# VALIDATION OF SAFETY OF THE INTENDED FUNCTIONALITY FOR AUTONOMOUS DRIVING SYSTEMS

**Jihas Khan**
**Chandni Sapna Vijay**
Transportation Business Unit, TATA ELXSI
India

Paper Number: 23-0009

## ABSTRACT

International organisation for standardisation (ISO) safety of the intended functionality (SOTIF) is a relatively new standard that explains the verification mechanism for handling the intended functionality of a system as well as reasonable misuse of the system. It is required to practically implement the ISO SOTIF based validation of advanced driver assistance system (ADAS) and autonomous driving. The objective of this paper is to explain the strategy of virtual simulation and synthetic scenario creation for the validation of ISO SOTIF by taking intelligent speed assistance (ISA) as an example. ISO SOTIF suggested process flow is taken as a reference for the derivation of test strategy by keeping technical and functional safety requirements as the foundation for testing. Hazard identification and risk evaluation are implemented by following the defined standard procedure. Virtual simulation tools are utilized for ISO SOTIF synthetic scenario creation. A scenario elicitation approach is proposed with elaborate examples. A tree diagram with all possible and relevant static and dynamic actors is used for generating scenarios. 'One' or 'two-liner' pseudo scenarios are created first, which are then extended to full-fledged scenario details. These detailed scenarios are then implemented in a virtual simulation tool. The algorithm under test is exposed to these ISO SOTIF scenarios in a SIL / MIL / HIL environment, to evaluate how the system responds to such corner cases. It is also possible to generate additional ISO SOTIF scenarios from the input requirement specification. A few scenarios involving varying environmental conditions and hazard simulation instances are showcased in the paper. The paper explains through real-world examples, on how to do ISO SOTIF based testing for autonomous driving systems. A novel and implementation independent ISO SOTIF validation strategy is proposed in this paper. Use cases of residual risks deemed acceptable are also explained in the paper intuitively. ISO SOTIF validation strategy is studied with intuitive examples.

## INTRODUCTION

Autonomous vehicles are inevitable for a safer future which assures reduced accidents, enhanced driving comfort, and improved efficiency. Ensuring the safety of the vehicles enabled with the autonomous driving feature is of paramount importance [1]. Autonomous driving is implemented using a set of sensors; a combination of electric, electronic, and mechanical systems; and software algorithms. The concept of functional safety considers the risks arising from systematic failures and random hardware failures caused due to technological complexity, software content, and mechatronic systems. These risks can be mitigated by following the guidelines prescribed by the international organization for standardization (ISO) 26262 series [2]. Risks can also arise from outside the conditions considered under ISO 26262 series. Safety of the intended functionality (SOTIF) is the absence of unreasonable risks which arise from the potentially hazardous behaviour caused by functional insufficiencies of the intended functionality applied in the vehicle or by reasonably foreseeable misuse by persons [3].

A detailed standard framework to ensure SOTIF is proposed in ISO/PAS 21448 and is aimed at systems that do not have well-established design, verification, and validation measures. It is intended to be applied to functionalities where comprehending a situation and having awareness of it is essential for safety such as that of an advanced driver assistance system (ADAS) with levels 1 and 2 on the society of automotive engineers (SAE) automation scales [4]. This understanding of a situation arises from different sensors and complex algorithms implemented in the system. ISO SOTIF guides how to conduct appropriate verification and validation of a particularly intended functionality in ADAS, such as adaptive cruise control (ACC), automatic emergency braking (AEB), etc., to reduce any risk or hazards that may arise after its implementation. A detailed flow chart, describing steps aimed at improvement of the intended functionality to ensure safety, is presented in the ISO SOTIF document. One can achieve SOTIF by following through with these definite steps.

One needs to test the intended functionality under different scenarios to improve safety and reach an acceptable risk level. A scenario describes how the surrounding scenes change with time through a series of actions and events from a particular point of view. In an ADAS system, these scenarios are created and formatted specifically

with respect to a functionality for an effective verification result. Figure 1 shows how a scenario can be classified into four distinct areas, based on two aspects which are 'safety level' and 'knowledge about situations'. The goal of ISO SOTIF is to assess the SOTIF in Area 2 and Area 3 and reach an acceptable level of residual risk in the ADAS system.

The probability of encountering known and unsafe scenarios in Area 2 can be reduced by explicitly evaluating specific scenarios. Similarly, for Area 3, the scenario can be evaluated by systematic analysis, dedicated experiments, or by standard industry practices. The vehicle is usually put to test by driving it under specifically designed scenarios. However, manual vehicle-based testing has certain drawbacks such as being costly, complex, not repeatable, and lack of assurance that all possible scenarios are covered such as corner cases, accident cases, etc. Hence, a shift from real vehicle testing to virtual validation in a lab-based environment is the current trend seen for all cases of ADAS feature validation. In this paper, by utilizing virtual simulation, the scenarios are designed and tested for areas 2 and 3 to reduce the residual risk. ISO SOTIF evaluation using virtual simulation for ADAS is an open area of research, which is being conducted here.

