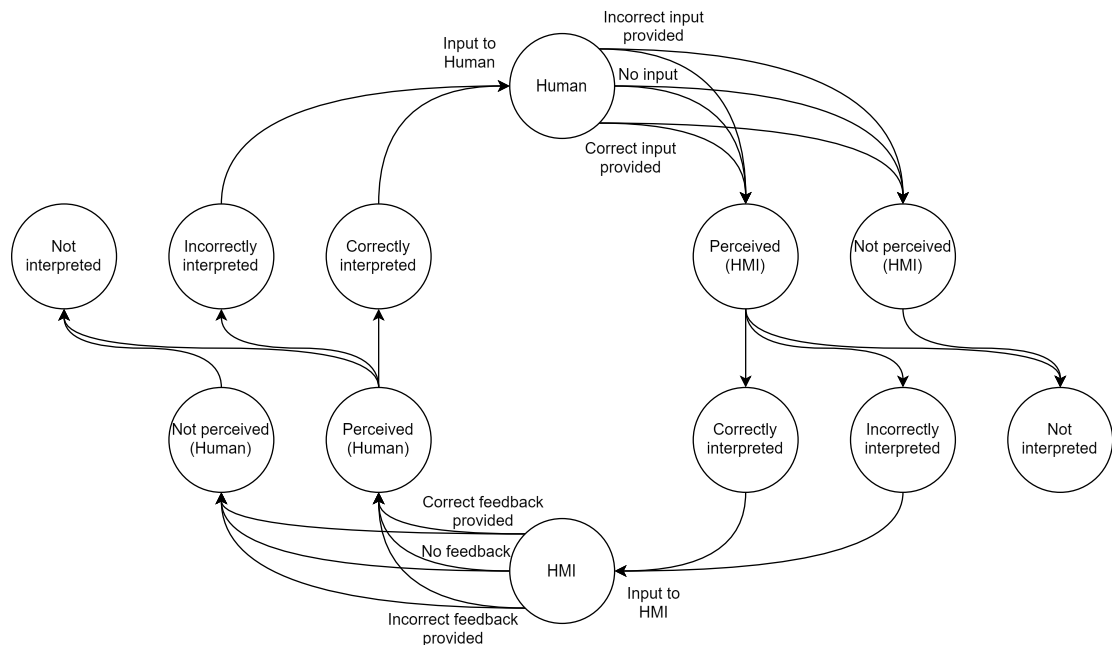


Figure 6.3: Possible functional insufficiencies in the "Human-HMI" communication chain. Example: when a driver provides the correct input, but it is interpreted incorrectly by the HMI, this could be perceived incorrectly by the driver, possibly resulting in mode confusion.

For each flow of information or input from the human user, the information/input can be considered to flow through a series of three consecutive gates (transmission, perception, understanding). At any of these stages, if the information does not pass through or incorrectly, there is the potential for mode confusion. The possible functional insufficiencies, resulting from the communication between driver and HMI, can then be highlighted through the graph in Figure 6.3.

Finally, an additional source could be latency in the feedback from the system to the user, particularly if it is longer than expected for the user.

Subsequently, an intersection can be identified between the different possible information/input types, and the different possible cases listed above, to identify possible situations in the specification or implementation of the system that could lead to mode confusion. This can be done in the form of a matrix that combines the possible cases of mode confusion with the input / information type, as shown in 6.4.

6.2.7 Identify measurement methods for each possible insufficiency

Finally, for each possible insufficiency identified in the previous step, a measurable test can be defined to check whether the specification and implementation of the function are adequate for safe operation and functioning. These parameters can then be validated on the actual vehicle through suitably designed stationary and on-road testing.

Status of Transmission of Information/User Input	Perception	Understanding	HMI to Human User			Human User to HMI			
			Visual	Auditory	Tactile	Gaze	Position of Hands	Actuation of Button/Lever	Voice Command
Not Transmitted	Not Perceived	-	Inadequate Specification	Inadequate Specification	Inadequate Specification	Insufficient understanding of the system	Insufficient understanding of the system	Insufficient understanding of the system	Insufficient understanding of the system
			Similar to other messages (location, size, colour, form)	Similar to other messages (tone, volume, location, frequency)	Similar to other messages (location, pattern, frequency, intensity)	Similar to other patterns (e.g. target location is similar to other functions); Wrong recognition of the gaze	Similar to other patterns (e.g. target location is similar to other functions); same button has multiple functions); Wrong recognition of the button	Similar to other patterns (e.g. target location is similar to other functions); Wrong recognition of the voice command.	Similar to other patterns (e.g. target location is similar to other functions); Wrong recognition of the voice command.
	Incorrectly Perceived	-							
Correctly Transmitted	Not Perceived	-	Not visible enough (colour, intensity, form, size)	Not audible enough (Tone, volume, location, frequency)	Not perceptible enough (Location, pattern, frequency, intensity)	Occluded view (e.g. sunglasses etc.); Inadequate specification (not trained for the target population)	Occluded view (e.g. Hands not visible); Inadequate specification (not trained for the target population)	Inadequate specification (not trained for target population (accent/tone/language))	Inadequate specification (not trained for target population (accent/tone/language))
			Similar to other messages (Location, size, colour, form)?	Not audible enough (Tone, volume, location, frequency)?	Not felt enough (Location, pattern, frequency, intensity)?	Similar to other patterns (e.g. target location is similar to other functions); Wrong recognition of the gaze	Similar to other patterns (e.g. target location is similar to other functions); same button has multiple functions); Wrong recognition of the button	Similar to other patterns (e.g. target location is similar to other functions); Wrong recognition of the voice command.	Similar to other patterns (e.g. target location is similar to other functions); Wrong recognition of the voice command.
	Incorrectly Perceived	-							
	Correctly Perceived	Incorrectly Understood	Insufficient understanding of the system	Insufficient understanding of the system	Insufficient understanding of the system	Inadequate Specification (Missing function)	Inadequate Specification (Missing function)	Inadequate Specification (Missing function)	Inadequate Specification (Missing function)
		Not Understood	Insufficient understanding of the system	Insufficient understanding of the system	Insufficient understanding of the system	Inadequate Specification (Missing function)	Inadequate Specification (Missing function)	Inadequate Specification (Missing function)	Inadequate Specification (Missing function)
Incorrectly Transmitted	-	-	Inadequate Specification	Inadequate Specification	Inadequate Specification	Insufficient understanding of the system	Insufficient understanding of the system	Insufficient understanding of the system	Insufficient understanding of the system

Figure 6.4: Examples of possible sources of mode confusion. Here, the different colours of the cells distinguish between the various sources of the mode confusion: white cells highlight an "Insufficient Implementation", orange cells highlight "Insufficient Specification" and the yellow cells highlight Insufficient Understanding".

7 Methodology application

To evaluate the proposed methodology, road tests were executed in the Düsseldorf area, Germany. A BMW 740d was selected for these trials due to its diverse range of driving modes, covering SAE levels from 0 to 3, with speeds of up to 60 km/h in level 3 mode.



Figure 7.1: BMW 740D testing vehicle.

This vehicle is particularly intriguing for testing because it incorporates a SAE level 3 ALKS system, in line with UNECE R157 on Automated Lane Keeping Systems [24], i.e., the vehicle is able to take over the dynamic driving task in certain conditions, with the driver as a fall-back. In addition, the vehicle is equipped with a SAE level 2 hands-off system, referred to as Driver Control Assistance Systems (DCAS) under UNECE R171 [25], i.e., the vehicle accelerates and steers itself without driver input, where the driver keeps its eyes on the road to monitor the situation. Finally, the vehicle is also equipped with the standard level 0-2 hands-on systems and active safety features. There are a few other vehicle options available with this wide array of modes. As of the time this was documented, two brands of L3 equipped vehicles are available on the market: Mercedes-Benz with the S-class and EQS, and BMW with the 7-series. For testing purposes, no EQS or S-class models from Mercedes-Benz were available with ALKS capable of 95 kph, meaning they would essentially offer the same functionality as the BMW but without the DCAS.

7.1 Pre-testing

7.1.1 Item definition

In this section, we introduce all the functions or modes that are considered in the scope of this experimental campaign, and in what form the user can actuate and/or react to the HMI. Note that the description of the functionality is largely taken from the manufacturer's owner manual [26]. Some of the exact state transitions were not clear by reading the manual (e.g., in which mode the vehicle ends when coming out of L3), these transitions were later filled based on simple vehicle tests. Although this is not pre-testing, it can be assumed that a vehicle assessor could reasonably ask an OEM for providing a relatively comprehensive state-transition diagram. First, the functions or modes of automation are summarized below.

- **A. Base (no active safety or comfort functions active):** In this mode, the vehicle does not have active warning systems and active safety systems.
- **B. Supporting safety functions active:** active safety systems such as the autonomous braking system, speed limit information, forward collision warning, and lane departure warnings are active.
- **C. Cruise Control:** Cruise Control allows a set speed to be specified using the buttons on the steering wheel. The set speed is then maintained by the system. It does this by automatically accelerating and braking the vehicle as necessary.
- **D. Distance Control:** With the Distance Control, a distance to a vehicle driving ahead can be set in addition to the Cruise Control.
- **E. Assisted Driving Mode:** Assisted Driving Mode enhances Distance Control with a Steering Assistant with tracking. The system helps the driver keep the vehicle in the lane. It does this by performing supporting steering wheel movements (i.e., eyes on, hands on).
- **F. Lane Change Assistant:** The vehicle can perform a lane change when initiated by the driver, which is done either through the turn indicator or by looking at the side mirror when a lane change is suggested by the vehicle itself.
- **G. Assisted Driving Mode Plus:** When available, the driver can release the steering wheel while still being responsible for monitoring the driving situation and intervening when necessary (i.e., eyes on, hands off).
- **H. Personal Pilot:** The Personal Pilot supports the driver in traffic queues on motorways. The Personal Pilot can temporarily take over the driving task for this purpose. The system performs the following functions:
 - Steering
 - Braking
 - Acceleration
 - Distance Control
 - Staying in lane
 - Avoidance manoeuvres within the lane
 - Forming an emergency lane (i.e., a lane in between driving lanes to allow emergency vehicles to pass)

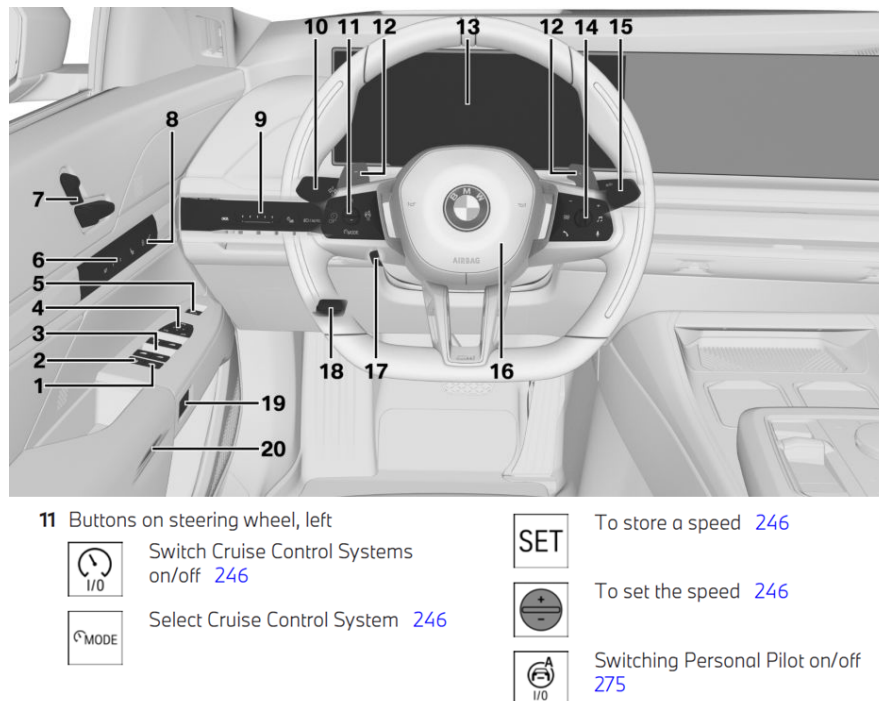


Figure 7.2: Steering interface of the BMW 740d [26].

