



## Simulation-Based Testing of Foreseeable Misuse by the Driver Applicable for Highly Automated Driving

---

Milin Patel, Rolf Jung and Yasin Cakir

EasyChair preprints are intended for rapid dissemination of research results and are integrated with the rest of EasyChair.

November 16, 2022

# Simulation-based Testing of Foreseeable Misuse by the Driver applicable for Highly Automated Driving

Milin Patel<sup>1</sup>, Rolf Jung<sup>1</sup>, and Yasin Cakir<sup>2</sup>

<sup>1</sup> Institut für Fahrerassistenz und vernetzte Mobilität, 87734, Germany  
{milin.patel, rolf.jung}@hs-kempten.de

<sup>2</sup> University of Applied Sciences Kempten, 87435, Germany  
yasin.cakir@stud.hs-kempten.de

**Abstract.** With Highly Automated Driving (HAD), the driver can engage in non-driving-related tasks. In the event of a system failure, the driver is expected to reasonably regain control of the Automated Vehicle (AV). Incorrect system understanding may provoke misuse by the driver and can lead to vehicle-level hazards. ISO 21448, referred to as the standard for Safety of the Intended Functionality (SOTIF), defines misuse as usage of the system by the driver in a way not intended by the system’s manufacturer. Foreseeable Misuse (FM) implies anticipated system misuse based on the best knowledge about the system’s design and the driver’s behavior. This is the underlying motivation to propose simulation-based testing of FM. The vital challenge is to perform a simulation-based testing for a SOTIF-related misuse scenario. Transverse Guidance Assist System (TGAS) is modeled for HAD. In the context of this publication, TGAS is referred to as the “system,” and the driver is the human operator of the system. This publication focuses on implementing the Driver-Vehicle Interface (DVI) that permits the interactions between the driver and the system. The implementation and testing of a derived misuse scenario using the driving simulator ensure reasonable usage of the system by supporting the driver with unambiguous information on system functions and states so that the driver can conveniently perceive, comprehend, and act upon the information.

**Keywords:** DSI, DVI, HAD, FM, SOTIF

## 1 Introduction

In HAD, longitudinal and lateral vehicle guidance is controlled by the system. However, when the system reaches its operational limits, the Human Driver (HD), referred to as a fallback-ready user in SAE J3016 taxonomy [1], is expected to regain driving control within a reasonable amount of time. Whenever the system is not capable of handling a situation within its Operational Design Domain (ODD), a Take-Over Request (TOR) is issued by the system as a notification indicating that the HD should promptly perform the driving tasks.

Transition in Automated Driving (AD) is the process and period of transferring responsibility and driving control over some or all aspects of the driving tasks between HD and the system. Transition can be either activation or deactivation of a function or a change from one driving state to another as per [2]. According to the SAE J3016 taxonomy [1], the driver has no active role or driving responsibilities when the system is operating within its ODD. Engagement in non-driving related task keeps the driver out of the loop, which leads to misuse when returning to Manual Driving (MD) in take-over situations [3].

To ensure smooth transition from AD to MD, the TOR must be presented through a well-designed interface. Therefore, the implications of Driver-Vehicle Interface (DVI) design on the interactions between driver and the system, abbreviated as Driver-System Interactions (DSI), must be studied so the driver can regain control over HAD while deterring misuse. The Figure 1 depicts a pictorial representation of the incorporation of the driver in terms of interactions with the system and interface with the Automated Vehicle (AV). One of the key subject in the SOTIF standard is FM, which is substantial consideration for human factors engineering [4]. It should be noted that this publication focuses on FM by the driver and as part of the testing, human factors during transition in HAD are taken into consideration, not the other way around.