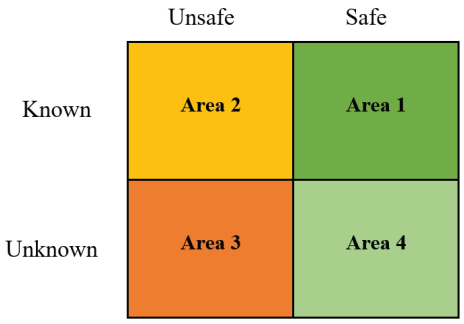



***Figure 1. SOTIF scenario categories.***

Hidetoshi Suhara *et al*. propose an integrated metamodel of test scenarios in [5] to conform to different safety standards including SOTIF. A detailed comparison between different automotive standards was conducted and the authors concluded that the proposed metamodel is the most useful one in describing test cases. The test case descriptions used in the comparison were made using scene, situation, and scenario as defined elaborately in [6]. These definitions were considered in our proposed work for making the test scenarios relating to intelligent speed assistance (ISA). The authors in [7] analyzed driving statistics and accident databases which led to the conclusion that the definition of test scenarios based on statistical data alone is insufficient. This led to the formulation of a requirement list, intended for scenario selection relating to the validation of SOTIF. The first requirement, mentioned in the paper, to use known properties of the road was incorporated while selecting scenarios specific to ISA. A Rulebooks framework showcases a set of pre-defined logical rules that leads to the choice of preferred trajectories for an autonomous vehicle [8]. It can help in identifying specific unsafe scenarios to speed up the validation process. Although integrating the framework with SOTIF method alone is not sufficient to demonstrate safety, the authors believe it offers an important step towards fulfilling the recommendations of ISO/PAS 21448.

The effectiveness of SOTIF can be seen in [9] where the implementation of an improvement in the safety of an autonomous logistics robot by following the SOTIF process led to the identification of hazards and triggering events. After identifying the risk factors, methods to reduce them were implemented with the help of SOTIF's suggested process flow by the authors. Similarly, SOTIF is proven to be efficient in [10] where SOTIF analysis based on system theory process analysis (STPA) was done for obstacle avoidance function, resulting in a more efficient refinement of the safety requirements. STPA method focuses on finding unsafe control behaviour that causes danger in a vehicle, identifying its root cause, obtaining, and refining the safety constraints to obtain safety needs.

Automated driving systems must consider a variety of driving scenarios that would comply with SOTIF. Work done by Max-Arno Meyer *et al*. [11] also shows the effectiveness of SOTIF where the validation and verification procedure suggested by ISO SOTIF was conducted to find out the hazards and triggering conditions in a car parking functionality. Model-based systems engineering (MBSE) is becoming increasingly important for the development of automotive applications as it is an enabler for complex system and test design. The authors address the issue that the common procedures involved in MBSE are neither scenario-based nor do they consider SOTIF.

MBSE was re-designed by including scenario-based system engineering, which is compliant with SOTIF, which led to achieving full traceability between scenarios and system requirements.

The objective of this paper is to showcase how virtual simulation and scenario creation can be utilized for the validation of SOTIF. The existing challenges addressed in this paper are:

- A standardized approach for scenario creation is not stated precisely in literature.
- A strategy for validation of ISO SOTIF using virtual simulation has not been defined yet.
- An ambiguity on how model-in-the-loop (MIL)/ software-in-the-loop (SIL)/ hardware-in-the-loop (HIL) testing based on ISO SOTIF can be done in virtual space is found.

To address these challenges, this paper is proposing certain novel contributions which are listed below.

- A standardized approach for scenario creation in ADAS is proposed.
- A testing and validation strategy using virtual simulation is derived by considering the ISO SOTIF suggested process flow.
- An approach to MIL testing based on ISO SOTIF using virtual simulation is derived.

ISA prevents drivers from exceeding the speed limit on a particular lane by detecting the road signs placed using a camera or by taking in information from global positioning system (GPS) linked speed limit databases [12]. It is a safety technology aimed at enabling safe driving and thus reducing the chances of an accident. Taking ISA as an example to depict the process flow for the improvement of intended functionality as described in ISO SOTIF, relevant scenarios were developed by using software tools such as RoadRunner® [13], Unreal® Engine [14], and MATLAB® [15]. Even though the ISA feature is taken as an example in this paper, the concepts and strategies derived here can be similarly extended to any ADAS feature. The standard approach for scenario creation for ADAS validation is proposed in the following section.

## SCENARIO CREATION

Various scenarios are required to validate ADAS algorithms in virtual space. It is essential to make sure that we have enough quantity and quality of scenarios that can cover the entire functional space of the ADAS algorithm under test. To ensure that all situations are taken into consideration for verification and validation of the algorithm, a definite approach to scenario creation is of necessity. Here, a process flow consisting of five steps for scenario creation is suggested as shown in Figure 2. The first step involves creating a tree diagram that captures all relevant stakeholders in that feature. Choosing a specific feature, the necessary and possible characteristics to create a scenario are considered to construct the tree diagram.