When the Personal Pilot is switched on, secondary activities are possible while driving, for example, using the communication systems or the Integrated Owner's Handbook. However, the driver must be able to resume the driving task at any time, for example, following a takeover request by the system or if irregularities are detected.

The physical interface with the driver is taken from the manual. The interface for the driver to turn on certain functionalities is located on the steering wheel, as depicted in Fig. 7.2. Apart from the physical controls, the steering wheel incorporates LEDs within its rim as shown in Fig. 7.3. These lights indicate the active function through different colours corresponding to function state, and alert the driver if their attention is needed, or an action is required ².

Besides the steering wheel interface, the dashboard displays various information, including the active driving assistance features and any alerts for the driver if manual control is needed. The dashboard interface is shown in Fig. 7.4, and all possible modes and notifications are given. In Appendix A a copy of the relevant BMW manual pages is provided. Finally, the vehicle has a heads-up display which offers a simplified view of the information provided on the dashboard.

7.1.2 ODD and Scenario definition

The ODD of each function or Operating Requirements (OR) are copied from the manual and written below.

²Please note that the BMW manual indicates that the Assisted Driving Mode and Assisted Driving Mode Plus activities should also be displayed via LEDs on the steering rim, with a green light specified. However, despite this option being explicitly enabled during the tests, only the driver take-over requests were indicated by the illumination of the steering wheel.

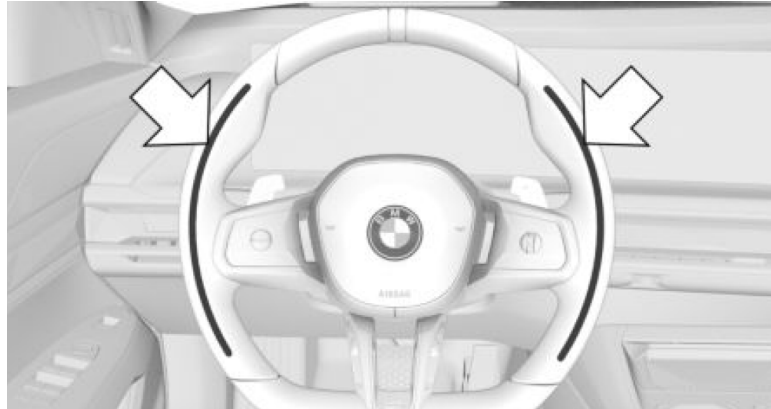
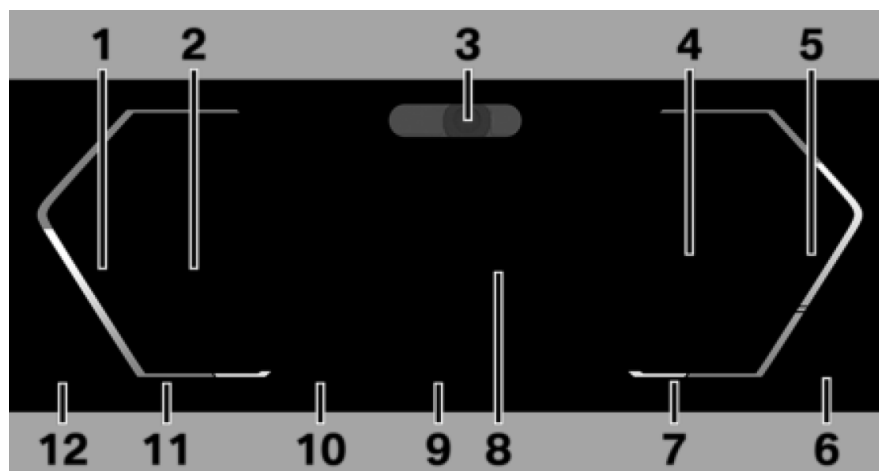


Figure 7.3: Steering wheel lighting interface of the BMW 740d. [26]



- | | | |
|---|--|---|
| 1 Speedometer | 5 Power display 174 | 11 Time 180 |
| 2 Driver assistance systems 243 | Revolution counter 175 | 12 Fuel level indicator 180 |
| Parking assistance systems 283 | 6 Engine temperature 176 | Range 180 |
| 3 Driver Attention Camera 236 | 7 Outside temperature 176 | |
| 4 Check Control 164 | 8 Central display area 176 | |
| Selector lever indication 149 | Shift Lights 176 | |
| Optimum shift indicator 174 | 9 My Modes drive mode 154 | |
| Selection lists 173 | 10 Speed Limit Info 243 | |
| Efficiency Coach 368 | Speed Limit Assist 268 | |

Figure 7.4: Dashboard interface of the BMW 740d [26].

- **C. Cruise Control:** The system can be activated starting at 30 km/h.
- **D. Distance Control:** The maximum speed which can be set is limited and depends on the vehicle and its equipment. Depending on the equipment, higher set speeds can also be selected after switching to Cruise Control without Distance Control. The system can also be activated when the vehicle is at a standstill. The system's detection capability and automatic braking capacity are limited. For example, two-wheeled vehicles may not be detected. The system does not decelerate in the following situations:
 - For pedestrians or similarly slow road users.
 - Depending on the equipment, at red traffic lights.
 - For crossing traffic.
 - For oncoming vehicles.

The vehicle cannot drive off automatically in some situations, for example:

- On steep upward gradients.
- Before bumps or rises in the road.
- When towing a heavy trailer.

In such cases, the accelerator pedal needs to be pressed.

- **E. Assisted Driving Mode:** The operating requirements are as follows:
 - Depending on the equipment: speed below 210 km/h or 180 km/h.
 - The lane width is sufficiently wide.
 - Hands on the steering wheel rim.
 - Sufficiently wide curve radius.
 - Driving in the centre of the driving lane.
 - The sensor system calibration process is complete.
 - Distance Control is active.
 - Seat belt on the driver's side fastened.
 - Front collision warning is active.
 - Depending on the equipment: Side collision warning is active.
 - With a trailer tow hitch: operation with a trailer or operation with a rear carrier must be set on the control display in accordance with the use.
- **F. Lane Change Assistant:** The operating requirements are as follows:
 - The functional requirements for Assisted Driving Mode are met.
 - Driving on a road without pedestrians or cyclists and with physical barriers separating oncoming vehicles, for example crash barriers.
 - There is sufficient longitudinal clearance between other vehicles in the adjacent lane
 - Lane boundaries that can be driven over are detected.
 - Maximum speed 180 km/h.
 - The minimum speed is country-specific.
 - With a trailer tow hitch: operation with a trailer or operation with a rear carrier must be set on the control display in accordance with the use.

- **G. Assisted Driving Mode Plus:** The operating requirements are as follows:
 - Assisted Driving Mode Plus must be available in the country in which the vehicle is being driven.
 - The functional requirements for Assisted Driving Mode are met. Assisted Driving Mode is active and the LED displays on the steering wheel are switched on.
 - Driving on roads similar to motorways without pedestrians or cyclists and with physical barriers as separation from oncoming vehicles, for example, crash barriers.
 - Lane boundaries are detected.
 - The lane width is sufficiently wide.
 - Sufficiently wide curve radius.
 - The road and position of the vehicle must be clearly recognised by the navigation system.
 - The function must be available on the road on which the vehicle is being driven.
 - Aerials located in the roof must not be covered, for example, by roof loads or snow residue.
 - The Driver Attention Camera in the instrument cluster detects that the driver is looking at the traffic situation.
 - With a trailer tow hitch: operation with a trailer or operation with a rear carrier must be set on the control display in accordance with the use.
 - Assisted Driving Mode Plus is enabled in the vehicle.
 - The navigation data must be up to date.
 - The systems in the vehicle, e.g. the Attentiveness Assistant and the Driver Attention Camera recognise that the driver is rested.
- **H. Personal Pilot:** The operating requirements are as follows:
 - The Personal Pilot must be available in the country in which the vehicle is being driven.
 - The Personal Pilot is activated in the vehicle.
 - The map data of the navigation system must be up to date.
 - The privacy settings must be activated.
 - There is an active ConnectedDrive contract.
 - Mobile phone reception must be guaranteed.
 - The vehicle is being driven on a motorway section approved for use of the Personal Pilot.
 - There is a traffic queue.
 - The current speed is below 60 km/h.
 - The road and position of the vehicle must be clearly recognised by the navigation system.
 - There are no hazard reports, for example, accident reports.
 - There is no unusual traffic situation detected by the system, for example, people on the road.
 - A passenger car or truck driving ahead is detected.
 - The distance to the vehicle ahead is not too large or too small.

- Vehicles in the adjacent lanes are detected.
- Lane boundaries are detected.
- An adequate lane width is detected.
- The bend radii are sufficiently large.
- The vehicle is driven in the centre of the driving lane.
- The road is dry.
- The outside temperatures are not too low.
- The systems in the vehicle, for example, the Driver Attention Camera, detect that the driver can take over the driving task.
- The turn indicators are switched off.
- The calibration process of the sensors after starting the vehicle is complete.
- Aerials located in the roof are not covered, for example, by roof loads or snow residue.
- The sensors are clean and unobstructed.
- Sufficient washing fluid is available for cleaning the laser scanner, the front camera and the Reversing Assist Camera in the vehicle.
- The driver is in an upright sitting position.
- The seat belt on the driver's side is fastened.
- The driver is not wearing gloves.
- There is no protective cover on the steering wheel.
- The tyres are in a safe operating condition, for example, the tyre inflation pressure.
- The vehicle is equipped with tyres recommended by the manufacturer of the vehicle. These specially developed tyres are marked with a star on the tyre sidewall.
- With trailer tow hitch: the ball head is not swivelled out.

7.1.3 AD State Flow Diagram

The AD state-flow diagram is partly constructed based on the operational needs and the ODD of the functionalities discussed in the prior section. Nevertheless, certain transitions were not completely evident from the manual. For instance, there was ambiguity about the mode in which the vehicle resumes driving once Personal Pilot is turned off. Moreover, there was uncertainty regarding the precise procedure to switch from the Assisted Driving Mode to Assisted Driving Mode Plus. The complete AD state flow diagram is depicted in Fig. 7.5.