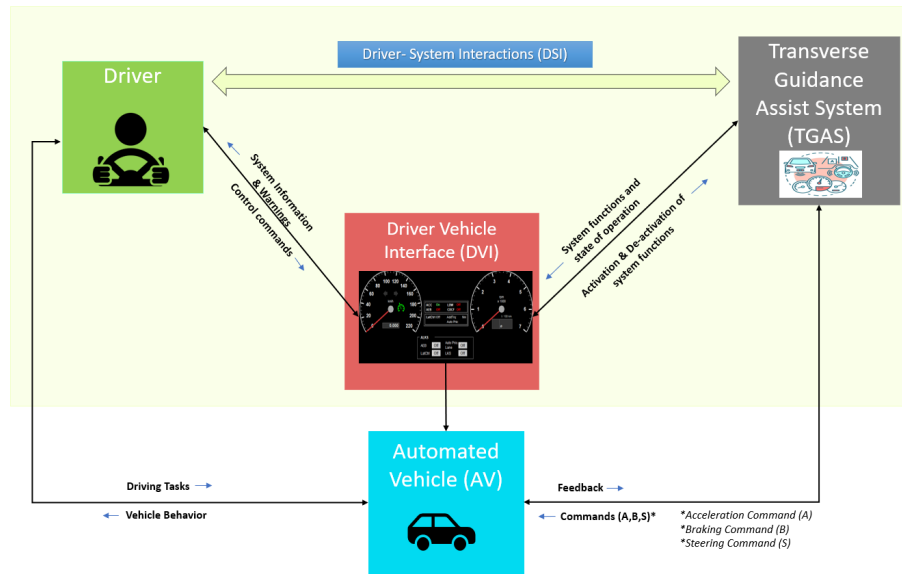


Fig. 1: Incorporation of the driver with the system and AV: interactions and the interface

The factors for FM considered in this publication are driver's Recognition & Judgment. Simultaneously, False recognition & Misjudgment, by the driver are causes for FM. The aforementioned factors and causes addressed in this publication are referred to as, human misuse process and guidewords, in the informative annex B of ISO 21448 [5]. The False recognition is analogous to the perceptual errors, where the driver's perception of the environment differs from reality. The Misjudgment is akin to the decision errors, in which the driver decides on an incorrect action for the given situation. [6]

This publication is structured as follows. Section 2 refers to description of a SOTIF-related misuse scenario. Section 3 outlines the strategy for implementing simulation-based testing of FM. Section 4 addresses the implementation using driving simulator and elaborates on results. Finally, Section 5 presents concluding remarks.

## 2 SOTIF-related misuse scenario

SOTIF-related misuse scenario can be derived from gained knowledge and brainstorming [5]. The methodology for systematically deriving SOTIF-related misuse scenario to support the safety analysis for the system is provided in the ISO 21448 [5]. The scenario shown in Figure 2 is derived to expose the driver to a situation

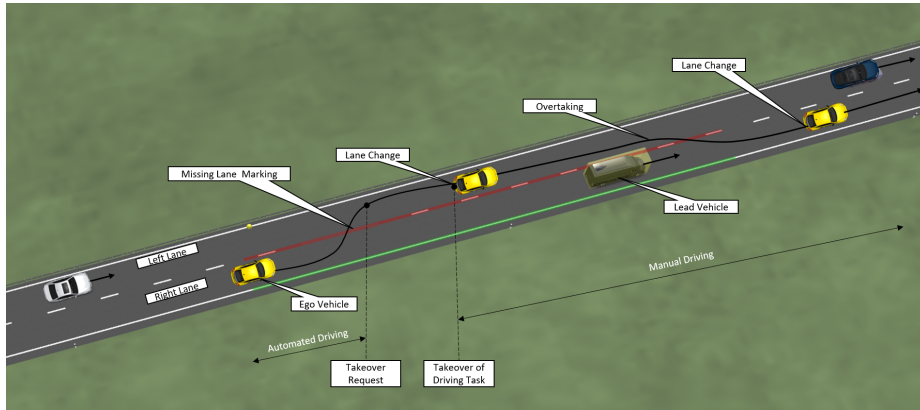


Fig. 2: Highway Lane Change Scenario

requiring transverse guidance that is formed by lateral and longitudinal maneuvering of the Ego-Vehicle in a high-speed highway environment. Ego-Vehicle in the context of this publication is defined as the AV equipped with TGAS. The entire scenario is divided into three maneuvers:

- Lane change from right to left lane

- Overtaking of lead-vehicle from left lane
- Lane change from left to right lane

The Table 1 outlines the derived SOTIF-related misuse scenario considered in this publication conforming to an example methodology given in annex B of ISO 21448 [5]. The DSI that influence the vehicle-level hazard related to FM, namely

Table 1: Description of SOTIF-related misuse scenario

Stake-holder	Foreseeable Misuse (FM)		Driver System Interactions (DSI)
	Factors	Causes	
Driver	Recognition	False recognition	Delayed Take-over
	Judgement	Misjudgement	Take-over & perform Under-steer
Environmental conditions	Potential SOTIF-related misuse scenario	Derived hazardous misuse scenario	
<ul style="list-style-type: none"> <li>– Weather : clear</li> <li>– Light Condition : day-light</li> <li>– Traffic Condition : light traffic</li> <li>– Roadway Surface and Features : missing lane markings</li> </ul>	<p>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.</p> <p>The camera sensor cannot estimate the location of the lane boundary due to a performance insufficiency. Ego-Vehicle starts to leave the lane and driver is notified to take control of the driving tasks by means of TOR.</p>	Driver fails to take-over the control of the driving tasks, resulting in lane departure of Ego-Vehicle.	

lane departure, are considered for deriving a SOTIF-related misuse scenario. Take-over is defined as transfer of the driving control between Human Driver (HD) and the system [7]. Under-steer means the driver fails to provide adequate steering input for the Ego-Vehicle to follow the lane.

### 3 Simulation-based Testing

The strategy depicted in the Figure 3 describes the steps in methodical order to perform simulation-based testing of the SOTIF-related misuse scenario described