The next step for scenario creation is making a pseudo scenario which is a one or two-liner description of a scenario that captures its basic essence. The third step involves developing a detailed scenario description from the pseudo scenario, which encompasses all relevant elements. The unique scenario thus derived is then subject to the variations of specific actors and/or their behaviour. The final output comprises unique and variation scenarios, which are at a level where implementing virtual simulation is made easier. The final step involves creating the virtual scenario using a virtual simulation tool (e.g. RoadRunner®) as per the detailed scenario description derived in the last step.

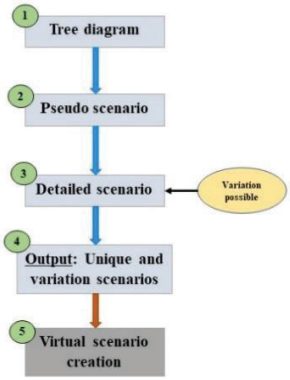



***Figure 2. Steps for scenario creation.***

In this paper, as the focus will be on testing and validating the ISA functionality, the process flow for scenario creation as mentioned in Figure 2 is followed for making the test case scenarios. Following step 1 of scenario creation, Figure 3 shows the tree diagram intended for ISA with some elements such as static and dynamic actors, environmental conditions (road surfaces and scene illumination level), ego vehicle (EV) behaviour, and situational components (bridges and lane details).

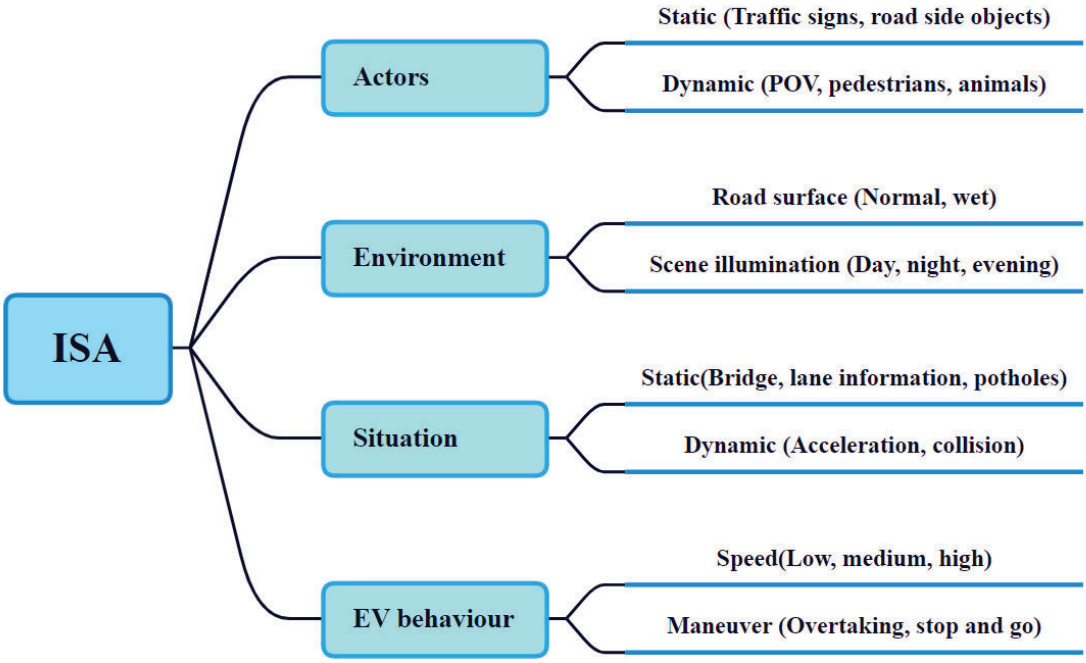



***Figure 3. Tree diagram for scenario generation.***

The development of a pseudo scenario, relating to ISA, by using the tree diagram is shown below. Following the second step in the scenario creation flow chart, a pseudo scenario consisting of EV and principle other vehicle (POV) is first created, as shown in Table 1.

***Table 1.***
***Pseudo scenario***

| Category | Pseudo scenario |
|---|---|
| ISA | EV moving on a highway at 80km/h where another POV is present in the vicinity, with a speed limit sign placed ahead. |

Next, a detailed scenario description (step 3) is derived. Here, the scenario is created such that the ISA functionality of the EV can be tested to see if it can detect the road sign indicating the speed limit and alert the driver. The detailed scenario description, as shown in Table 2, consists of pre-conditions that the scenario needs to have along with the steps to be followed during the execution of this scenario. The expected outcome is also expressed in the detailed description of the scenario.