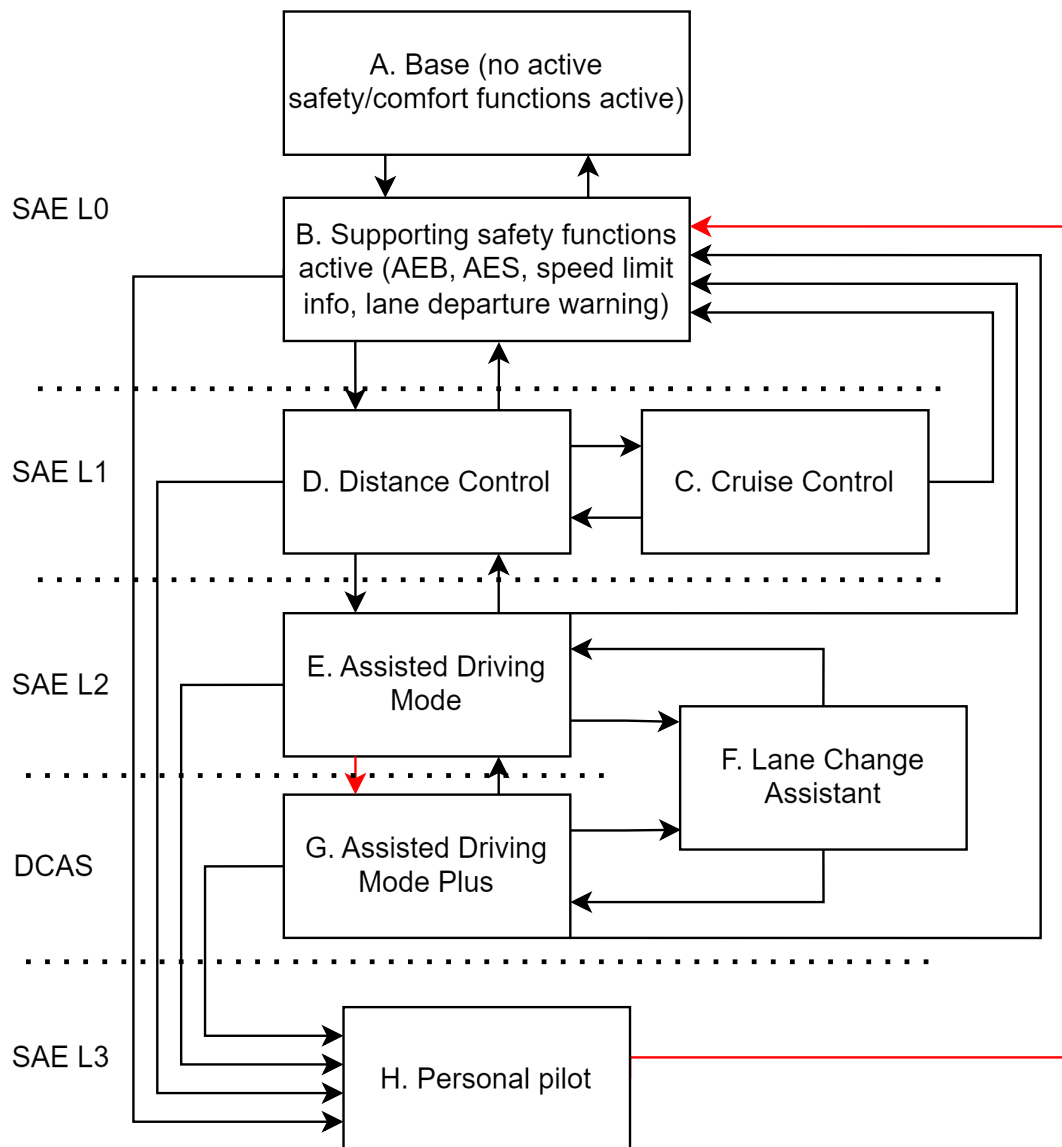


Figure 7.5: State-flow diagram for the BMW 740d derived from both the manual and supplementary experimental investigations, conducted in situations where the manual lacked clarity. The red transitions mark the ones that are studied further in the pilot experimental campaign.

It should be noted that this section of the report does not aim to provide a comprehensive examination of all potential vulnerabilities concerning mode confusion in the BMW 740d. Our goal here is to demonstrate the potential to identify vulnerabilities and evaluate them through experimental analysis. Accordingly, two state transitions in Fig. 7.5 are highlighted in red to indicate these transitions are examined further using interaction flow diagrams in the following section and in the subsequent analysis of potential functional deficiencies. The two transitions studied are related to the transition from L2 to DCAS, and from L3 to the full manual mode (i.e., L0). Based on the experimental campaign, we have found these transitions to be most relevant for causing possible mode confusion to the driver.

7.1.4 Interaction Flow Diagrams

In this section, we develop interaction-flow diagrams utilizing pre-existing knowledge regarding how the vehicle operates. Here, we assume that the driver has thoroughly reviewed the operating manual, and no additional information about the vehicle's operation was obtained.

7.1.4.1 Interaction under Test 1: Assisted Driving Mode (ADM) to Assisted Driving Mode Plus (ADM+) (L2 to DCAS)

Based on the BMW operational manual (page 267), the Assisted Driving Mode Plus is "automatically offered when Assisted Driving is active and all functional requirements for Assisted Driving Mode Plus are met". Hence, the diagram can be depicted as in Fig. 7.6, where, at first, the green steering wheel icon denoting the Assisted Driving Mode function is shown. Since the manual does not give any specific instructions on how to activate Assisted Driving Mode Plus, it is assumed that whenever the vehicle is in the appropriate driving condition, it would automatically transition, hence changing the icon as perceived by the driver.

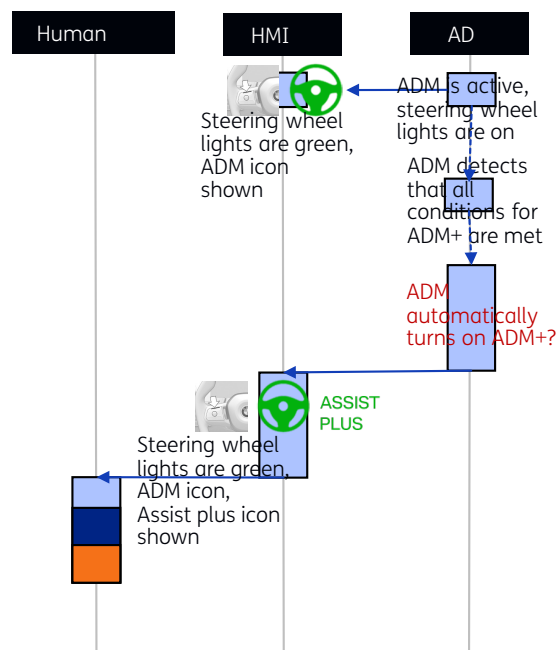


Figure 7.6: Interaction diagram from Assisted Driving Mode to Assisted Driving Mode Plus, as based on the operational manual. The different coloured blocks in the Human User part denote the different internal steps (Perception, Comprehension, Decision).

Subsequently, the interaction between the HMI and the human driver can be analyzed by breaking it down into potential functional shortcomings that might lead to mode confusion. In particular, the only interaction available to illustrate these shortcomings is the human driver's perception of the Assisted Driving Mode Plus activation. The possible functional insufficiencies in this context include:

- The icon is perceived, but incorrectly interpreted.
- The icon is perceived, but not interpreted (possibly due to cognitive distraction of the driver).

- The icon is not perceived and hence not interpreted.

7.1.4.2 Interaction under Test 2: Personal Pilot to Manual (L3 to L0)

Transitioning from Personal Pilot (PP) back to full manual mode can be done in different ways. First, there is the option for the human driver to take over, by holding the steering wheel and:

- Pressing the "I/O" button for the Personal Pilot functionality, or
- Using the throttle pedal, or
- Using the brake pedal, or
- performing active steering

The vehicle can also issue a takeover request when it finds the driving conditions unsuitable for its current function. Consequently, the driver must resume control by holding the steering wheel (both lateral and longitudinal control transitions back to the driver's responsibility).

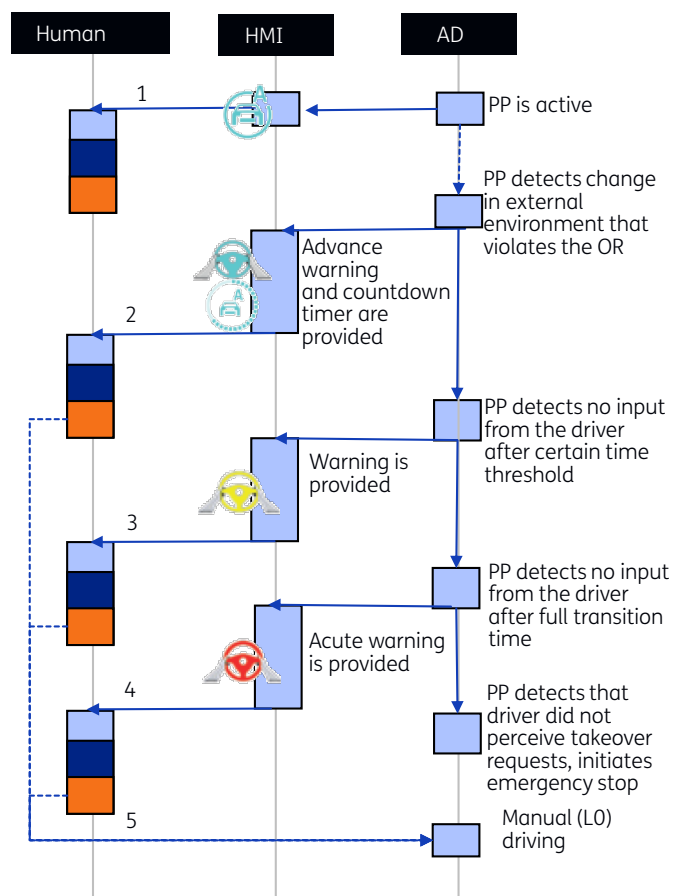


Figure 7.7: Interaction diagram from takeover from Personal Pilot to manual mode, as based on the operational manual.

Within this document, we examine the scenario where the vehicle shifts into a condition where the Personal Pilot ceases to be operational, necessitating a handover back to the driver. This handover process is illustrated in the interaction diagram in Fig. 7.7. At first, the vehicle

alerts the driver with an initial warning and a countdown indicating the need to resume control shortly. If the driver fails to respond, the situation escalates to a warning, followed by an acute warning, and ultimately results in an automatic emergency stop if the driver does not successfully regain control of the vehicle. In the end, we can identify five interactions from which we can derive the following (possible) functional insufficiencies that could lead to mode confusion (as a result of incorrect perception of system behaviour):

- **1: Personal Pilot is active notification**
 - Perceived, but incorrectly interpreted.
 - Perceived, but not interpreted (possibly due to distraction of the driver).
 - Not perceived and hence not interpreted.
- **2: Advance warning of the takeover request**
 - Perceived, but incorrectly interpreted.
 - Perceived, but not interpreted (possibly due to distraction of the driver).
 - Not perceived and hence not interpreted.
- **3: Warning of the takeover request**
 - Perceived, but incorrectly interpreted.
 - Perceived, but not interpreted (possibly due to distraction of the driver).
 - Not perceived and hence not interpreted.
- **4: Acute warning of the takeover request**
 - Perceived, but incorrectly interpreted.
 - Perceived, but not interpreted (possibly due to distraction of the driver).
 - Not perceived and hence not interpreted.
- **5: Takeover by the driver**
 - Perceived by the HMI/vehicle, but incorrectly interpreted.
 - Perceived by the HMI/vehicle, but not interpreted (e.g., not a valid input)
 - Not perceived by the HMI/vehicle, hence not interpreted.

7.2 Formulating the Test Matrix

Designing a test matrix for a vehicle with different automation modes involves more than simply verifying whether each individual feature works as intended. When the vehicle is composed of multiple automation levels with interconnected features, it is essential to adopt a rigorous, structured approach to testing the transitions between the different levels of automation, and the potential causes of mode confusion. The test matrix serves as a guide for this evaluation process.

An excerpt from the designed test matrix is shown in Fig. 7.8. The complete testing matrix and vehicle configuration are provided in Appendices B and C, respectively. The test matrix is scenario-based and transition-focused. Each row represents a unique test case, while the columns point to the structure and evaluation of each test case.

S. No.	Start State	End State	Description	Variation	Check Box	Time Log	Comments/Notes
14	Distance control		Vehicle in front comes to a complete halt. The system should comprehend if the conditions allow. But "Otherwise the driver should drive independently" --> What does this mean	1	<input checked="" type="checkbox"/>		Stood behind a truck. Complete halt. vehicle accelerated itself once lead vehicle started moving.
15				2	<input checked="" type="checkbox"/>		Stood behind a different truck. Complete halt. vehicle accelerated itself once lead vehicle started moving.
16				3	<input checked="" type="checkbox"/>		Sometimes it recognizes traffic lights and starts to accelerate itself. Sometimes, it does not.
17	Distance control		Does pressing the gas pedal give an override?		<input checked="" type="checkbox"/>		Yes, pressing the gas pedal overrides distance control.
18	Assisted Driving Mode	Lane Change Assistant	Does it suggest a lane change if we are stuck behind a slower vehicle and the next lane is free?	1 (Extra large gap to lead vehicle)	<input checked="" type="checkbox"/>	14:01	Lane change assistant requires a destination selected in the navigation (route guidance). Fast approaching a truck in the right-most lane. Lane change (LC) suggestion
19		Lane Change Assistant		2 (Large gap to lead vehicle)	<input checked="" type="checkbox"/>	14:04	Same as above
20		Lane Change Assistant		3 (Normal gap to lead vehicle)	<input checked="" type="checkbox"/>	13:57	When gap is available, decelerate in own lane first and then accelerate in the target lane

Figure 7.8: Excerpt of the test matrix

The start state refers to the initial system condition before the test is executed. The end state is the expected outcome or system condition after a certain action is taken. Description presents a narrative of what the test does and test intent. Variation specifies changes to inputs, or configuration. This allows for testing of alternative paths, making the coverage more robust. The check box is used during testing to mark pass/fail status and indicate completion. The time log records execution timestamps, and finally, the comment field is a free-text field for notes, anomaly flags, or follow-ups. This test matrix supports state-driven testing by emphasizing the transitions across different driving modes and respective outcomes.

