SIMULATION-BASED APPLICATION OF SAFETY OF THE INTENDED FUNCTIONALITY TO MITIGATE FORESEEABLE MISUSE IN AUTOMATED DRIVING SYSTEMS

Milin **PATEL**[1], Rolf **JUNG**[2]

[1] *Institute for Advanced Driver Assistance Systems and Connected Mobility, Germany*, [2]*Kempten University of Applied Sciences, Germany*
milin.patel@hs-kempten.de , rolf.jung@hs-kempten.de

Keywords: ADS, FM, Simulation-based testing, SOTIF

Abstract*: The development of Automated Driving Systems (ADS) has the potential to revolutionize the transportation industry, but it also presents significant safety challenges. One of the key challenges is ensuring that the ADS is safe in the event of Foreseeable Misuse (FM) by the human driver. To address this challenge, a case study on simulation-based testing to mitigate FM by the driver using the driving simulator is presented. FM by the human driver refers to potential driving scenarios where the driver misinterprets the intended functionality of ADS, leading to hazardous behavior. Safety of the Intended Functionality (SOTIF) focuses on ensuring the absence of unreasonable risk resulting from hazardous behaviors related to functional insufficiencies caused by FM and performance limitations of sensors and machine learning-based algorithms for ADS. The simulation-based application of SOTIF to mitigate FM in ADS entails determining potential misuse scenarios, conducting simulation-based testing, and evaluating the effectiveness of measures dedicated to preventing or mitigating FM. The major contribution includes defining (i) test requirements for performing simulation-based testing of a potential misuse scenario, (ii) evaluation criteria in accordance with SOTIF requirements for implementing measures dedicated to preventing or mitigating FM, and (iii) approach to evaluate the effectiveness of the measures dedicated to preventing or mitigating FM. In conclusion, an exemplary case study incorporating driver-vehicle interface and driver interactions with ADS forming the basis for understanding the factors and causes contributing to FM is investigated. Furthermore, the test procedure for evaluating the effectiveness of the measures dedicated to preventing or mitigating FM by the driver is developed in this work.*

1. INTRODUCTION

Automated Driving System (ADS) is a complex system that is designed to perform some or all of the driving tasks that are traditionally performed by a human driver [1]. This includes acceleration, braking, steering, and navigation with the goal of improving road safety and reducing driver workload. Safety is crucial in ADS due to its reliance on perception sensors and complex algorithms for situational awareness. Malfunctions or failures in these systems can have hazardous consequences for vehicle occupants and other road users.

Foreseeable Misuse (FM) refers to the potential for human drivers to intentionally or unintentionally misuse ADS, leading to unsafe situations. This can occur when drivers do not fully understand the capabilities and limitations of the ADS, or when they engage in behaviors that are not consistent with the intended use of the system. FM can also occur when drivers fail to take over control of the vehicle when required, such as in situations where the system is unable to operate safely, or when the driver is required to take over control due to a system malfunction [2].

The safety challenges associated with FM are significant because they can lead to serious accidents and injuries. To address these challenges, it is important to develop and implement effective mitigation measures that can prevent or reduce the risk of FM. This requires a comprehensive evaluation of the ADS that considers a wide range of driving scenarios and human factors, including the driver's understanding of the system's capabilities and limitations, their responsibilities, and their ability to comprehend and respond to warnings and alerts.

To illustrate the significance of addressing FM, consider the fatal accident involving a Tesla Model S in 2016. The driver was using the Autopilot system, which is intended to assist with steering, braking, and acceleration. However, the driver was not paying attention to the road and did not take over control of the vehicle when required. As a result, the autopilot system failed to detect a truck that was crossing the road, and the vehicle collided with the truck, resulting in the driver's death [3].

ISO 21448[2] is the standard for Safety of the Intended Functionality (SOTIF) that provides guidance to identify and analyze potential hazards and risks associated with the intended functionality of an ADS that may arise due to foreseeable misuse by human drivers. In the following, the term 'system' is used in place of ADS.

Testing for FM is a challenging task due to the system's complexity and the vast range of potential misuse scenarios. Anticipating all potential misuse scenarios poses challenges in designing and testing the system to effectively prevent or mitigate such occurrences. Additionally, testing for FM can be time-consuming and expensive, requiring extensive testing and evaluation to ensure that the system meets intended safety requirements.