*Table 2.*
*Detailed scenario*

| Test case description | Pre-condition | Steps/Command | Expected |
|---|---|---|---|
| EV is travelling on a four-lane straight road, approaching the speed limit sign. | 1. A track of four-lane straight road with a POV in the same lane.<br>2. Traffic sign board present at 200m from origin indicating the speed limit of 40km/h.<br>3. Length of straight road is 1km. | 1. EV travelling at 60km/h.<br>2. POV present ahead of EV moving at speed of 35km/h. | EV shall detect the speed limit sign and reduce speed accordingly while keeping a safe distance from the POV. |

Different variations of the above scenario description can be created (step 4) by varying parameters like:

1. Velocity of EV
2. Speed limit value on the traffic sign
3. Velocity of POV
4. Number of lanes
5. Environment conditions
6. Time of the day

From the specifics obtained from the detailed scenario description, a virtual scenario is created using RoadRunner® (step 5) as shown in Figure 4.


***Figure 4. Virtual scenario created for ISA.***

After creating the needed scenarios, the verification and validation strategy proposed in ISO SOTIF needs to be tested for the intended functionality which is discussed in the next section.

## VERIFICATION BASED ON ISO SOTIF

The safety of the intended functionality implemented in any ADAS system is increased by following through the steps described in the flow chart as shown in Figure 5. The execution of these steps is discussed in detail in this paper.

### Functional Specification

The process starts by describing the functional and system specification needed for the specified functionality which is step number 5 highlighted in Figure 5. It needs to have all the information necessary to initiate the SOTIF related activities. As an example:

ISA functionality uses a front-facing camera to detect the road signs ahead on the road and learn the speed limit. If it detects that the velocity of the EV is more than the detected speed, ISA acts by reducing the velocity of the EV accordingly.

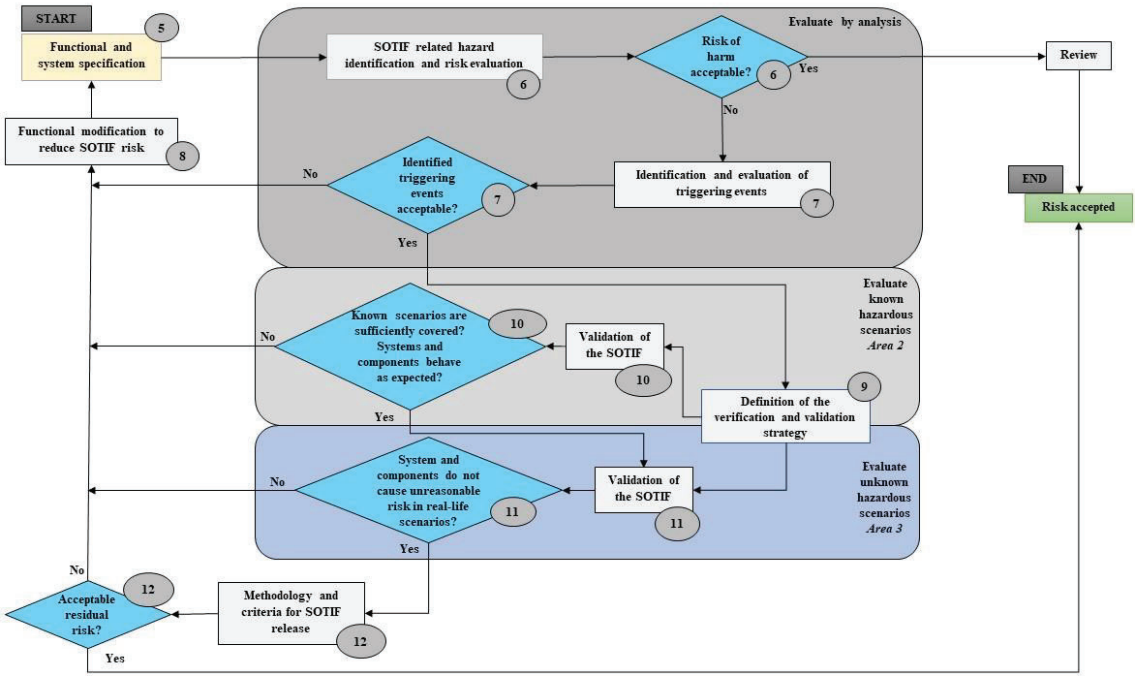



***Figure 5. ISO SOTIF flow chart.***

**Hazard Identification and Risk Evaluation**

After defining the system specifications, it is essential to identify hazardous events which are a combination of a hazard caused by a malfunction and a specific operational situation. Evaluating the risks involved in the identified hazards is also important. This leads to the next step in the SOTIF flow chart, which is hazard identification and risk evaluation (step 6) wherein we identify the potential hazardous events caused by functionality or by reasonably foreseeable misuse of the function by a user and evaluate the risks involved in these events. Having knowledge about the function and its potential deviations is the key to identifying a hazardous event. This hazard identification can be done by following through the methods proposed in ISO 26262 which are illustrated in Figure 6, using ISA as an example. A known situation that can affect ISA and its potential hazardous behaviour are described briefly below. This situation is taken for describing a known triggering event for hazard analysis.

Traffic situation: Driving with ISA active. Few vehicles present around.

Potential hazard: Unwanted speed adjustment could lead to a collision with other vehicles.