7.3 Testing

7.3.1 Interaction under Test 1: ADM to ADM+ (L2 to DCAS)

During testing of the vehicle under test, it was found that the assumed interaction flow as depicted in Fig. 7.6 was incorrect. The revised flow based on experimental tests is shown in Fig. 7.9. The revised diagram in Fig. 7.9 opens new doors to possible insufficiencies to identify while driving (similar to the one identified in the previous section); however, next to the already identified type of mode confusion, no other insufficiencies were found in this transition. From here, it is clear how the "Assist plus ready" state on the dashboard denotes the fact that the vehicle is in the appropriate circumstances to activate Assisted Driving Mode Plus (see also Fig. 7.10). However, the transition to this mode is only done once the driver of the vehicle releases the steering wheel and therefore transitions control (but not supervision) to the vehicle (see Fig. 7.11).



Figure 7.10: Assisted Driving Mode active and Assisted Driving Mode Plus "ready".

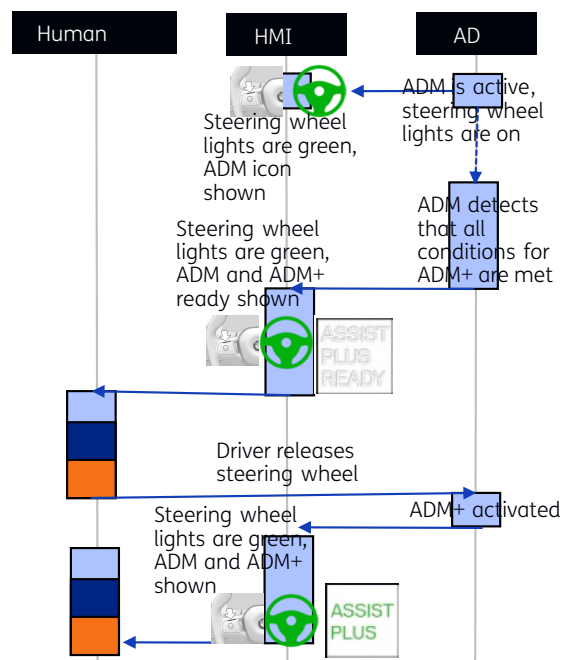


Figure 7.9: Interaction diagram from Assisted Driving Mode to Assisted Driving Mode Plus, as based on the operational manual and revised after experimental testing.

In this context, the risk of mode confusion emerges as follows. At first, there is a discrepancy between the actual vehicle operation and the user's interpretation of it based on the manual. This situation illustrates "type II" mode confusion, where the user incorrectly assumes that reading the operational manual provides sufficient insight into the system's functioning.

7.3.2 Interaction under Test 2: Personal Pilot to Manual (L3 to L0)

For this interaction, we first introduce a short anecdote from one of the test drivers during the transition:



Figure 7.11: Assisted Driving Mode Plus active because the driver released the steering wheel.



Figure 7.12: Personal Pilot activated.

Personal Pilot available! "BMW Voice: The Personal Pilot is now active".... Yeah... okay, now we are a hazard on the road... it doesn't do... what was that? I couldn't press the throttle, it would not accelerate?

For a brief period, the Personal Pilot feature was active and operational (see Fig. 7.12). However, within a few seconds, the slow-moving traffic ahead began to accelerate, rendering the environment unsuitable for the Personal Pilot to operate. Consequently, an immediate alert prompted the driver to resume control of the vehicle. Observing the departing traffic, the driver instinctively executed a full kickdown, meaning they applied full throttle to the vehicle. During this action, the driver was observed to be lightly touching (see Fig. 7.13), but not firmly gripping, the steering wheel, resulting in the vehicle not recognizing the driver's hold on the steering wheel. As a result, according to the manual, throttle, and/or brake response within L3 mode is ignored. Eventually, the driver firmly gripped the steering wheel and was able to drive off using the throttle. The possible insufficiencies, including the observations from the tests are shown below.

- **1: Personal Pilot is active notification** The Personal Pilot being active was perceived cor-



Figure 7.13: A few seconds later, Personal Pilot requests the driver to take control. The hands slightly touch the wheel, but not enough for the driver to regain full longitudinal control of the vehicle.

rectly, hence none of the aforementioned possible functional insufficiencies apply.

- **2: Advance warning of the takeover request:** The vehicle did not give an advance warning. The operational manual states that "depending on the respective situation, the takeover request is issued as a prewarning, warning or acute warning". Hence, this pre-warning was not issued by the vehicle (and therefore, not perceived, and not interpreted by the human) because the prevailing circumstances did not allow for this.
- **3: Warning of the takeover request:** *This warning was received by the driver, but incorrectly interpreted.* The driver was told to take over control of the vehicle. He believed that at that time taking over longitudinal control was the appropriate action to take given the accelerating traffic in front.
- **4: Acute warning of the takeover request:** Since the driver regained control before the acute warning phase started, this warning was not given by the vehicle.
- **5: Takeover by the driver:** The vehicle expected the steering wheel to be gripped in order to detect that the takeover was successfully initiated. The driver lightly touched, but at first did not grip the steering wheel. Even though the driver gave a throttle input, assuming control, it was ignored by the vehicle since the steering wheel was not held correctly. *Hence, input (i.e., throttle signal) was perceived by the HMI/vehicle, but not interpreted.*

From the enumeration we can conclude that for this specific example we can extract two functional insufficiencies from the human-machine interface/interaction:

1. Initially, the warning to the driver to assume control was misinterpreted. Considering the circumstances, applying the throttle was the most reasonable action to take control, as the vehicle was properly positioned in the lane, yet the gap to the vehicle ahead was growing rapidly. We expect that these conditions were specifically a trigger condition for functional insufficiency to manifest, because in other instances during our testing campaign, different drivers managed to respond effectively as there was no urgent need for throttle or brake intervention. In these scenarios, reclaiming control of the steering wheel was the most rational approach.

2. When the driver was asked to take control, he pressed the throttle and the vehicle did not respond. In theory, this is in accordance with the UNECE ALKS regulation R157 [24] Articles 6.2.5.1 and 6.2.5.2 stating that the system can be deactivated using a throttle only in combination with holding the steering wheel. In that sense, labeling this event as a functional insufficiency would label the requirement of UNECE as a possible cause of mode confusion. One can argue, however, that the system could have benefited from responding to the throttle input, e.g., with an auditory warning that the driver also needs to grip the steering wheel, hence clarifying the situation.

Given this interaction flow, with just a very short activation of the L3 functionality, two functional insufficiencies were uncovered that could lead to mode confusion due to "incorrect perception of system behavior". These functional insufficiencies manifested as a result of relatively specific conditions (activating due to slow traffic, and shortly thereafter the traffic driving off), begging the question how to exhaustively identify all possible functional insufficiencies, as our test matrix likely did not contain all the possible triggering conditions that could activate such insufficiencies. This remains an open question.

7.3.3 Incorrect interpretation of the safety implications of system functioning

A situation was encountered during the use of the vehicle's L3 conditional automation mode which relates to the incorrect interpretation of the safety implications of system functioning. Expecting L3 systems to always provide appropriate lead time to resume control, underestimating the need for immediate readiness is associated with poor understanding of the safety implications causing mode confusion. In this case, the vehicle was driving along the moderately congested German highway in the right-most lane when the operating conditions of personal pilot became valid. The traffic was moving at around 25 km/h which was just slow enough to activate the vehicle's Personal Pilot mode. The driver, initially attentive, had correctly engaged the system under appropriate conditions.

At some point, the vehicle detected an upcoming situation outside of its predefined ODD (roadworks ahead). In response, the system displayed a message in the driver's Heads-Up Display: "Personal Pilot ending soon." There was no countdown or indication of exactly when the mode would disengage — just a warning (see Fig. 7.14). For drivers who have seen this message many times before, it may not evoke urgency. Since this was the first instance, it was interpreted as a preliminary reminder rather than an imminent demand for action. In this particular case, the driver happened to be alert and watching the road, so when a distinctive audible alert was suddenly accompanied by flashing dashboard lights — signalling a Takeover Request (TOR) — they responded promptly and resumed control.



Figure 7.14: "Personal Pilot is ending soon" is shown on the HMI.

There is a growing perception that L3 systems are designed to take over most driving responsibilities under specific conditions, particularly in steady highway traffic. In this particular situation, if the driver had been distracted or browsing their phone under the comfort of assumed system capability, the driver's vigilance is understandably down. The Head-Up Display (HUD) message — "L3 ending soon" — might have gone unnoticed, especially since its wording does not convey urgency. The TOR lead time is very short, and the vehicle's manual does not clarify the system's takeover buffer, leaving it up to the driver's intuition. L3 systems may only provide five to ten seconds, perhaps less, between issuing a TOR and disengaging automation. That is not much time for a distracted person to shift their attention to the driving environment, assess situational driving context, place their hands properly, and make safe driving decisions. If the driver misses the TOR entirely — perhaps due to loud music, noise-cancelling headphones, or a lapse in focus — the vehicle might perform a Minimal Risk Manoeuvre (MRM), such as slowing to a stop within its lane or attempting to move to the shoulder lane. While technically compliant with regulations, this manoeuvre can be hazardous in real-world traffic, particularly on busy highways where a slow-moving or stationary vehicle in an active lane can be rear-ended.

The main issue lies in the ambiguous communication of system limits and expectations. The indication on the HUD "Personal Pilot: ending soon" is unquantified, and can be easily missed or neglected. Without a countdown or clear indication of how long "soon" really means, drivers tend to project their own assumptions — perhaps expecting 10-30 seconds of grace time or a gradual slowdown process. Drivers can assume that the vehicle is capable of a fall-

back manoeuvre if they do not respond, without realizing how limited or unsafe that fallback might be depending on traffic, road layout, and surrounding vehicles. There are many reasons for a TOR to be issued and not all of them are observable for the driver: a TOR might be triggered by the system's internal thresholds being crossed — say, a degraded sensor or GPS signal — not necessarily by road conditions the driver can easily perceive. So the moment of transition can feel arbitrary and abrupt. Worse, it might occur at crucial locations: while passing an on-ramp with merging traffic, or just before an unexpected lane closure. If the driver's response is even slightly delayed, the system might time out and execute a MRM in a live traffic environment.

Therefore, one major safety implication, stems from the misinterpretation that L3 automation (Personal Pilot in this case) grants ample, predictable time for re-engagement. This false sense of security is fuelled by factors such as system designs or unclear language without fully explaining users on its limitations.

8 Conclusion

8.1 Summary and conclusions of the report

The scope of the assignment from the Ministry of Infrastructure and Water Management in The Netherlands has been to investigate the possibility of using the SOTIF approach to evaluate the quality of interaction processes between the vehicle and the user, in the context of advanced driver assistance systems and automated driving systems. The primary concern is that a lack of quality in these interaction processes could result in hazardous situations. In the scope of this report, the lack of quality has mainly been attributed to its ability to cause mode confusion, i.e. the driver misunderstands or is unaware of the system's current operational mode and capabilities. Three different factors causing mode confusion have been identified from the literature and elaborated further in this report.

Subsequently, a summary was given on the different types of safety-constructs currently existing in the automated driving domain. First, an overview of functional safety was given, although its applicability to assess human-machine interaction is relatively restricted, since it mainly covers the probability of faults in the E/E system. The SOTIF line of thinking was identified to fit better with the notion of mode confusion, since the inability of an HMI to work well together with a human driver fits well with the notion of functional insufficiency (Def. 3).

As a result of the identified synergy between SOTIF and the context of mode confusion in HMI interaction, a methodology has been proposed that aims to extract possible functional insufficiencies that could lead to mode confusion, from the possible interactions that occur when a vehicle transitions from one automation mode to another. The methodology has been put into practice by testing it experimentally with an SAE L3 and DCAS equipped vehicle. Here, it is seen that the systematically identified (possible) functional insufficiencies are supporting the targeted testing and extraction of the functional insufficiencies that were, in fact, applicable, and could lead to a form of mode confusion.