Simulation-based testing overcomes the above-mentioned challenges by creating a controlled environment to systematically evaluate potential misuse scenarios, replicating challenging or hazardous real-world scenarios. Simulation-based testing offers a safer and more efficient means of comprehensively evaluating a system's responses, robustness, and ability to effectively prevent or mitigate misuse effects.

Patel et al.[4] proposed a simulation-based approach for testing FM by the driver in highly automated driving systems and discussed the importance of managing driver-system interactions and the implications of driver-vehicle-interface design on these interactions. However, the proposed approach in the paper[4] does not focus on the mitigation of FM.

Mitigation of FM refers to the process of identifying potential misuse of the intended functionality of the system and taking measures to reduce the associated risks to an acceptable level.

The major contribution of the presented work lies in defining the simulation-based test procedure for evaluating the effectiveness of the measures dedicated to preventing or mitigating FM by the driver. In this context, the main contributions of this work are to:

- Define the test requirements: The test requirements must specify the simulation environment, including the vehicle model, the sensor models, and the simulation software. The test requirements must be designed to ensure that the simulation accurately represents the real-world scenario and that the system's response to the scenario can be evaluated.

- Formulate evaluation criteria: The evaluation criteria must be designed to ensure that the measures are effective in preventing or mitigating FM and that they do not introduce new hazards or adversely affect the vehicle's intended functionality.

- Propose an approach to evaluate the effectiveness of measures dedicated to preventing or mitigating FM: The approach must include testing the system's response to potential misuse scenarios, to ensure that the system can detect and respond appropriately to these scenarios.

A. Structure of the paper

The subsequent chapters of this paper are organized as follows: Chapter 2 presents an extensive background, briefly explaining misuse types in ADS, factors and causes of misuse, accompanied by a case study on simulation-based testing of foreseeable misuse. In Chapter 3, the concept for simulation-based application is proposed, detailing the workstation setup and defining essential test requirements. Chapter 4 delves into approach to evaluate the effectiveness of measures dedicated to prevent or mitigate FM, emphasizing conditional probability analysis and the assessment of simulation results. Finally, Chapter 5 concludes by summarizing key findings and implications, and suggesting future research directions.

2. BACKGROUND

A. Types of Misuse

ISO 21448[2] defines two types of misuse in the ADS: direct misuse and indirect misuse. Direct misuse involves conditions that can trigger hazardous behavior in the system, while indirect misuse refers to driver behavior that reduces controllability or increases the severity of an accident without directly causing hazardous behavior in the system.

Instances of direct misuse in ADSs include overconfidence in system performance, misunderstanding of the system's capabilities, lack of understanding regarding system functions, incorrect assumptions about driver interaction based on design specifications, and driver expectations that do not align with the system's capabilities [2].

Indirect misuse instances involve driver fatigue leading to decreased ability to interact with or monitor automation features, distractions stemming from mobile devices or other passengers, reduced attentiveness due to prolonged use or monotonous driving conditions, and over-reliance on automated driving functions without maintaining situational awareness [2].

B. Factors and causes of misuse

Driver Recognition (DR), and Driver Judgment (DJ) are factors and causes of misuse that can contribute to direct or indirect misuse scenarios.

Driver Recognition (DR): Driver recognition refers to the process of perceiving and interpreting the driving environment, including the road, traffic, and surrounding objects. Failures in driver recognition may manifest when drivers overlook the limitations of ADS or misinterpret the driving environment.

For example, a driver may fail to recognize that the ADS is not capable of detecting certain objects like pedestrians or bicycles, and may rely on the system to avoid collisions. This can lead to unsafe situations if the ADS fails to detect these objects, and the driver does not take appropriate action.[5]

Driver Judgment (DJ): Driver judgment refers to the process of making decisions based on the driving environment and the capabilities of the ADS. FM related to driver judgment can occur when drivers make erroneous decisions based on incorrect assumptions about the ADS or the driving environment.

For example, a driver assuming that the ADS is capable of navigating through heavy rain or fog, even though the system is not designed for this purpose. The ADS may not be

able to detect the road markings or other objects in such conditions, and the driver may not take appropriate action, leading to a collision. [5]

C. Case Study on Simulation-based testing for Foreseeable Misuse by the driver

Patel et al.[4] proposed a strategy for implementing simulation-based testing of FM resulting from the system-initiated transition between the human driver and the ADS. The system-initiated transition is the process and period for transferring responsibility and driving control over some or all aspects of the driving tasks between the human driver and the system.