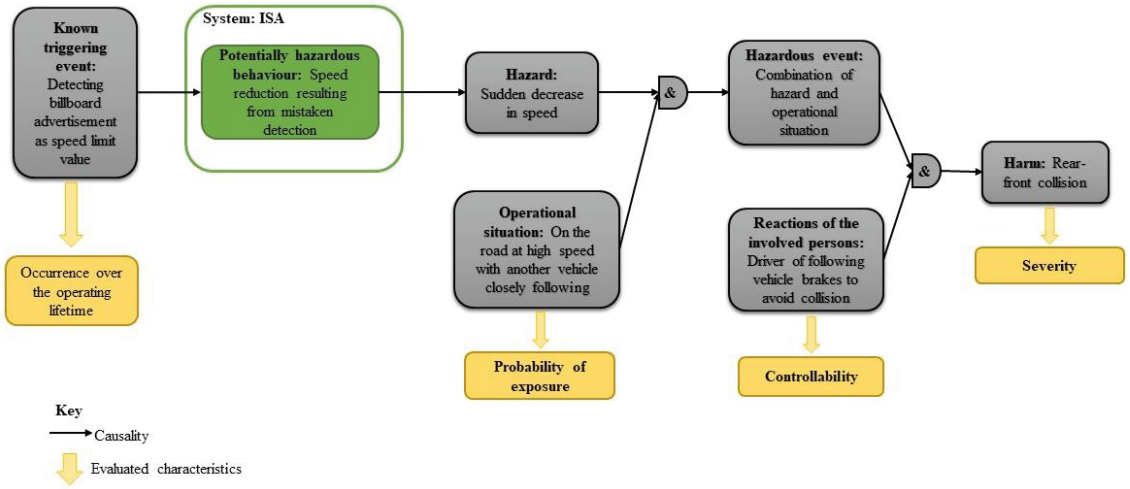



***Figure 6. Hazard analysis of ISA according to ISO 26262.***

After identifying the possible hazards, the question arises if the risk of harm is acceptable or not (step 6). From the hazard analysis done, the severity of potential harm and controllability of hazardous event involved in the known triggering event are derived to determine the credibility of the resulting harm (risk evaluation). To analyse the risk acceptability level, the severity and controllability level are measured according to ISO 26262 which is depicted in Table 3. There is a possibility that the driver of the EV will rely on the functionality and not be quick enough to adjust the faulty speed value to avoid a rear collision with the trailing vehicle. It is understood from the severity classes and controllability classes defined in ISO 26262 that the severity and controllability of the identified hazardous event are not S0 (no resulting harm) and C0 (controllable in general), which is the condition for the risk to be acceptable. This is summarised below:

| Risk not acceptable. Driver might rely on the function and be unable to take control of the vehicle in time. |
|---|

***Table 3.***
***Hazard analysis***

| **Hazardous event** | **Potential consequence** | **Severity** | | **Controllability** | |
|---|---|---|---|---|---|
| | | **Rating** | **Note** | **Rating** | **Note** |
| Unintended ISA activation to reduce speed from x m/s to y m/s while operating on a highway. | Rear collision with the following vehicle. | S>0. | Effective impact speed: v ≥ x km/h. | C>0. | The following vehicle might not be quick enough to avoid a rear collision. The driver of EV might not be able to take control of speed in time. |

.

**Identification and Evaluation of Triggering Events**

Since the acceptability of risk of harm fails, next step, which is identifying and evaluating the triggering events (step 7) for such a hazard, is performed. Analysis of triggering events deals with identifying the system weaknesses that involve the decision algorithm, sensors; and identifying relevant scenarios that could lead to the hazard mentioned above. Here, a triggering event relating to sensor functionality is mentioned as follows:

| Triggering event: Misreading of sign boards on road. |
|---|

False detection of road signs can lead to unwanted speed adjustment. The identified triggering event is evaluated as per the criteria specified in risk identification and evaluation. It is likely to occur according to the exposure level identified (E>0) using ISO 26262. The triggering event is not deemed acceptable as the probability of the system causing this hazardous event is not lower than the target value taken for validation (E0). It leads to the following conclusion:

> Triggering event is not acceptable. The controllability of the function by the driver needs to be ensured.

To reduce the SOTIF risk, the following functional modification is implemented (step 8). The detected speed value is crosschecked with the value available from high-definition (HD) map. In the case of a mismatch, an alert is sent to the driver, through a human-machine interface (HMI), to take over the speed control and adjust the speed accordingly. This is briefly depicted below:

> Functional improvement: Driver to be advised to take over speed control in case of a speed mismatch.

**Definition of Verification and Validation Strategy**

After modifying the functionality of the ISA feature, the entire process is repeated (steps 5 – 7), to ensure that the risks are minimised. The system specifications and functionalities are appropriately updated. The triggering events are analysed again resulting in an acceptable risk condition.

> SOTIF related risk is acceptable.