8.2 Discussion

It is shown in this report that it is possible to apply the SOTIF line-of-thinking to identifying possible factors contributing to mode confusion. In this section, we discuss possible shortcomings when using this approach, possible topics for future research, and the applicability of the proposed approach for assessing parties, to determine the quality of the HMI.

8.2.1 Mapping of the methodology on SOTIF workflow

The process for assessing and improving the Safety of the Intended Functionality is depicted in Fig. 8.1. The SOTIF process starts with the definition of the specification and design, which can be updated through one or several iterations of the SOTIF activities by a system designer. In Clause 6 of the norm, the potential hazardous behaviours of the intended functionality are tested with a hazard identification and risk evaluation. Here, risk is assessed (using risk acceptance criteria), and it is determined whether or not hazardous events need to be considered (e.g., through additional design measures). Note that in this work, we assume that the "mode confusion" is the primary hazardous event of interest. Hence, no downstream analy-

sis has been done on how mode confusion possibly propagates toward risk of harm. In that sense, the term mode confusion refers to a large group of hazardous events, each of which might pose a different risk of harm.

Clause 7 identifies the possible root causes for the hazardous behaviour of the intended functionality. In addition, it evaluates whether the risk resulting from possible functional insufficiencies and triggering conditions thereof is reasonable. This report, in that sense, primarily aligns with the workflow from Clause 7, i.e., proposing a set of possible triggering conditions (i.e., the state transitions between different ADS) and extracting possible functional insufficiencies that could occur from that. Given that all the interactions of a human driver with the vehicle can be mapped through interaction diagrams, our method therefore offers to exhaustively identify the possible functional insufficiencies that could occur from that and could lead to mode confusion. However, it should be noted that here no risk calculations have been done of the downstream effect of functional insufficiencies manifesting. Having such a risk analysis would allow one to assess which functional insufficiencies would require redesign of the system due to an unacceptable risk of harm (mainly related to Clause 8).

Clauses 9 to 11 primarily concern the verification and validation of the design, being out of scope of the problem setting in which this work is located. Finally, Clause 12 relates to the assessment of residual risk. Clause 13 is set up to define a field monitoring process to ensure the SOTIF during the operational phase.

In summary, looking at Fig. 8.1, it can be concluded that the results of this report mainly relate to Clause 7, that is, identifying the possible triggering conditions and functional insufficiencies. Calculation of risk as a result of, e.g., mode-confusion would therefore need to be assessed to fully assess the SOTIF.

8.2.2 Applicability of the SOTIF method to assess human-machine interaction

Several shortcomings and recommendations for future research are discussed in the sections below.

8.2.2.1 Identification of all possible interactions

In this study, we examined the state transitions between specific AD functions to identify potential user-HMI interactions that might initiate mode confusion. Each interaction was traced from the moment the user or vehicle begins the state transition to the point where the transition occurs and the driver is informed. However, it is possible that within certain functions, interactions occur that could form a triggering condition towards mode confusion. Consequently, solely mapping the interactions from state transitions might not fully capture all interactions that could cause mode confusion. Future research seeks to determine how to identify all interactions pertinent to this analysis. This investigation should produce a method or a set of criteria that applicants, such as OEMs, can reasonably use to advance vehicle safety evaluation.

8.2.2.2 The effect of mental models and prior knowledge

This study operates under certain presumptions regarding the user's background in handling the vehicle's HMI. Specifically, within the experimental testing framework, it is assumed that the user relies solely on the manual in relation to the exact functioning of the vehicle. This raises the initial question of whether it is reasonable to expect a user to thoroughly read such

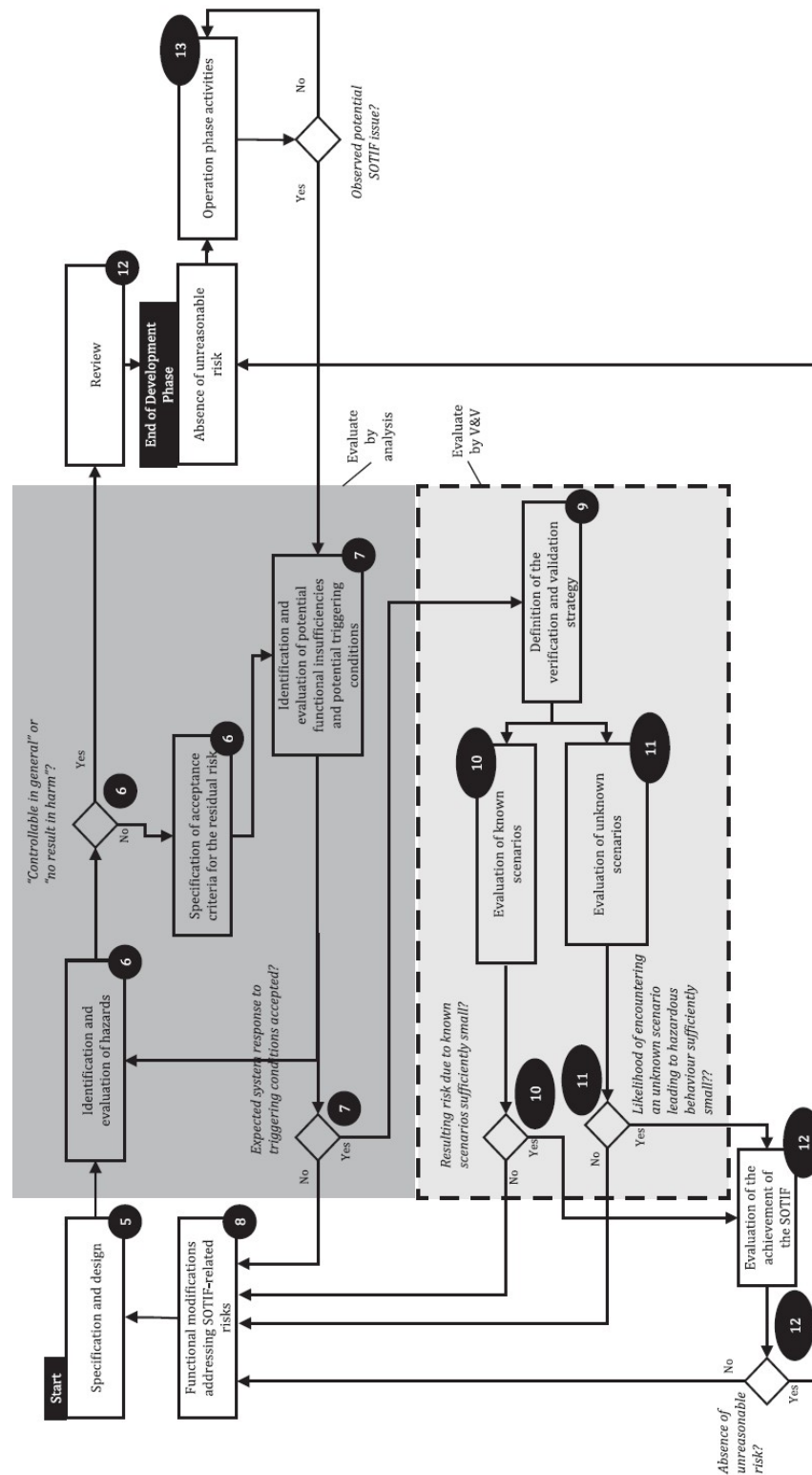


Figure 8.1: SOTIF system design procedure [1].

a comprehensive manual. In addition, memory (remembering the details of the manual, but also having earlier exposure to other such systems) plays a crucial role here. A driver with prior exposure to L3 and DCAS vehicles may have certain assumptions about the operation of a new vehicle (e.g. with another configuration or from a different OEM) that differ from its actual functionality. Another area for future research could involve examining various mental models influenced by the user's experience and prior understanding, as these factors might contribute to the underlying causes of mode confusion.

8.2.2.3 Extension beyond mode confusion

This report utilizes mode confusion as a case study to examine whether the SOTIF-line-of-thinking can be applied to pinpoint potential shortcomings in human-machine interactions. Nonetheless, mode confusion is just one of several contributors to unsafe scenarios stemming from human-machine interactions. Another factor that might lead to such hazardous situations is workload, encompassing the mental, physical, and perceptual demands imposed on the driver while interacting with the vehicle's systems. With slight adjustments to the methodology, it is anticipated that other metrics affecting safety through HMI interactions can also be evaluated. Particularly, it is expected that the steps going from possible triggering conditions to possible functional insufficiencies (in Figure 6.1) requires modifications to accurately represent the various conditions impacting the assessed metric. Future work could explore expanding this methodology to incorporate alternative methods.

8.2.3 Applicability of the proposed approach for assessing parties

In the end, it is up to an applicant to prove the safety of the AD system and up to the assessor to study the proof of the applicant and decide whether the system complies with the applicable regulations and avoids an unreasonable risk of harm. In the scope of assessing the quality of the interaction between the vehicle user and HMI, it is believed that this approach is a promising direction to use as a complementary method, in addition to checking the vehicle's compliance with existing rules and regulations. In order to be able to use this framework as an assessor, the following aspects need to be taken into account:

- **Experience of the assessor during testing:** To test the hypothesis of whether mode confusion could occur, care must be taken with the bias and experience of the assessor. Such aspects could affect the integrity of the analysis since, as mentioned earlier, prior knowledge and memory play a large role in the type of mode confusion that could occur. An approach for using this as an assessor could be to ask the applicant for ir-refutable proof that the identified "possible" functional insufficiencies do not occur. As a result, experiments by the assessing party may not be necessary.
- **Future work recommendations:** As discussed earlier, there are various areas for further investigation. These areas consist of broadening mode-confusion metrics to encompass additional metrics, exploring the impact of mental models that involve prior knowledge and experience, and elaborating on the interactions where functional insufficiencies relative to specific metrics can be identified.

8.2.4 Link to the SWOV work on mode confusion

As noted in Section 3.2, a recent study, conducted by the Institute for Road Safety Research (SWOV), has also sought to investigate the phenomenon of mode confusion using a distinct methodological approach that complements and enriches our findings.

SWOV approached mode confusion by first conducting a conceptual analysis to establish its theoretical underpinnings and relevance in the context of increasing vehicular automation. They classified mode confusion into general mode confusion and transient mode confusion. General mode confusion refers to cases where the system's user lacks understanding on how the system works and what the user is supposed to do while transient mode confusion refers to cases where the user is unaware if a particular system is activated or deactivated. Based on certain criteria, they selected two commercially available vehicles with multiple levels of automation and examined publicly available documentation, including user manuals and owner discussions on online forums, to identify potential triggers of mode confusion. Their experimental methodology centered around a virtual reality (VR) based driving simulator environment which used mock-ups to create triggers of mode confusion identified from the manuals and online forums for the two vehicles. A freeze-probe technique was employed as participants were engaged in the simulations — temporarily halting the scenario to query participants about their understanding of the system's mode at that moment. This approach allowed for controlled measurement of mode confusion and revealed promising results in the applicability of freeze probes as a tool to measure mode confusion.

In contrast, TNO opted for a field-driven experiment to implement the SOTIF methodology to identify potential functional insufficiencies that might act as triggers for mode confusion. After a similar preliminary examination of the vehicle owner's manual, we focused on identifying specific functional insufficiencies — features whose design or presentation might inadvertently cause a misunderstanding of the vehicle's automation status. Instead of simulating conditions, we deployed a test vehicle (in this case, the BMW 740d) with multiple automation modes in actual highway traffic conditions. We conducted drive tests and made real-time annotations in the test matrix, capturing instances of potential confusion as they arose during naturalistic driving. This approach facilitated the observation of driver responses to actual traffic environment stimuli and interface behaviours, producing data with direct implications for system design and interface optimization.

While both studies shared a common goal — understanding and mitigating mode confusion — their divergence in method illustrates the complexity of the phenomenon under investigation. The classification of mode confusion by SWOV can be mapped to the types of mode confusion identified in this study. General mode confusion is covered by the causes - incorrect knowledge of system functioning and incorrect interpretation of the safety implications of system functioning while transient mode confusion is related to the incorrect perception of system behaviour. SWOV's VR-based driving simulator approach offers tightly controlled conditions and systematic probing, making it ideal for isolating test variables as well as assessment techniques like the freeze probe method. Meanwhile, the in-situ testing in this study provides context-based insights into how mode confusion manifests in everyday naturalistic driving, where unexpected events and environmental complexity play significant roles. The current approach also allows us to utilise an existing OEM's system, and conduct a safety assessment which can be a challenging task in a simulator environment.