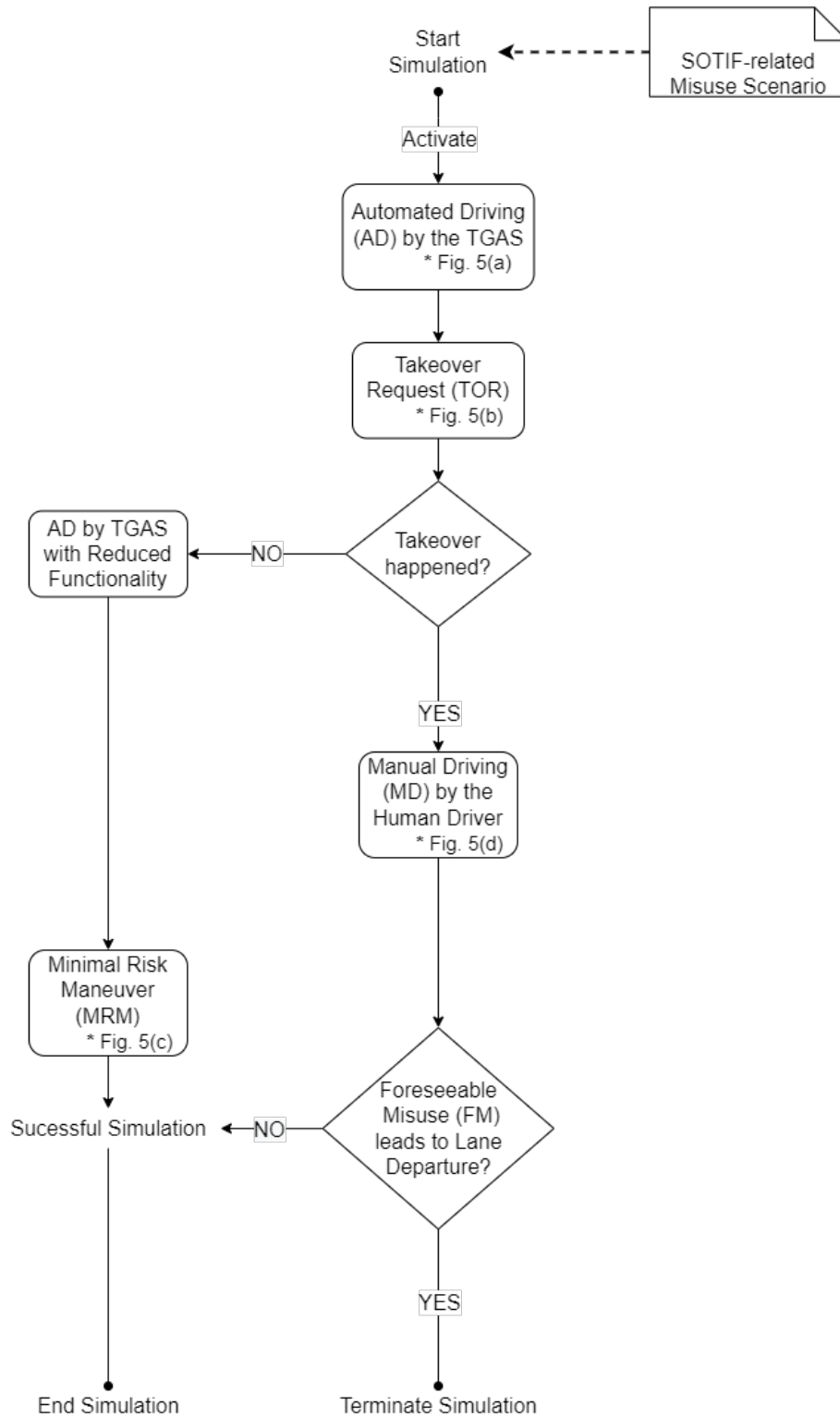


Fig. 3: Simulation-based testing

in Table 1. The scenario and maneuvers is modeled using IPG CarMaker, as per the description given in Section 2. The TGAS performs AD of the Ego-Vehicle by providing lateral and longitudinal control in the modeled scenario. When the system reaches its operational limits, it notify the driver by issuing TOR. Driver take-over at operational limits and the corresponding TOR are not obligatory in HAD [8]. The system is expected to remain operational until the driver is able to regain control [6].

The driver might not be able to take-over driving control within a specified take-over time and FM is expected, attributing false competencies to the system. It may lead to lane departure of the vehicle, addressed as a vehicle-level hazard. If the driver does not take-over the driving tasks in the event of TOR, the system will transition to the AD with reduced functionality. Subsequently, a minimal risk maneuver (MRM) [9] is performed 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 [10]. The driver may be asked to take-over at the end of the MRM.

## 4 Implementation and Results

The simulation-based testing is carried out using a driving simulator as illustrated in Figure 4 allowing driver to control the Ego-Vehicle in the virtual test environment.



Fig. 4: Driving Simulator

The driving simulator is equipped with the hardware tools (Logitech G29-steering wheel, pedals, and gearbox) integrated with a simulation tool (IPG Car-Maker). Likelihood that the driver can cope with the driving situation including operational limits and system failures is determined using the driving simulator. The Driver Vehicle Interface (DVI) as illustrated in the Figure 5 is designed to incorporate the interactions between driver and the system. The DVI design is in concordant with the design guidance provided in [11].