This leads to the next important step, defining the verification and validation strategy (step 9). The strategy is defined such that it supports the reasoning of SOTIF. The validation strategy is integrated with different testing activities so that the following factors are addressed within its scope: ability of the sensor functionality, the efficiency of the decision algorithm implemented for the speed adjustment, the effectiveness of the HMI interface, and how effective the overall functionality of the feature is? This involves creating different test cases based on the clauses mentioned below:

> Definition of test cases for evaluating the ISA function based on Clause 9 and Clause 10 of ISO SOTIF standard.

**Validation of the SOTIF (Area 2)**

It is necessary to validate the SOTIF by taking known and unknown scenarios separately. This section focusses on the known hazardous scenarios. A test case relating to the analysis of triggering events, which is based on Clause 9 (Table 4, Method N) of the ISO SOTIF standard, is taken for verification and validation, as depicted in Figure 7 (step 10 of ISO SOTIF flowchart). This is described briefly below:

> The EV is travelling at 100km/h with a POV closely following behind. When the vehicle approaches the billboard, the number which indicates the number of lives saved, is falsely detected as a speed limit value. This difference in speed is analysed by the ISA using HD map speed values assigned for each road lane. An alert message indicating this is sent to the driver.


***Figure 7. Detection of billboard by white EV with ISA functionality followed by a red POV.***

Testing using selected SOTIF relevant use cases and scenarios based on Clause 10 (Table 5, Method F) is also performed. The ability of the ISA to detect the road sign in foggy weather conditions and the ability to detect a road sign at night are evaluated for known scenario testing (step 10). Brief descriptions of the test cases are given below:

| |
|---|
| EV is travelling on a foggy road where a road sign indicating the speed limit is placed nearby as shown in Figure 8. |

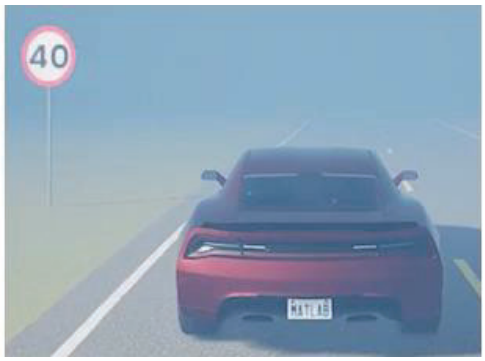



***Figure 8. Detection of speed sign by ego vehicle on a foggy road.***

| |
|---|
| EV is travelling on a highway during the night where a speed limit sign is seen as shown in Figure 9. |

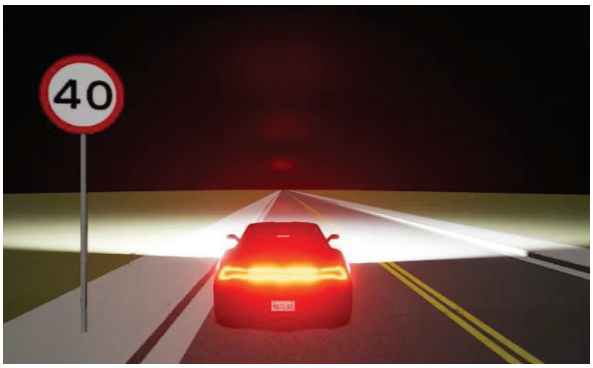



***Figure 9. Detection of speed sign during the night by ego vehicle.***

Increasing driver awareness can be realized due to the warnings made from the functional modification. Evidence of sufficient controllability can be seen from the simulation of different test cases. Next, the question arises if known scenarios are sufficiently covered and if the system and components behave as expected. This is answered conclusively from the test cases developed with the help of the clauses mentioned earlier. A similar analysis is done for Area 3 as well.

**Validation of the SOTIF (Area 3)**

After ensuring that all possible known test cases are covered and that the system behaves optimally, we move on to verifying the unknown situations (step 11). This involve long-term vehicular tests, randomised tests, and analysis of worst-case scenarios. These tests are run based on a knowledge-based driving database to prove controllability in further (unknown) scenarios. Next, we ensure through these tests that the system and components do not cause unreasonable risk in real-life scenarios (step 11) by comparing with the target values and using the GAMAB (*in French* "globally at least as good") principle. The outcome of these tests is as shown below:

| Risk level complies with GAMAB principle. |
|---|

GAMAB principle ensures that the residual risk relating to the safety of any new system is not higher than that of existing systems with comparable functionality and hazards.

**Methodology and Criteria for SOTIF Release**

For the SOTIF release (step 12), a methodology is proposed in the standard where all the information obtained from carrying out the different steps in the flow chart and the acceptability of the residual risk involved are evaluated. This information collected is reviewed against a set of questions which helps in answering the question: if SOTIF release is possible or not? The questions formulated check whether relevant test cases coming under the scope of the functionality are considered for validation or not?; whether the intended functionality achieved minimum risk conditions?; and whether the needed validation and verification strategies are met in order to have confidence that the risk is not unreasonable? Following the methodology proposed in SOTIF, a recommendation about the SOTIF release is obtained. If the conditions in the methodology are met, we come to the end of the SOTIF testing process and move on to its release.