It is worthwhile to highlight how TNO's real-world validation of functional insufficiencies extends the findings of SWOV's more controlled exploratory framework. By operating in naturalistic conditions, this study attempts to bridge the gap between simulation and application. Collectively, the complementary nature of these investigations shows the importance of a hybrid framework. The simulation-driven freeze probe approach, as performed by SWOV, enables precision and repeatability, while real-world experimentation, as undertaken in this project, ensures that conclusions remain grounded to practical realities. Together, these approaches pave the way for designing more intuitive and unambiguous HMIs and ultimately reducing the risk of mode confusion in ADS.

References

- [1] ISO 21448:2022 Road vehicles - Safety of the intended functionality. 2022. URL: <https://www.iso.org/standard/77490.html> (visited on 03/29/2023).
- [2] Maartje De Goede et al. *Who is driving? A study into mode confusion*. 2025. URL: <https://swov.nl/sites/default/files/bestanden/downloads/R-2025-02.pdf> (visited on 07/16/2025).
- [3] *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*. 2021. URL: https://www.sae.org/standards/content/j3016_202104/.
- [4] Katja Blömacher, Gerhard Nöcker, and Markus Huff. "The evolution of mental models in relation to initial information while driving automated". In: *Transportation Research Part F: Traffic Psychology and Behaviour* 68 (Jan. 2020), pp. 198–217. ISSN: 1369-8478. DOI: 10.1016/j.trf.2019.11.003. URL: <https://www.sciencedirect.com/science/article/pii/S1369847819302086> (visited on 03/20/2025).
- [5] Yasemin Dönmez Özkan et al. "Mode Awareness Interfaces in Automated Vehicles, Robotics, and Aviation: A Literature Review". en. In: *13th International Conference on Automotive User Interfaces and Interactive Vehicular Applications*. Leeds United Kingdom: ACM, Sept. 2021, pp. 147–158. DOI: 10.1145/3409118.3475125. URL: <https://dl.acm.org/doi/10.1145/3409118.3475125> (visited on 07/17/2025).
- [6] Jan Bredereke and Axel Lankenau. "A Rigorous View of Mode Confusion". en. In: *Computer Safety, Reliability and Security*. Ed. by Gerhard Goos et al. Vol. 2434. Series Title: Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, pp. 19–31. ISBN: 978-3-540-44157-1 978-3-540-45732-9. DOI: 10.1007/3-540-45732-1_4. URL: http://link.springer.com/10.1007/3-540-45732-1_4 (visited on 03/06/2025).
- [7] Andrew Monk. "Mode errors: a user-centred analysis and some preventative measures using keying-contingent sound". In: *International Journal of Man-Machine Studies* 24.4 (Apr. 1986), pp. 313–327. ISSN: 0020-7373. DOI: 10.1016/S0020-7373(86)80049-9. URL: <https://www.sciencedirect.com/science/article/pii/S0020737386800499> (visited on 05/23/2025).
- [8] Shabnam Haghzare, Jennifer L. Campos, and Alex Mihailidis. "Classifying Older Drivers' Gaze Behaviour during Automated versus Non-Automated Driving: A Preliminary Step towards Detecting Mode Confusion". en. In: *International Journal of Human-Computer Interaction* 40.2 (Jan. 2024), pp. 241–254. ISSN: 1044-7318, 1532-7590. DOI: 10.1080/10447318.2022.2112933. URL: <https://www.tandfonline.com/doi/full/10.1080/10447318.2022.2112933> (visited on 02/14/2025).
- [9] Christina Kurpiers et al. "Mode Awareness and Automated Driving—What Is It and How Can It Be Measured?" en. In: *Information* 11.5 (May 2020). Number: 5 Publisher: Multidisciplinary Digital Publishing Institute, p. 277. ISSN: 2078-2489. DOI: 10.3390/info11050277. URL: <https://www.mdpi.com/2078-2489/11/5/277> (visited on 02/14/2025).
- [10] Frederik Naujoks et al. "Driving performance at lateral system limits during partially automated driving". In: *Accident Analysis & Prevention* 108 (Nov. 2017), pp. 147–162. ISSN: 0001-4575. DOI: 10.1016/j.aap.2017.08.027. URL: <https://www.sciencedirect.com/science/article/pii/S000145751730307X> (visited on 03/20/2025).

- [11] Hwisoo Eom and Sang Hun Lee. “Mode confusion of human-machine interfaces for automated vehicles”. en. In: *Journal of Computational Design and Engineering* 9.5 (Nov. 2022), pp. 1995–2009. ISSN: 2288-5048. DOI: 10 . 1093 / jcde / qwac088. URL: <https://academic.oup.com/jcde/article/9/5/1995/6679564> (visited on 03/06/2025).
- [12] Trent W. Victor et al. “Automation Expectation Mismatch: Incorrect Prediction Despite Eyes on Threat and Hands on Wheel”. In: *Human Factors* 60.8 (Dec. 2018). Publisher: SAGE Publications Inc, pp. 1095–1116. ISSN: 0018-7208. DOI: 10.1177/0018720818788164. URL: <https://doi.org/10.1177/0018720818788164> (visited on 03/20/2025).
- [13] Natasha Merat et al. “Highly Automated Driving, Secondary Task Performance, and Driver State”. In: *Human Factors* 54.5 (Oct. 2012). Publisher: SAGE Publications Inc, pp. 762–771. ISSN: 0018-7208. DOI: 10 . 1177 / 0018720812442087. URL: <https://doi.org/10.1177/0018720812442087> (visited on 07/17/2025).
- [14] Fredrik Warg et al. “Towards Safety Analysis of Interactions Between Human Users and Automated Driving Systems”. In: *10th European Congress on Embedded Real Time Software and Systems (ERTS 2020)*. TOULOUSE, France, Jan. 2020. URL: <https://hal.science/hal-02441382> (visited on 02/14/2025).
- [15] Christian P. Janssen et al. “A Hidden Markov Framework to Capture Human-Machine Interaction in Automated Vehicles”. In: *International Journal of Human-Computer Interaction* 35.11 (July 2019). Publisher: Taylor & Francis, pp. 947–955. ISSN: 1044-7318. DOI: 10 . 1080 / 10447318 . 2018 . 1561789. URL: <https://www.tandfonline.com/doi/full/10.1080/10447318.2018.1561789> (visited on 02/14/2025).
- [16] Zhenji Lu and Joost C.F. De Winter. “A Review and Framework of Control Authority Transitions in Automated Driving”. en. In: *Procedia Manufacturing* 3 (2015), pp. 2510–2517. ISSN: 23519789. DOI: 10 . 1016 / j . promfg . 2015 . 07 . 513. URL: <https://linkinghub.elsevier.com/retrieve/pii/S2351978915005144> (visited on 03/20/2025).
- [17] Martin Krampell, Ignacio Solís-Marcos, and Magnus Hjälm Dahl. “Driving automation state-of-mind: Using training to instigate rapid mental model development”. In: *Applied Ergonomics* 83 (Feb. 2020), p. 102986. ISSN: 0003-6870. DOI: 10.1016/j.apergo.2019.102986. URL: <https://www.sciencedirect.com/science/article/pii/S0003687018303211> (visited on 07/17/2025).
- [18] Mica R. Endsley. “Autonomous Driving Systems: A Preliminary Naturalistic Study of the Tesla Model S”. In: *Journal of Cognitive Engineering and Decision Making* 11.3 (Sept. 2017). Publisher: SAGE Publications, pp. 225–238. ISSN: 1555-3434. DOI: 10 . 1177 / 1555343417695197. URL: <https://doi.org/10.1177/1555343417695197> (visited on 02/14/2025).
- [19] Victoria A. Banks et al. “Is partially automated driving a bad idea? Observations from an on-road study”. en. In: *Applied Ergonomics* 68 (Apr. 2018), pp. 138–145. ISSN: 00036870. DOI: 10 . 1016 / j . apergo . 2017 . 11 . 010. URL: <https://linkinghub.elsevier.com/retrieve/pii/S0003687017302594> (visited on 02/14/2025).
- [20] Kyle M. Wilson et al. “Driver trust & mode confusion in an on-road study of level-2 automated vehicle technology”. In: *Safety Science* 130 (Oct. 2020), p. 104845. ISSN: 0925-7535. DOI: 10 . 1016 / j . ssci . 2020 . 104845. URL: <https://www.sciencedirect.com/science/article/pii/S0925753520302423> (visited on 02/14/2025).
- [21] Jan Erik Stellet et al. “Formalisation and algorithmic approach to the automated driving validation problem”. In: *2019 IEEE Intelligent Vehicles Symposium (IV)*. ISSN: 2642-7214. June 2019, pp. 45–51. DOI: 10 . 1109 / IVS . 2019 . 8813894. URL: <https://ieeexplore.ieee.org/document/8813894> (visited on 02/11/2025).
- [22] *ISO 26262-1:2018 Road vehicles - Functional safety*. 2018. URL: <https://www.iso.org/standard/68383.html> (visited on 03/29/2023).

- [23] *DRIVE PILOT*. nl-NL. URL: <https://www.mercedes-benz.nl/passengercars/technology/drive-pilot.html> (visited on 08/04/2025).
- [24] *UN Regulation No. 157 - Automated Lane Keeping Systems (ALKS)* | UNECE. 2021. URL: <https://unece.org/transport/documents/2021/03/standards/un-regulation-no-157-automated-lane-keeping-systems-alks> (visited on 02/08/2024).
- [25] *UN Regulation No. 171 - Driver Control Assistance Systems (DCAS)* | UNECE. 2024. URL: https://unece.org/sites/default/files/2024-02/ECE_TRANS_WP.29_2024_37e.pdf (visited on 02/08/2024).
- [26] *Owner's Handbook, BMW 7 Series, Online Edition for Part. no 01405B37439*. 2024.

Appendix A

BMW Manual Excerpt

◀ An arrow symbol next to the Check Control message indicates whether the Check Control message can be hidden.




To hide Check Control messages, tilt the knurled wheel on the steering wheel to the left.

Displaying saved Check Control messages

Additional information, for example the cause of the fault and any action required, can be called up via Check Control.

It is possible to select additional assistance depending on the Check Control message.

1.  Apps menu
2. "Vehicle"
3. "Vehicle status"
4. "Check Control"
5. Select the required text message.

Display

A Check Control message is displayed on the instrument cluster as a text message with icon.

With urgent messages, additional instructions will be displayed automatically on the control display.

If a number of malfunctions have occurred at the same time, the messages are displayed in succession.

Certain messages displayed when driving are displayed again when the drive-ready state is switched off.



Icons on the instrument cluster indicate an active or saved Check Control message.

Indicator lights and warning lights

Principle

The indicator lights and warning lights on the instrument cluster show the status of some vehicle functions. The indicator lights and warning lights indicate faults in monitored systems.

General

The indicator/warning lights may illuminate in various combinations and colours.

When switching on drive-ready state, the functionality of some lights is checked and they illuminate briefly.

Red lights

Seat belt warning



Seat belt is not buckled.

For further information:

Seat belt warning, see page [125](#).

Airbag system



Warning light is illuminated briefly; this indicates that the entire airbag system and seat belt tensioners are operational when the vehicle is switched on.

Warning light does not illuminate or illuminates continuously: The airbag system or belt tensioners may not be functioning. Have the vehicle checked immediately by an authorised Service Partner or another qualified Service Partner or a specialist workshop.

For further information:

Airbags, see page [198](#).

CONTROLS

Displays

Parking brake



The parking brake is engaged.
For further information:
Parking brake, see page 157.

Brake system



The brake pads are worn or there is a fault in the brake system.
The braking force assistance may be not functional. A higher pedal force may be required during the braking process.
Have the vehicle checked immediately by an authorised Service Partner or another qualified Service Partner or a specialist workshop.

Emergency Stop Assistant



The Emergency Stop Assistant is triggered.
For further information:
Emergency Stop Assistant, see page 227.