Simulation-based testing involves using a driving simulator to simulate a modeled misuse scenario in the virtual test environment and analyzing the results to determine whether the system meets the intended safety requirements. However, simulation can be limited by the underlying assumptions about environmental conditions, sensors, and the vehicle model.

Patel et al. [4] acknowledged that the strategy presented is to demonstrate an approach for simulation-based testing of FM and is not intended to be a distinctive or optimal measure dedicated to mitigating FM. Also, the implementation of the strategy has not been evaluated in practice, and therefore, the effectiveness of the measures dedicated to preventing or mitigating FM has not been evaluated.

3. PROPOSED CONCEPT FOR SIMULATION-BASED APPLICATION

A. Determining SOTIF-related Misuse Scenario

To derive a misuse scenario, various sources, including lessons learned, expert knowledge, and brainstorming, can be utilized. ISO 21448 (Annex B1) provides a systematic approach for deriving an SOTIF-related misuse scenario. [2]

The process for identifying a misuse scenario begins with understanding the intended functionality of the system. This entails comprehending the system's purpose, its designated user base, and the environment in which it will operate. Once the intended functionality is understood, the next step is to identify potential misuses of the system. This includes understanding how the system could be used in unintended ways and how these misuses could lead to hazards. [6]

The potential misuses can be categorized based on their severity and likelihood. This helps prioritize the misuses that pose the greatest risk to safety. Based on the potential misuses identified, a misuse scenario should be developed. The misuse scenario should describe how the system could be misused, the potential consequences of the misuse, and the likelihood of the misuse occurring. [6]

Lastly, the evaluation of the misuse scenario is crucial to determine its impact on the

safety of the ADS. This includes assessing the likelihood of the misuse occurring, the severity of the consequences, and the effectiveness of any mitigation measures that could be implemented. It is important to note that misuse scenarios should not only consider deliberate violations but also human driver errors that could lead to the unintended use of the system.

The Table 1 depicts a description of a misuse scenario derived from [4], in accordance with an example methodology outlined in ISO 21448 (Annex B1).

Table 1: Description of SOTIF-related misuse scenario, adapted from [2]

Potential SOTIF-related misuse scenario	Stake-holder	Foreseeable Misuse		Driver-System Interactions	Environmental Conditions	Derived Hazardous Scenario
		Factors	Causes			
Described below [1]	Driver	Recognition	False recognition	Described below [2]	Described below [3]	Described below [4]
		Judgement	Misjugment			

[1] The Ego-Vehicle encounters a road with missing lane markings during automated driving on a two lane one-way highway and executing lane change maneuver from right to left lane. The camera sensor cannot estimate the location of the lane boundary due to a performance limitation of the camera sensor. Ego-Vehicle starts to leave the lane and driver is notified to take control of the driving tasks by means of Take-Over-Request (TOR).

[2] "Delayed Take-over" and/or "Take-Over and perform Over/Understeer"

Weather: clear

Light Condition: daylight

Traffic Condition: light traffic

Roadway Surface and Features: missing lane markings

[4] Driver fails to take-over the control of the driving tasks, resulting in lane departure of Ego-Vehicle.

B. Workstation setup for Simulation-based Testing

The workstation has been developed with an integrated driving simulator equipped with hardware tools, including the Logitech G29 steering wheel, pedals, and gearbox, integrated with a simulation tool, IPG CarMaker, to perform simulation-based testing of foreseeable misuse. The driving simulator is static simulator that allows a human driver to engage in the simulation-based application.