As part of SOTIF verification, MIL system testing for the ISA functionality is implemented in this paper which is described in detail in the next section.

**MIL SYSTEM TESTING**

MIL testing is a technique utilised for testing single or multiple systems in a model-based development environment such as MATLAB Simulink® from MathWorks®. As shown in Figure 10, Simulink® blocks are utilised and simulated in a closed loop to correct the ego vehicle velocity in accordance with the detected speed limit sign.

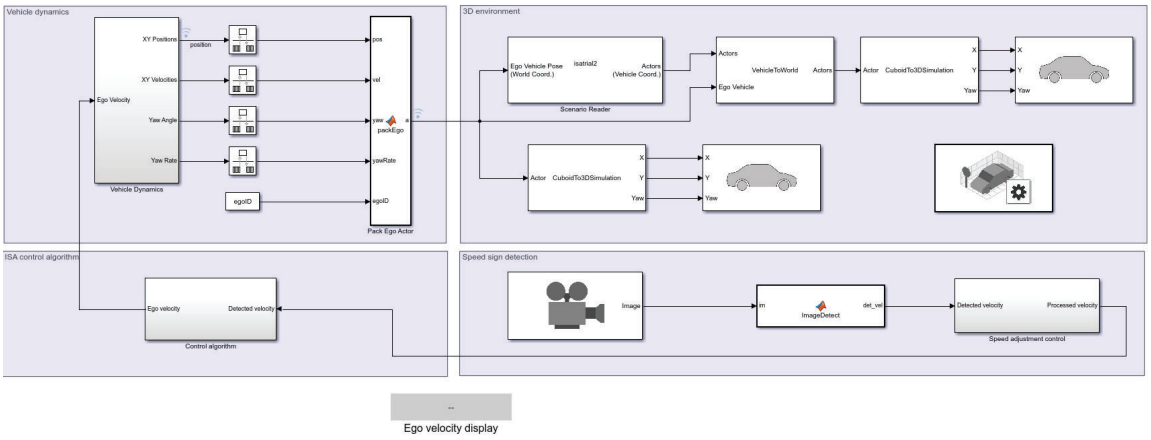
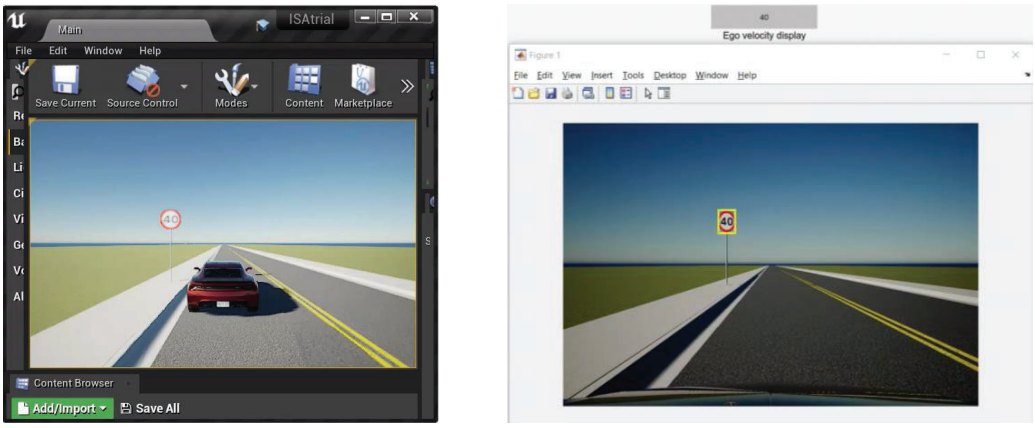



***Figure 10. Simulink model of ISA.***

The ISA Simulink model proposed in this paper consists of a vehicle dynamics block, a 3D simulation block, a speed sign detection block, and an ISA control algorithm block. The vehicle dynamics block computes properties like position, velocity, and heading of EV based on certain mathematical computations. A scenario comprising a road network and a traffic speed limit sign is designed using RoadRunner® and is visualized using the 3D simulation block. The traffic speed limit sign is detected and passed on to the control algorithm block using the speed sign detection block. The control algorithm section of the proposed model is responsible for sending the appropriate ego velocity value to the vehicle dynamics. This functionality works in a closed loop throughout the model execution.

The necessary scenario is simulated in Unreal Engine® as shown in Figure 11. The speed limit value of 40km/h is detected successfully from the sign. It is also compared with the allowed speed defined in the HD map for the specific road lane. This is then sent to the control algorithm, where a comparison between the detected value of 40km/h and the EV velocity value of 60km/h is done. A new EV velocity value of 40km/h is sent to the vehicle dynamics block and the EV velocity is corrected accordingly. This completes the MIL testing. The replacement of the control algorithm block with the code generated from it and testing it in a simulation environment is called SIL testing. For HIL testing, the generated code from the control algorithm is flashed in to a microcontroller based electronic control unit (ECU). The environment, scenario, sensor model, vehicle dynamics, etc. shall be modelled and compiled to generate code, which will run in real time inside a HIL simulator. There will be real-time closed-loop communication between the ECU and the HIL simulator. Thus, ECU believes that it is actually sitting inside a real vehicle and the HIL testing of the ECU is conducted in such a manner.