Risk of collision



Warning light is illuminated or flashes in conjunction with an acoustic signal if a collision is imminent.
For further information:
Front collision warning, see page 204.

Pedestrian warning



Warning light illuminates: risk of collision with a person, e.g. pedestrian or cyclist, has been detected. Increased awareness is required.
Warning light flashes and signal sounds: risk of impending collision with a person, e.g. pedestrian or cyclist, has been detected. Immediately start braking or an avoidance manoeuvre.
For further information:

Warning function for pedestrians, see page 210.

Collision Warning



Warning light illuminates: risk of collision, e.g. with a vehicle, has been detected. Increased awareness is required.

Warning light flashes and signal sounds: risk of impending collision with a vehicle has been detected. Immediately start braking or an avoidance manoeuvre.

For further information:

Warning function in rear collision situations, see page 207.

Crossroads Warning: vehicle detected from the right



Warning light illuminates: risk of collision with a vehicle crossing from the right has been detected. Increased awareness is required.

Warning light flashes and signal sounds: risk of impending collision with a crossing vehicle has been detected. Immediately start braking or an avoidance manoeuvre.

For further information:

Warning function at road junctions, see page 211.

Crossroads Warning: vehicle detected from left



Warning light illuminates: risk of collision with a vehicle crossing from the left has been detected. Increased awareness is required.

Warning light flashes and signal sounds: risk of impending collision with a crossing vehicle has been detected. Immediately start braking or an avoidance manoeuvre.

For further information:

Warning function at road junctions, see page 211.

Distance Control



Warning light flashes and an acoustic signal sounds: brake and perform avoidance manoeuvre, if necessary.

For further information:

Distance Control, see page 252.

Assisted Driving Mode



The warning light flashes and a signal sounds:

The system is switching off or an interruption of the system is imminent.

The warning light is illuminated and a signal sounds:

The driver's line of vision is not directed towards the traffic situation. A system interruption is imminent. The system reduces the speed to a standstill if applicable. The system may possibly not perform any supporting steering wheel movements.

For further information:

Assisted Driving Mode, see page 259.

Assisted Driving Mode: hands not on the steering wheel



The warning light is illuminated and a signal sounds:

Hands are not gripping the steering wheel or, depending on vehicle equipment and national-market version, the driver is not looking toward traffic. A system interruption is imminent.

The system reduces the speed to a standstill if applicable.

The system may possibly not perform any supporting steering wheel movements.

Immediately place both hands on the steering wheel and pay attention to the traffic situation.

For further information:

Assisted Driving Mode, see page 259.

Personal Pilot



The warning light is illuminated and a signal sounds:

The driver must take over the driving task immediately.

Immediately grasp the steering wheel with your hands and take over the driving task yourself.

For further information:

Personal Pilot, see page 275.

Personal Pilot



The emergency stop function of Personal Pilot has been triggered. The vehicle brakes and stops in the current lane.

For further information:

Personal Pilot, see page 275.

Yellow lights

Anti-lock Braking System



There is a malfunction or the system is faulty. The Anti-lock Braking System (ABS) is not available.

Ease of steering may be restricted during full braking.

Have the vehicle checked immediately by an authorised Service Partner or another qualified Service Partner or a specialist workshop.

For further information:

Anti-lock Braking System (ABS), see page 238.

CONTROLS

Displays

Brake system



The brake pads are worn or there is a fault in the brake system.

Have the vehicle checked by an authorised Service Partner or another qualified Service Partner or a specialist workshop.

Assisted Driving Mode



The warning light is illuminated and a signal sounds: a system interruption is imminent.

The warning light flashes: a lane boundary has been crossed.

For further information:

Assisted Driving Mode, see page 259.

Assisted Driving Mode: hands not on the steering wheel



Hands are not holding the steering wheel. System remains active.

Grab the steering wheel with your hands.

For further information:

Assisted Driving Mode, see page 259.

Personal Pilot



It is imperative for the driver to take over the driving task.

Hold the steering wheel with your hands and take over the driving task yourself.

For further information:

Personal Pilot, see page 275.

Front collision warning restricted or failed



Depending on the equipment and national-market version: functional limitation detected, for example due to system limits of the camera or system failure. It is

possible to continue driving. Where applicable, observe the information from Check Control messages.

For further information:

Front collision warning, see page 204.

Dynamic Stability Control



Warning light pulsates: Dynamic Stability Control is regulating the drive and brake forces. The vehicle is being stabilised. Reduce speed and adjust the driving style to the road conditions.

Warning light is illuminated: Dynamic Stability Control has failed or is initialising. The driving stabilisation is restricted or has failed.

If the warning light is continuously illuminated, have the vehicle checked immediately by an authorised Service Partner or another qualified Service Partner or a specialist workshop.

For further information:

Dynamic Stability Control, see page 238.

Dynamic Stability Control deactivated or increased driving dynamics activated



Dynamic Stability Control is deactivated or increased driving dynamics is activated.

For further information:

- Dynamic Stability Control, see page 238.
- Setting for increased driving dynamics, see page 239.

Drive-off support



The drive-off support is activated.

For further information:

Drive-off support, see page 240.

Flat tyre monitor



The warning light illuminates: flat tyre or a tyre pressure loss has been detected.

Reduce your speed and carefully stop the vehicle. Avoid heavy braking and sudden steering manoeuvres.

For further information:

Flat tyre monitor, see page [390](#).

Tyre Pressure Monitor



The warning light illuminates: flat tyre or a tyre pressure loss has been detected. Note the information in the Check Control message.

Warning light flashes and is then illuminated continuously: the system is unable to detect flat tyres or tyre pressure losses.

- ▶ Fault due to systems or devices with the same radio frequency: the system is automatically reactivated upon leaving the field of interference.
- ▶ For tyres with special approval: the Tyre Pressure Monitor was unable to complete the reset. Reset the system again.
- ▶ Wheel without wheel electronics is fitted: if necessary have it checked by an authorised Service Partner or another qualified Service Partner or a specialist workshop.
- ▶ Malfunction: have the system checked by an authorised Service Partner or another qualified Service Partner or a specialist workshop.

For further information:

Tyre Pressure Monitor, see page [384](#).

Steering system



The steering system may be faulty. Have the system checked by an authorised Service Partner or another

qualified Service Partner or a specialist workshop.

For further information:

Integral Active Steering, see page [241](#).

Exhaust emissions



- ▶ When the warning light flashes:
There is an engine fault which could damage the catalytic converter.
Have the vehicle checked immediately.

- ▶ When warning light illuminates:
deterioration of the exhaust gas quality.
Have the vehicle checked as soon as possible.

Have the vehicle checked by an authorised Service Partner or another qualified Service Partner or a specialist workshop.

Lane Departure Warning



Depending on equipment and national-market version:

Warning light is illuminated: functional limitation detected, for example, due to low sun or system failure. It is possible to continue driving. Where applicable, observe the information from Check Control messages.

Warning light flashes: a warning is issued actively. The system does not carry out any steering interventions.

For further information:

Lane Departure Warning, see page [215](#).

Rear fog light



Rear fog light is switched on.

For further information:

Rear fog light, see page [191](#).



CONTROLS

Displays

Acoustic pedestrian protection



Acoustic protection for pedestrians has failed. Increased caution when manoeuvring.

In case of repeated malfunctions, have the system checked by an authorised Service Partner or another qualified Service Partner or a specialist workshop.

For further information:

Acoustic protection for pedestrians, see page [146](#)

Green lights

Turn indicators



The turn indicator is switched on. If the indicator light flashes more rapidly than usual, a turn indicator bulb has failed.

For further information:

Turn indicators, see page [184](#).

Side lights



The side lights are switched on.

For further information:

Side light, low-beam headlight, see page [187](#).

Low-beam headlight



The low-beam headlight is switched on.

For further information:

Side light, low-beam headlight, see page [187](#).

High-beam Assistant



Low-beam headlight is switched on and the High-beam Assistant is activated.

The high-beam headlight is switched on and off automatically according to traffic situation.

For further information:

High-beam Assistant, see page [185](#).

Lane Departure Warning



Depending on equipment and national-market version:

Indicator light flashes: the system actively issues a warning. If necessary, the system performs a steering intervention.

For further information:

Lane Departure Warning, see page [215](#).

Automatic Hold: vehicle is held automatically



Automatic Hold is ready to operate. The vehicle is held automatically when at a standstill.

For further information:

Automatic Hold, see page [159](#).

Automatic Hold: vehicle secured against rolling away



The vehicle is automatically secured against rolling away after stopping.

For further information:

Automatic Hold, see page [159](#).

Manual Speed Limiter



Indicator light illuminates: the system is switched on.

Indicator light flashes: set speed limit is exceeded.

For further information:

Manual Speed Limiter, see page [248](#).

Cruise Control



The system is active.
For further information:
Cruise Control, see page [250](#).

Distance Control



Indicator light illuminates: system has detected a vehicle ahead. The vehicle symbol goes out if no vehicle in front is detected.

Indicator light flashing: vehicle in front has driven off.

For further information:
Distance Control, see page [252](#).

Speed Limit Assist



The detected speed limit can be applied with the SET button. As soon as the speed limit has been adopted, a green tick is displayed.

For further information:
Speed Limit Assist, see page [268](#).

Assisted Driving Mode



The system is helping the driver keep the vehicle in the driving lane.

For further information:
Assisted Driving Mode, see page [259](#).

Lane Change Assistant: lane change in progress



Green arrow symbol for lane-changing: the system is carrying out a lane change.

For further information:
Lane Change Assistant, see page [264](#).

Lane Change Assistant Lane: lane change not possible



Grey line for lane boundary on the appropriate side: the system has detected the lane change request. Lane change not currently possible.

For further information:
Lane Change Assistant, see page [264](#).

Assisted Driving Mode Plus



The system is active.
For further information:
Assisted Driving Mode Plus, see page [265](#).

Turquoise lights

Personal Pilot



The Personal Pilot is active and has taken over the driving task.

For further information:
Personal Pilot, see page [275](#).

Personal Pilot



It is necessary for the driver to take over the driving task.

Hold the steering wheel with your hands and take over the driving task yourself.

For further information:
Personal Pilot, see page [275](#).

Personal Pilot



The display shows the remaining time within which the driver must take over the driving task.

For further information:
Personal Pilot, see page [275](#).



CONTROLS

Displays

Blue lights

High-beam headlight



The high-beam headlight has been switched on.

For further information:

High-beam headlight, see page [184](#).

High-beam Assistant



High-beam headlight was switched on by High-beam Assistant.

For further information:

High-beam Assistant, see page [185](#).

Grey lights

Manual Speed Limiter



The system is interrupted.

For further information:

Manual Speed Limiter, see page [248](#).

Distance Control



Indicator light flashes: the requirements for operation of the system are no longer being met. The system has been deactivated but will continue to brake until you actively take over by depressing the brake or accelerator pedal.

For further information:

Distance Control, see page [252](#).

Assisted Driving Mode



System is on standby and does not make any steering wheel movement.

The system activates automatically when all operating requirements are met.

For further information:

Assisted Driving Mode, see page [259](#).

Assisted Driving Mode Plus



The system is interrupted and activates automatically as soon as all functional requirements are met.

For further information:

Assisted Driving Mode Plus, see page [265](#).

Front collision warning



Depending on vehicle equipment and national-market version: the system is switched off.

For further information:

Front collision warning, see page [204](#).

Lane Departure Warning



Depending on equipment and national-market version:

Warning light is illuminated: the system is switched off or automatically deactivated, for example, because DSC OFF is activated.

Warning light flashes: a warning is issued actively. The system does not carry out any steering interventions.

For further information:

Lane Departure Warning, see page [215](#).

White lights

Cruise Control with Distance Control



No Distance Control because the accelerator pedal is being pressed.

For further information:

Distance Control, see page [252](#).

Assisted Driving Mode Plus



The system can be activated.

For further information:

	Displays	CONTROLS 
--	----------	--

Assisted Driving Mode Plus, see page 265.

Personal Pilot



The Personal Pilot is available and can be used.

For further information:

Personal Pilot, see page 275.

Selection lists

Principle




The instrument cluster or the Head-up display can show lists for certain functions and can be used for operation where applicable.