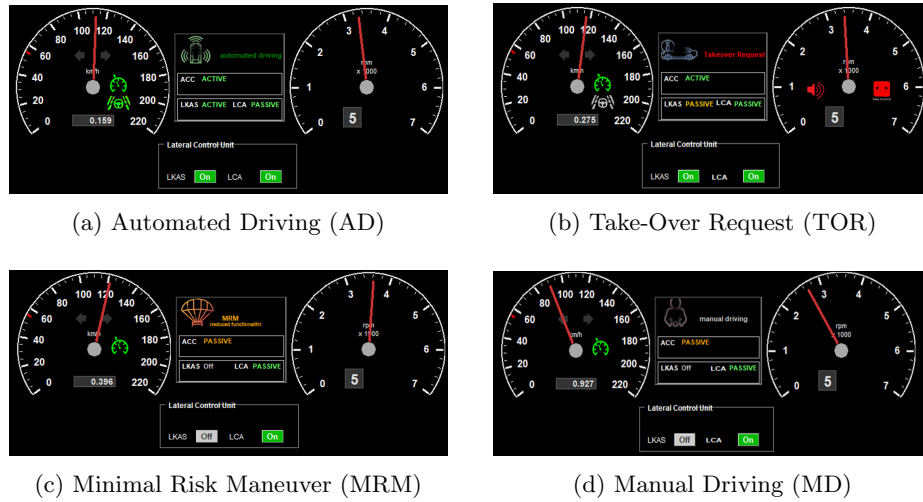


Fig. 5: Implementation of Driver Vehicle Interface (DVI)

Based on literature study pertaining to the design of automated take-over requests in HAD from diverse aspects such as procedure [12], timing [13] and modality [14], the TOR is cued by a combination of an auditory alert and visual notification on the designed DVI. The HD does the take-over of driving control by pushing a button on the steering wheel of driving simulator. It is conceivable that the HD might engage in FM, especially if the HD is convinced that the HAD operates practically flawless [15] and will prevent vehicle-level hazard in the driving environment by choosing safe driving maneuvers [16].

A limitation of the current implementation is the usage of a static driving simulator, where haptic motion cannot be experienced. However, the implemented DVI make it easier to keep the driver's workload at an acceptable level by providing simultaneous auditory alert and visual notification to the driver with supporting information about the system functions and state of operation.



## 5 Conclusion and Future Work

When driving with Highly Automated Driving (HAD), the Human Driver(HD) is allowed to engage in non-driving related tasks. It is reasonable to anticipate higher likelihood of the system misuse [17]. The publication outlines the concept of Foreseeable Misuse (FM) emphasized in SOTIF standard [5] for a described SOTIF-related misuse scenario, illustrated in Section 2, applicable to HAD. An exemplary of the strategy defined for implementing simulation-based testing of FM resulting from system-initiated transition between HD and the system is demonstrated in Section 3. It should be noted that the implementation shown in Section 4 is intended to demonstrate an approach for simulation-based testing of FM rather than to be a distinctive or optimal measure dedicated to mitigate FM. The relevance of this publication is that it adds to the understanding of the factors and causes contributing to FM by incorporating the concepts of DVI & DSI, and applies it to a SOTIF-related misuse scenario.

The fundamental premise is to incorporate and manage all driver and system interactions. The simulation-based testing approach is applied to investigate the factors and mitigate the causes responsible for FM by the driver. The incorporation of DSI and DVI to address FM is briefly described but has not been evaluated. A reasonable next step for future work will be to characterize and quantify the DSI, considering aspects of HD take-over in HAD. Analysing the system specification for inappropriate interactions by the driver is a brainstorming task. One of the possible approach for analysis is System-Theoretic Process Analysis (STPA) which aims to identify the hazardous interactions in the absence of system failures [18]. Identification of factors contributing FM by STPA and effectiveness of the mitigation measures to prevent FM for the described SOTIF-related misuse scenario are suggested for future work. The implication of the proposed method is to exhibit how the concepts of DVI and DSI are interrelated with FM. Recommendations can be made on how, DVI design, TOR presentation modalities, driver improper interactions with system, can be adopted to address the challenges of risks that could impact functionality of HAD.