The block diagram in *figure 1* represents a workstation setup consisting of several components that collaborate to execute driving tasks.
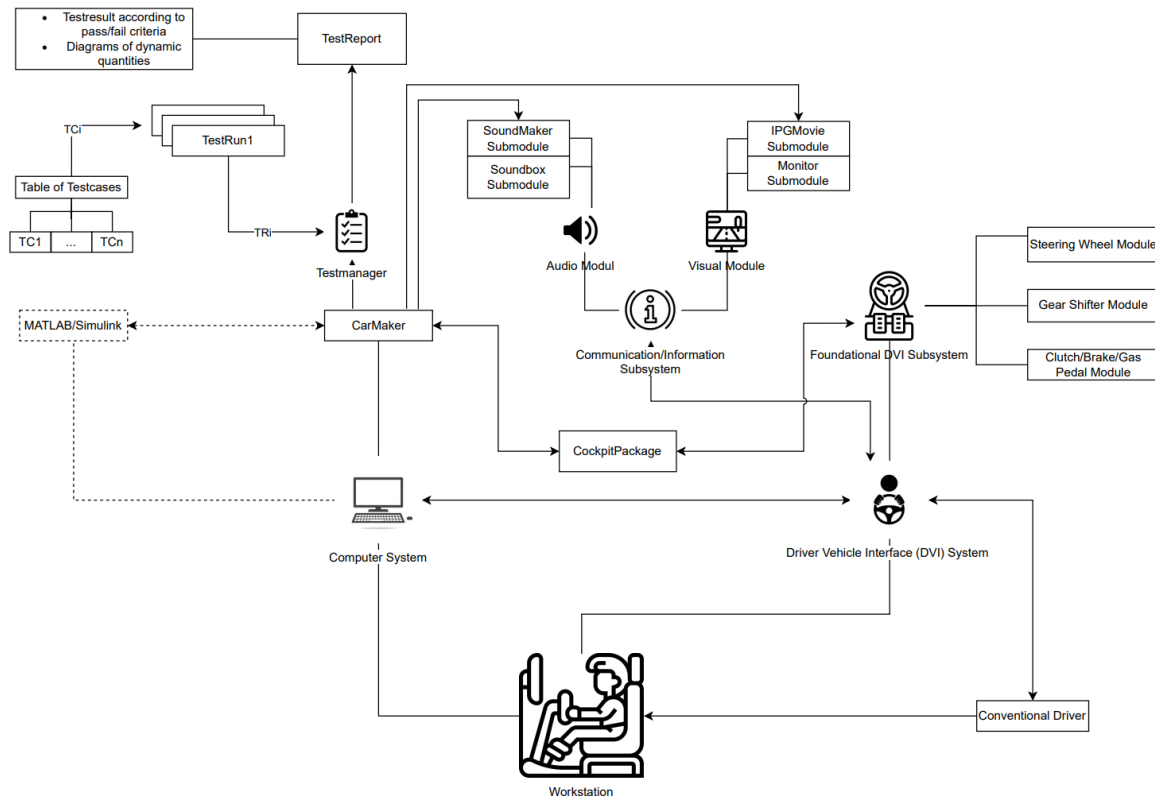
Fig. 1: Representation of a workstation setup to perform simulation-based testing of foreseeable misuse by the driver

The "Foundational DVI subsystem" is responsible for man- ual driving and allows the driver to interact with sensor module, controller module, environment module, and other ehicle modules.

"CarMaker" is a software tool for developing and testing virtual vehicle models, while "CockpitPackage" is an exten- sion in CarMaker that facilitates the integration of hardware components including steering wheels, clutch/brake/gas ped- als, and gear shifters into the simulation environment.

The "Communication/Information" subsystem provides vi- sualization of the simulation and includes modules like IPG- Movie for real-time 3D animation of the virtual driving simulation and Sound-Maker software for 3D audio. It also en- compasses the Visual Module, which contains the Instruments Panel sub-module for providing information to the driver about the current status of the driving mode and warnings in case of upcoming events.

TestManager is a software tool employed in CarMaker for simulating Test Cases (TC). It permits the creation, execution, and management of TC. The test cases are a set of predefined procedures that are used to verify the functionality of the system under test. The TestManager sequentially invokes the TestRuns to execute a Test-case Series (TCS). After each TCS, a TestReport is generated, displaying all executed TC and their outcomes. The TestManager also allows the addition of pass/fail criteria to determine TCS success.

C. Defining test requirements for performing simulation-based testing

The simulation requirements become relevant at different phases of simulation-based testing. Therefore, test requirements are formulated in form of a checklist, encompassing a series of questions. The checklist is presented in form of question cards.

Table II illustrates the template of the presented question cards. In the top-right corner of the question card, the question number is denoted by [1, 2, ..., n], followed by the primary question. On the bottom-left, possible responses to the ques- tion are provided. An explanation for the respective question is provided in the bottom-right corner of the table.

Table 2: Template of the checklist

Question Number	[1,2,. . .,n]
Main Question	
Possible Response	Explanation

In the following, a set of questions (No.1 – No.10) representing the requirements for the simulation-based testing are provided in Table 3 below.