- ▶ Entertainment source.
- ▶ Current audio source.
- ▶ Recent calls list.

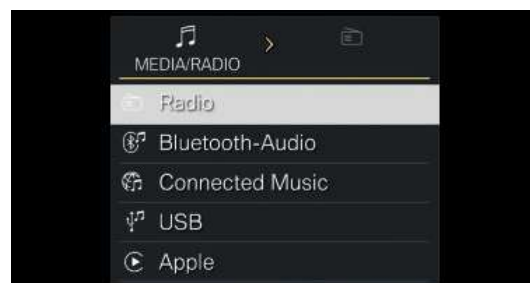
If applicable, the relevant menu is opened on the control display.

Displaying and using the list

The selection lists can be displayed and operated using the operating elements on the steering wheel.



Operating elements	Function
	Change the entertainment source. Press the button again to close the list currently displayed.
	Display the last calls list.
	Turn the knurled wheel: display the list of the currently selected entertainment source or scroll up or down in the list. Tilt the knurled wheel in the corresponding direction: move the selection to the left or right. Press the knurled wheel: confirm the selection.

Display



The selection lists, for example, entertainment sources, are displayed in the instrument cluster.

Example: selecting a radio station

1.  Press the button for entertainment sources.
2.  To switch to the list of radio stations, tilt the knurled wheel to the right.

Appendix B

Testing Matrix

S. No.	Start State	End State	Description	Variation	Check box	Time Log	Comments/Notes
1	Personal Pilot		Start in a prescribed state, turn on L3, turn off L3 again. Check state at the end.	L0 -> L3 -> ? L1 -> L3 -> ? L2 -> L3 -> ? L3 -> L0 -> ?	<input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	11:29 11:30 14:08 15:02	L3 reverted back to manual control Personal Pilot activated and deactivated within a few seconds. Cannot adjust seat. Removal of seat belt will deactivate personal pilot
2	Personal Pilot		Driver is required to sit in an upright sitting position. What happens if you change position?	Change positions	<input checked="" type="checkbox"/>		
3	Personal Pilot		With L3 active, pressing accelerator pedal should switch it off		<input checked="" type="checkbox"/>	14:08	Pressed throttle but without touching the steering wheel, it did not work (not ideal)
4	Supporting functions active (AEB, AEB-Speed limit info, lane departure warning)		Start driving without turning on Personal Pilot. Is this offered to you during the drive then?	-	<input checked="" type="checkbox"/>		In the default menu, if you switch PP on, only then it is offered to you.
5	Supporting functions active (AEB, AEB-Speed limit info, lane departure warning)		If we have not disabled Distance control with cruise control setting on the center screen, can we see the Cruise Control option when we toggle through the Cruise Control Mode button?	-	<input checked="" type="checkbox"/>		Cruise control mode is not visible when disabled.
6	Distance control	Assisted Driving Mode	What happens when we turn on the system when the vehicle is not fully in the center of the lane (e.g. a bit more to the right of the lane)? -> Is this not permitted? Or is there a sudden intervention from the ADM, which could lead to a (unintentional) counter-movement by the driver?	1 2 3 4 5	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	13:12 13:14	When close to lane markings, Assisted Driving Mode (ADM) does not get activated. It doesn't help that the car is very wide. Same. Need to be in the center of the lane and hold the steering wheel to activate ADM again. Distance control is available but not ADM
7	Distance control		Vehicle in front comes to a complete halt. The system should comprehend if the conditions allow. But, Otherwise the driver should drive independently. -> What does this mean?	1 2 3	<input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>		Stood behind a truck. Complete halt, vehicle accelerated itself once lead vehicle started moving. Stood behind a different truck. Complete halt, vehicle accelerated itself once lead vehicle started moving. Sometimes I recognize traffic lights and starts to accelerate itself. Sometimes, it does not.
8	Distance control		Does pressing the gas pedal give an override?		<input checked="" type="checkbox"/>		Yes, pressing the gas pedal overrides distance control.
9	Assisted Driving Mode	Lane Change Assistant	Does it suggest a lane change if we are stuck behind a slower vehicle and the next lane is free?	1 (Extra large gap to lead vehicle)	<input checked="" type="checkbox"/>	14:01	Lane change assistant requires a destination selected in the navigation (route guidance). Fast approaching a truck in the right-most lane. Lane change (LC) suggestion
10	Lane Change Assistant			2 (Large gap to lead vehicle)	<input checked="" type="checkbox"/>	14:04	Same as above
11	Lane Change Assistant			3 (Normal gap to lead vehicle)	<input checked="" type="checkbox"/>	13:57	When gap is available, decelerate in own lane first and then accelerate in the target lane
12	Assisted Driving Mode		Automatic or manual lane change assistant. Manual	Manual 1	<input type="checkbox"/>		
13	Assisted Driving Mode		-> Confirm the functioning, note down experience	Manual 2	<input type="checkbox"/>		Works well (you need to look in the side mirror)
14	Assisted Driving Mode		Manual: Needs activation by the user using indicator on their free will	Automatic 1	<input checked="" type="checkbox"/>		Initially, it was thought that only LC to the left were suggested. But, this is not the case. It also suggests LC to the right.
15	Assisted Driving Mode		Steering wheel jerks when the system makes a lane change suggestion: Could lead to confusion for the driver.	Automatic 2	<input checked="" type="checkbox"/>		No (major) steering wheel jerk
16	Assisted Driving Mode		Automatically offered when ADM is active and operational requirements of ADM+ are met. What does this mean? How is this prompted?	Once	<input checked="" type="checkbox"/>		Indicated on the screen that ADM+ is available. However, to activate it, you need to release the steering wheel. It was unclear in the beginning which led to the question of why ADM+ was not activating. The message on the HMI says ADM+ allows one to keep their hands in a comfortable position near the steering wheel without directly saying hands off.
17	Assisted Driving Mode		Does pressing the gas pedal give an override?	Once	<input checked="" type="checkbox"/>		Yes, it overrides
18	Assisted Driving Mode		If ADM is interrupted, which state do you		<input checked="" type="checkbox"/>		System interrupted -> Driver distraction -> Switches to ADM

Potential Functional Insufficiencies and Testing.xlsx

S. No.	Start State	End State	Description	Verification	Check box	Time Log	Comments/Notes
29	Driving Mode Plus		go to? Multiple variants could exist, based on the situations encountered		<input type="checkbox"/>		General remarks
30							At 11:10, door of the car was opened but car started moving momentarily.
31							Speed limit update takes a few seconds
32	Assisted Driving Mode Plus		Can you turn off ADMP without turning off ADMP?		<input type="checkbox"/>		No clear indication on the display as to why a certain maneuver is suddenly executed or aborted.
33	Assisted Driving Mode Plus		Does pressing the gas pedal give an override?		<input checked="" type="checkbox"/>		ADM or ADM+ are not indicated with green lights on the steering wheel. Not sure if this vehicle-specific. Manual pilot activation and use was indicated with turquoise lights.

Potential Functional Insufficiencies and Testing.xlsx

S. No.	Start State	End State	Description	Verification	Check box	Time Log	Comments/Notes
34	-		When you turn off any system (e.g. ADM) using the cruise control button (VO) -> when you press the (VO) button again, does it turn ADM back on directly?	ADM -> IO -> ? ADM -> IO -> ?	<input checked="" type="checkbox"/>		ADM -> Off -> ADM ADM -> Off -> ADM
35							
36				Distance Control -> > IO -> ?	<input checked="" type="checkbox"/>		Distance control -> Off -> Distance control
37				TP -> IO -> ?	<input type="checkbox"/>		
38	-		With engine running, change the settings. Do a complete shut down, lock/unlock the vehicle, restart vehicle. Settings still there?	Once	<input checked="" type="checkbox"/>		Yes, Settings remain the same as they were before switching off.

Appendix C

Testing vehicle settings



Potential Functional Insufficiencies and Testing.xlsx

S. No.	Menu/Control	Setting	Check Box	Comments/Notes
1	1. Apps menu 2. "Vehicle" 3. "Driving settings" 4. "Driver assistance" 5. "Driving" 6. "Assisted Driving"	"Lane Change Assistant": on	<input checked="" type="checkbox"/>	
2	1. Apps menu 2. "Vehicle" 3. "Driving settings" 4. "Driver assistance" 5. "Driving" 6. "Assisted Driving"	"Auto. Lane Change Assistant": on (if available)	<input checked="" type="checkbox"/>	
3	1. Apps menu 2. "Vehicle" 3. "Driving settings" 4. "Driver assistance" 5. "Driving" 6. "Assisted Driving" 7. "Emerg. Corridor Assistant"	"Emerg. Corridor Assistant": on	<input checked="" type="checkbox"/>	Could not find the option of Emergency Corridor Assistant in Assisted Driving
4	1. Apps menu 2. "Vehicle" 3. "System settings" 4. "Pop-ups" 5. Select the desired setting.	Personal Assistant: Off	<input type="checkbox"/>	Offers voice control, also for vehicle functions (e.g. >Increase the ACC distance<). Let's not dive into this...
5	1. Apps menu 2. "Vehicle" 3. "Driving settings" 4. "Driver assistance" 5. "Driving" 6. "Notifications"	<Unclear what the options are>	<input checked="" type="checkbox"/>	Expanded setting was chosen (not sure what it meant here) Make a choice and register it. Perhaps the choices you make here influence the likelihood of mode confusion.

Potential Functional Insufficiencies and Testing.xlsx

S. No.	Menu/Control	Setting	Check Box	Comments/Notes
6	Adjusting the distance 1. Apps menu 2. "Vehicle" 3. "Driving settings" 4. "Driver assistance" 5. "Driving" 6. "Distance control" 7. "Distance"	<Unclear what the options are>	<input checked="" type="checkbox"/>	Avoid overtaking to the right option is turned on Cruise control only setting is turned off Make a choice and register it.
7	1. Apps menu 2. "Vehicle" 3. "Driving settings" 4. "Driver assistance" 5. "Driving" 6. "Distance control" 7. "Situational distance control"	<Unclear what the options are>	<input checked="" type="checkbox"/>	Choose small (default), explanation says: Distance adjusted automatically depending on the speed Make a choice and register it.
8	1. Apps menu 2. "Vehicle" 3. "Driving settings" 4. "Driver assistance" 5. "Feedback via steering wheel" 6. "Light elements"	Driver assistance + personal pilot Only when personal pilot is on are the possible settings	<input checked="" type="checkbox"/>	Driver assistance + personal pilot (did not work for driver assistance though...) Make a choice that does show lights on the SW and register it
9	1. Apps menu 2. "Vehicle" 3. "Driving settings" 4. "Driver assistance" 5. "Driving" 6. "Route and junction assistant"	"Automatically adjust speed to route" (if available) means that it will eg stop at traffic lights	<input checked="" type="checkbox"/>	on

Potential Functional Insufficiencies and Testing.xlsx

S. No.	Menu/Control	Setting	Check Box	Comments/Notes
10	Automatic Hold	<p>Activate Automatic Hold</p> <p>1. Switch on drive-ready state.</p> <p>2.  Press the button. The LED is illuminated.</p> <p> The indicator light illuminates green. Automatic Hold is activated.</p>	<input checked="" type="checkbox"/>	P160 manual
11	1. Apps menu 2. "Vehicle" 3. "Driving settings" 4. "Driver assistance" 5. "Driving" 6. "Speed Limit Assistant" 7. "Speed limits" 8. Select the desired setting:	"Adjust automatically"	<input checked="" type="checkbox"/>	Adjust automatically was chosen
12	Personal pilot	Availability map available in-vehicle	<input checked="" type="checkbox"/>	
13	ADM+	on	<input checked="" type="checkbox"/>	
		Front Collision Warning		Early
		Lane Departure Warning		Expanded
		Lane Change Warning		Expanded (reduced or off are the other options)
		Side Collision Warning		On
		Steering Intervention & Warning When Turning		On (might be a part of LCW)
		Road Priority Warning		Medium
		Exit Warning (expanded)		Warning tone
		Emergency Stop		On
		Attentiveness Assistant		Sensitive (standard/off)
		Speed warning		
		Warning for Speed Limits		

Mobility & Built Environment

Automotive Campus 30
5708 JZ Helmond
www.tno.nl