## References

1. SAE International and On-Road Automated Driving (ORAD) committee, “Sae j3016: Taxonomy and definitions for terms related to on-road motor vehicle automated driving systems,” United States, (revised) April, 2021.
2. Z. Lu, R. Happee, C. D. Cabrall, M. Kyriakidis, and J. C. d. Winter, “Human factors of transitions in automated driving: A general framework and literature survey,” *Transportation Research Part F: Traffic Psychology and Behaviour*, vol. 43, pp. 183–198, 2016. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1369847816304120>
3. N. Merat and J. D. Lee, “Preface to the special section on human factors and automation in vehicles: Designing highly automated vehicles with the driver in mind,” *Human Factors*, vol. 54, no. 5, pp. 681–686, 2012.

4. A. Walker, "Sotif the human factor," in *Systems, Software and Services Process Improvement*, ser. Communications in Computer and Information Science, A. Walker, R. V. O'Connor, and R. Messnarz, Eds. Cham: Springer, 2019, vol. 1060, pp. 575–584.
5. ISO 21448: 2022, "Road vehicles - safety of the intended functionality," Switzerland, 2022-06.
6. 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." [Online]. Available: <https://rosap.ntl.bts.gov/view/dot/53628>
7. ISO/TR 4804:2020, "Road vehicles — safety and cybersecurity for automated driving systems — design, verification and validation," Switzerland, 2020-12.
8. A. Feierle, M. Holderied, and K. Bengler, "Evaluation of ambient light displays for requests to intervene and minimal risk maneuvers in highly automated urban driving," in *2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC)*, 2020, pp. 1–8.
9. M. Wood et al., *Safety First For Automated Driving*, 2019. [Online]. Available: <https://www.apiv.com/docs/default-source/white-papers/safety-first-for-automated-driving-apiv-white-paper.pdf>
10. Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs and GROW.DDG1.C.4, "Guidelines on the exemption procedure for the eu approval of automated vehicles," 2019. [Online]. Available: <https://ec.europa.eu/docsroom/documents/34802>
11. J. L. Campbell, J. L. Brown, J. S. Graving, C. M. Richard, M. G. Lichty, L. P. Bacon, J. F. Morgan, H. Li, D. N. Williams, and T. Sanquist, "Human factors design guidance for level 2 and level 3 automated driving concepts." [Online]. Available: <https://trid.trb.org/view/1574671>
12. S. S. Borojeni, A. Meschtscherjakov, A. G. Mirnig, S. Boll, F. Naujoks, I. Politis, and I. Alvarez, "Control transition workshop: Handover and takeover procedures in highly automated driving," in *Proceedings of the 9th International Conference on Automotive User Interfaces and Interactive Vehicular Applications Adjunct*, ser. AutomotiveUI '17. New York, NY, USA: Association for Computing Machinery, 2017, pp. 39–46.
13. 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.
14. F. Naujoks, C. Mai, and A. Neukum, "The effect of urgency of take-over requests during highly automated driving under distraction conditions," vol. 7, 2014.
15. T. Fuest, A. Feierle, E. Schmidt, and K. Bengler, "Effects of marking automated vehicles on human drivers on highways," *Information*, vol. 11, no. 6, 2020. [Online]. Available: <https://www.mdpi.com/2078-2489/11/6/286>
16. J. Josten, T. Schmidt, R. Philipsen, L. Eckstein, and M. Ziefle, "What to expect of automated driving: Expectations and anticipation of system behavior," in *Advances in Human Aspects of Transportation*, N. A. Stanton, Ed. Cham: Springer International Publishing, 2018, pp. 606–617.
17. N. Schömig, V. Hargutt, A. Neukum, I. Petermann-Stock, and I. Othersen, "The interaction between highly automated driving and the development of drowsiness," *Procedia Manufacturing*, vol. 3, pp. 6652–6659, 2015. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S235197891501121X>
18. B. Kaiser, "Applying stpa in the context of sotif for adas and automated vehicles," ResearchGate. [Online]. Available: <https://www.researchgate.net/publication/351348419>