Table 3: Question Cards

Question Number	1
Does the system performs automated driving of the ego-vehicle by providing longitudinal and lateral control in the modeled scenario?	
Yes / No	The simulation starts initially in automated driv-ing mode. It is intended to provide longitudinal control of the Ego-Vehicle on a right lane in a one way two-lane highway environment. All automated driving function should be active and work.
Question Number	2
Does the Ego-Vehicle encounters a road with unclear lane markings during the initialization of the lane change from right lane to left lane?	
Yes / No	The Ego-Vehicle encounters a part of the road with unclear lane markings while executing lane change maneuver from right to left lane.
Question Number	3
Does the ADS send a warning to the driver when the Ego-Vehicle encounters the specified road conditions in Question 3?	
Yes / No	Visually and auditory warning is sent out at 6.04 seconds of the simulation time and the lane departure warning is activated because unclear lane markings are detected.
Question Number	4
If the driver not respond to the warnings, does the system notify the driver by issuing imminent Take-Over-Request (TOR)?	

Yes / No	If the driver not response to the warning then the ADS will request the driver to Take-Over (TO). The TOR is sent at 7.96 seconds of the simulation time.
Question Number	**5**
Does the driver response to the TOR?	
Yes / No	The driver can respond to the TOR and does the TO of driving task by means of driver- vehicle-interface (Logitech G29 Steering Wheel buttons). The system is expected to remain op- erational in automated driving mode until the driver is able to regain control of the driving task.
Question Number	**6**
Does the system transition into automated driving with reduced function- ality mode and performs minimal risk maneuver?	
Yes / No	If the driver does not TO the driving tasks in the event of TOR, the system will transition to the automated driving with reduced functionality. Subsequently, a minimal risk maneuver is per- formed by the system to keep the Ego-Vehicle in its lane and to automatically stop the Ego- Vehicle on the side of the road in a safe manner [7].
Question Number	7
Does the driver TO of the driving task in the specified time?	
Yes / No	The driver does take-over in time, if the TO time is less than 1.77 seconds [8]. The TO-time is the difference between TOR and TO. Take-over after 1.77 seconds are considered as delayed TO (i.e., considered as FM).
Question Number	**8**
Does the adjusted Steering wheel Angle (SWA) by the driver after TO lead to Oversteer or Understeer (i.e, considered as FM) ?	
Yes / No	Ideal SWA could be defined as the SWA that will centre the Ego-Vehicle in the middle of the current lane (left lane). · Over-steer if the adjusted SWA is greater than ideal SWA. · Understeer if the adjusted SWA is smaller than ideal SWA.
Question Number	**9**
Does the FM by the driver lead to Hazard?	
Yes / No	Hazard if the Ego-Vehicle departs lane. a. Lane departure towards the east from left lane or b. Lane departure towards the west from left lane
Question Number	**10**
Does the driver able to handle the driving situation (after TO by driver), measured as controllability?	
Yes / No	Likelihood that the driver can cope with driving situations including the system limits and system failures is defined as "controllability" [9]. · Controllability is provided if driver does TO successfully without leading to hazard. · Controllability is not provided if driver TO unsuccessfully leading to hazard.

4. APPROACH TO EVALUATE THE EFFECTIVENESS OF MEASURES DEDICATED TO PREVENTING OR MITIGATING FORESEEABLE MISUSE

A. Conditional Probability Analysis

Conditional probability analysis is chosen as the primary approach to establish a systematic and quantifiable approach to understanding relationships between factors and causes of FM within the ADS. In particular, the focus is on two key elements: False Recognition (FR) and Misjudgment (MJ).

The choice of employing the conditional probability anal- ysis approach is informed by the methodology outlined by Mkrtchyan et al. [10], which demonstrates the applicability of this approach in evaluating safety-critical systems.

The below provided analysis is based on considering the SOTIF-related misuse scenario described in *Table 1*, and in accordance with defined requirements in *Table 3*.

Misjudgment (MJ): It relates to situations where the driver makes an erroneous decision during the Take-Over (TO) pro- cess, potentially resulting in under-steering or over-steering, and potential for a lane departure (i.e., hazard).

The probability of Misjudgment is assessed under two conditions:

1) when there is no delayed take-over (TO ≤ 1.77 seconds) and a Hazard (H) is present, mathematically expressed as:

$$P(MJ|TO \leqslant 1.77\,s, H) = \frac{P(TO \leqslant 1.77\,s \cap H)}{P(MJ \cap TO \leqslant 1.77\,s \cap H)} \qquad (1)$$

2) when there is a delayed take-over (TO > 1.77 seconds) in the presence of a Hazard (H), mathematically expressed as:

$$P(MJ|TO > 1.77\,s, H) = \frac{P(TO > 1.77\,s \cap H)}{P(MJ \cap TO > 1.77\,s \cap H)} \qquad (2)$$

False Recognition (FR): It occurs when the driver fails to promptly recognize the necessity of take-over control. This can result in delayed takeover, leading to a delayed take-over and the potential for a lane departure (i.e., hazard).

The probability of False Recognition is evaluated under the condition of a delayed take-over (TO > 1.77$ seconds) when a hazard (H) is present, mathematically expressed as:

$$P(FR|TO > 1.77\,s, H) = \frac{P(TO > 1.77\,s \cap H)}{P(FR \cap TO > 1.77\,s \cap H)} \qquad (3)$$

As a visual aid, *figure 2* illustrates a probability tree dia- gram depicting the relationships between Misjudgment (MJ) and False Recognition (FR). This diagram provides a struc- tured representation of conditional probabilities, enhancing the understanding of the interactions among various factors and causes of FM.
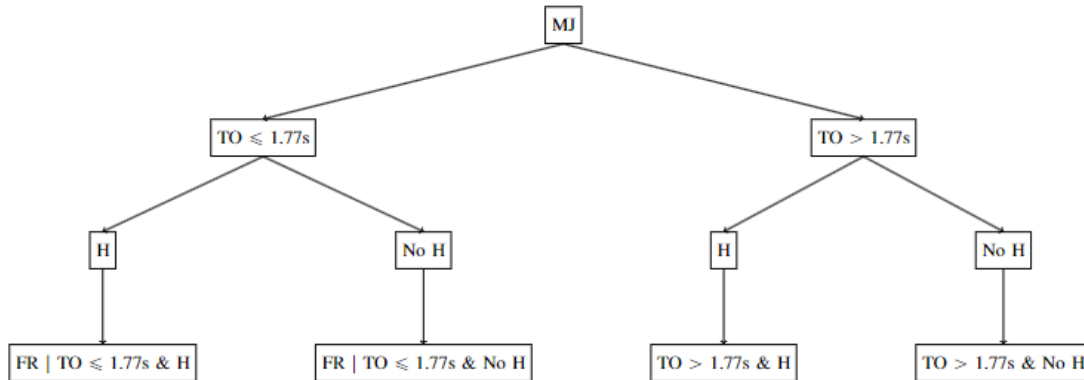

Fig. 2: Probability Tree Diagram for Misjudgment (MJ) and False Recognition (FR)

- The top level represents the conditional probability of Misjudgment (MJ).
- The second level represents the two scenarios based on Takeover (TO) time being less than or greater than 1.77 seconds.
- The third level represents the presence or absence of Hazard (H) in each scenario.
- The last level represents the conditional probability of False Recognition (FR) based on the Takeover (TO) time and Hazard (H) conditions.

B. Evaluation of simulation-based application

An exemplary Table 4 of Test Case Series (TCS) is presented based on results of simulation-based application of FM. Because of the high amount of TC, all simulation results of TC are not entailed. Only a exemplary Table 4 is provided to demonstrate the results.

TestManager is a tool employed in software CarMaker for simulating Test Cases (TC). TestManager allows the creation, execution, and management of TC. The TestManager sequen- tially invokes the TC to execute a Test-case Series (TCS).

Table 4: Exemplary Test Case Series (TCS)

TC	TO	TO t2 [s]	delta T2 [s]	DelTO	SWA [deg]	H	H t3 [s]	delta T3 [s]
1	1	10.2300	2.2700	1	12.5144	0	0.0000	0.0000
2	1	10.7300	2.7700	1	3.2086	0	0.0000	0.0000
3	1	11.0800	3.1200	1	15.2058	1	11.1000	0.0200
4	1	9.1200	1.1600	0	32.1657	1	10.4000	1.2800
5	1	11.3500	3.3900	1	10.5064	1	11.1000	0.4600
...	...	...	...	...	...	...	...	...
TCn	...	...	...	...	...	...	...	...

The Test Cases (TC) encompass various parameters, includ- ing Takeover (TO), Delayed TO (DelTO), and Hazard (H), which are logic values, either 0 or 1. The explanations for each parameter are presented below.

1) *Takeover (TO):* The parameter "TO" signifies whether the driver take-over control of the driving task in a given TC. A value of 1 indicates a take-over of the driving task by the driver.

2) *Delayed Takeover (DelTO):* The parameter "DelTO" is set to 1 when the driver take-over control after or/ more than 1.77 seconds. To calculate DelTO, "delta_T2" is used, representing the time difference between the Takeover Re- quest (TOR) time (fix value=7.96 seconds [4]) and the actual Takeover time (TO_t2). For instance, in TC 1, "DelTO" is 1 because the driver does take-over after 2.27 seconds.

3) *Hazard (H):* The parameter "H" indicates the lane departure of the vehicle (i.e., hazard) during a TC. It equals 1 if a hazard occurs. For instance, In TC 3, TC4 and TC5, "H" is 1 that indicates a lane departure.

4) *Hazard Time (H_t3)* and *Delta_T3*: The parameter "H_t3" represents the time of a hazard in a TC, and "Delta T3" is the time difference between "H_t3" and "TO_t2". In TC_3, "H_t3" is 11.1 seconds, and "Delta_T3" is 0.02 seconds.

5) *Steering Wheel Angle (SWA):* The parameter "SWA" reflects the driver's steering input at take-over. It is calculated as the difference between SWA at "TO_t2" and the maximum steering input immediately after take-over.

C. Assessment of Simulation Results

As mentioned in requirement Table 3, question 10, likeli- hood that the driver can cope with driving situations including the system limits and system failures is defined as "controlla- bility".

Within the simulation-based application, a total of 50 Test Cases (TC) were conducted. Among these, 22 TC (44%) exhibit controllability, signifying that the driver could regain control of the vehicle after a take-over. Conversely, 28 TC (56%) revealed a lack of controllability, resulting in hazard.

Table 5 presents probability analysis results based on simulation results. It outlines the likelihood of different events related to driver controllability. The outcomes reflect the chances of a specific scenario, including Misjudgment (MJ) and False Recognition (FR) under different driving conditions:

Table 5: Probability Analysis Results Based on Simulation Data

Probability Condition	Number of Test Cases	Percentage
P(TO 1.77s ✕ H)	10	20%
P(MJ ✕ TO 1.77 s ✕ H)	6	12%

Probability Condition	Number of Test Cases	Percentage
P(TO ⩽ 1.77 s ✗ H)	2	4%
P(MJ ✗ TO ⩽ 1.77 s ✗ H)	8	16%
P(FR ✗ TO ⩽ 1.77 s ✗ H)	2	4%

The conditional probabilities, as outlined in Table 5, can be calculated from Chapter 4.A

Misjudgment (MJ) Probability:

1) When there is no delayed take-over (TO ≤ 1.77 seconds) and a Hazard (H) is present

$$P(MJ|TO \leqslant 1.77\,s, H) = \frac{10}{6} = 1.67$$

(4)

This signifies that a driver is 1.67 times more likely to misjudge a situation when there is no delayed take-over (TO ≤ 1.77 seconds) and a Hazard (H) is present.

2) When there is a delayed take-over (TO > 1.77 seconds) in the presence of a Hazard (H):

$$P(MJ|TO > 1.77\,s, H) = \frac{2}{8} = 0.25$$

(5)

In this case, the likelihood of misjudgment is significantly reduced when there is a delayed take-over (T O > 1.77 seconds) in the presence of a Hazard (H).

False Recognition (FR) Probability: The probability ofFalse Recognition is evaluated under the condition of a delayed take-over (T O > 1.77 seconds) when a hazard (H) is present:

$$P(FR|TO > 1.77\,s, H) = \frac{2}{2} = 1$$

(6)

This implies that the probability of false recognition remains at 100% when there is a delayed take-over (TO > 1.77 seconds) and a Hazard (H) is present, indicating a high likelihood of recognizing a false situation.

It is important to note that these calculated probabilities are specific to particular conditions and a scenario with a limited number of test cases used in the simulation. These values are derived based on a specific threshold of 1.77 seconds for take-over time, and results may vary with different thresholds. Additionally, these results do not account for other potential factors that could influence driver behavior.

5. CONCLUSION AND FUTURE WORK

The paper introduces a comprehensive strategy for eval- uating the effectiveness of measures designed to prevent or mitigate Foreseeable Misuse (FM) within Automated Driving Systems (ADS). The primary approach employed for the assessment is Conditional

Probability Analysis (CPA), with a specific focus on key factors and causes for FM, including False Recognition (FR) and Misjudgment (MJ). The applica- tion of CPA is directed applied to a Safety of the Intended Functionality (SOTIF)-related misuse scenario.

The analysis provides valuable insights into the conditional probabilities associated with the occurrence of Misjudgment and False Recognition under various driving conditions. It is notably observed that the likelihood of Misjudgment diminishes significantly when a delayed Take-Over (TO) takes place, especially in the presence of a hazard (H). In contrast, the probability of False Recognition remains considerably high when TO is delayed and leads to a Hazard (H).

While these findings offer valuable insights into the evalu- ation of FM within ADS, it is essential to acknowledge that the calculated probabilities are specific to a specific misuse scenario and limited number of Test-cases utilized in the simulation. These values provide a foundational starting point for further refinement and adaptation to real-world scenarios, accounting for variations in threshold values for TO and other potentially influential factors affecting driver behavior.

There are several promising directions for future research. To begin, future investigations should prioritize the collection and analysis of real-world data to authenticate the outcomes from the simulation-based approach. Validating these findings in actual driving scenarios is pivotal for a more precise understanding of Foreseeable Misuse (FM).

Additionally, conducting sensitivity analyses on the thresh- old value of Take-Over (TO) time is crucial. This exploration will provide more insights into how alterations in the TO threshold value affect conditional probabilities. Moreover, an extensive examination of driver behavior and cognitive pro- cesses during take-over scenarios is necessary. This research should explore elements like driver fatigue, distractions, and driver experience and their conspicuous influence on FM likelihood.

REFERENCES

[1]   SAE J3016, *Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles - ground vehicle stan- dard: On-road automated driving (orad) committee*, United States, April.2021.

[2]   ISO 21448:2022, *Road vehicles – safety of the intended functionality*, Switzerland, 2022-06. [Online]. Available: https://www.iso.org/standard/ 77490.html.

[3]   National Transportation Safety Board, *Collision between a car oper- ating with automated vehicle control systems and a tractor-semitrailer truck near Williston*, Florida, May 7, 2016. Available: https://www.ntsb.gov/investigations/AccidentReports/Reports/HAR1702.pdf.

[4]   M. Patel, R. Jung, and Y. Cakir, *Simulation-based testing of foresee- able misuse by the driver applicable for highly automated driving*, in Proceedings of Eighth International Congress on

Information and Communication Technolog*y*, X.-S. Yang, R. S. Sherratt, N. Dey, and A. Joshi, Eds. Singapore: Springer Nature Singapore, 2024, pp. 183– 191.

[5] C. Becker, J. C. Brewer, and L. Yount, *Safety of the Intended Functionality of Lane-Centering and Lane-Changing Maneuvers of a Generic Level 3 Highway Chauffeur System*, 2020. [Online]. Available: https://rosap.ntl.bts.gov/view/dot/53628.

[6] F. Warg, S. Ursing, M. Kaalhus, and R. Wiik, *Towards safety analysis of interactions between human users and automated driving system*, 2020.

[7] M. Wood et all., *Safety First For Automated Driving*, 2019. [Online]. Available: https://www.aptiv.com/docs/default-source/white-papers/safety-first-for-automated-driving-aptiv-white-paper.pdf

[8] A. Eriksson and N. A. Stanton, *Takeover time in highly automated vehicles: Noncritical transitions to and from manual control*, Human Factors, vol. 59, no. 4, pp. 689–705, 2017.

[9] A. Knapp, M. Neumann, M. Brockmann, R. Walz, and T. Winkle, *ADAS Code of Practice (Code of Practice for the Design and Evaluation of ADAS)*, 2009.

[10] L. Mkrtchyan, L. Podofillini, and V.N. Dang, *Methods for building conditional probability tables of bayesian belief networks from limited judgment: An evaluation for human reliability application*, Reliability Engineering & System Safety, vol. 151, pp. 93–112, 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0951832016000132.