*(a)* *(b)*

***Figure 11. (a)Visualization of created scenario (b)Perception from the camera with detection overlay.***

## CONCLUSION

This paper explains how ISO SOTIF based virtual testing can be implemented for autonomous driving systems through real-world scenario examples. The process of scenario creation using a tree diagram, development of a pseudo scenario from the tree diagram, and developing a detailed scenario from the pseudo scenario were described in detail. Simulation and virtual space were used for the explanation of the validation concept of ISO SOTIF. Different scenarios relevant to ISA were implemented and MIL-based system testing for ISA was successfully demonstrated. The method on how to extend the same validation concept to a real-world/real vehicle situation can be taken up for future scope or development.

## ACKNOWLEDGEMENT

We would like to extend our gratitude to MathWorks® and Epic Games® for their software tools which were utilised to implement the research conducted in this paper.

## REFERENCES

[1] Margarita Martínez-Díaz, Francesc Soriguera, “Autonomous vehicles: theoretical and practical challenges”, Elsevier, XIII Conference on Transport Engineering, CIT2018, Transportation Research Procedia 33 (2018) 275–282.

[2] ISO 26262-3, “Road vehicles – Functional safety”, International Organization for Standardization, Tech. Rep., 2018, ISO 26262-3:2018(E).

[3] ISO/PAS 21448, “Road vehicles — Safety of the intended functionality”, International Organization for Standardization, Tech. Rep., 2019, ISO/PAS 21448:2019(E).

[4] SAE, “Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles”, Surface Vehicle Recommended Practice, J3016, 2021.

[5] Hidetoshi Suhara, Yasuharu Nishi, “An Integrated Metamodel of Test Scenario to Conform Automotive Standards”, IEEE International Conference on Software Testing, Verification and Validation Workshops, Porto, Portugal, Oct. 2020.

[6] Simon Ulbrich, Till Menzel, Andreas Reschka, Fabian Schuldt, and Markus Maurer, “Defining and Substantiating the Terms Scene, Situation, and Scenario for Automated Driving”, IEEE International Conference on Intelligent Transportation Systems, Gran Canaria, Spain, Sep. 2015.

[7] Oleg Kirovskii, "Determination of Validation Testing Scenarios for an ADAS Functionality: Case Study", SAE Technical Paper, 2019-01-0137, 2019, doi:10.4271/2019-01-0137.

[8] Anne Collin, Artur Bilka, Scott Pendleton and Radboud Duintjer Tebbens, “Safety of the Intended Driving Behavior Using Rulebooks”, IEEE Intelligent Vehicles Symposium, 2020.

[9] Kyoung Lak Choi, Min Joong Kim, Young Min Kim, “On Safety Improvement through Process Establishment for SOTIF Application of Autonomous Driving Logistics Robot”, International Journal of Internet, Broadcasting and Communication, Vol.14, No.1, 209-218, 2022.

[10] Kuang Xiaojun, Zhang Yafei, Li Hongpeng, “SOTIF Requirement Analysis Based on STPA”, International Conference on Algorithms, Computing and Artificial Intelligence, ACM, Article No.: 44, Pages 1–5, https://doi.org/10.1145/3508546.3508590, Dec. 2021.

[11] Max-Arno Meyer, Sebastian Silberg, Christian Granrath, Christopher Kugler, Louis Wachtmeister, Bernhard Rumpe, Sébastien Christiaens and Jakob Andert, “Scenario- and Model-Based Systems Engineering Procedure for the SOTIF-Compliant Design of Automated Driving Functions”, IEEE Intelligent Vehicles Symposium, Aachen, Germany, Jun. 2022.

[12] ACEA - European automobile manufacturers association, “Road safety – Safe vehicles, safe drivers, safe roads”, 2019.

[13] https://in.mathworks.com/products/roadrunner.html

[14] https://www.unrealengine.com/en-US/

[15] https://in.mathworks.com/

**Identifying Effective *STPA Control Structures to Characterize SOTIF Areas 1,2,3, and 4 in Automated Vehicles.***

**Xuezhu, Yang**

**Zhongju, Di**

China FAW Corporation Limited

China

**Juan Pimentel**

**Rolf Johansson**

**Greg Gruska**

OMNEX (US) Co. Ltd

US

**Ruoyu, Xu**

**Fu, Xu**

OMNEX (Shanghai) Co. Ltd

China

Paper Number 23-0019

## ABSTRACT

Developing and automated driving system (ADS) for an automated vehicle with a sufficient level of safety has turned out to be a much more difficult problem than anticipated by the industry. The challenges are multiple, for example the existence of a very large number of critical scenarios that would require testing vehicles for billions of miles to guarantee safety. In this paper we propose using System Theoretic Process Analysis, STPA, to characterize SOTIF areas 1, 2, 3, and 4 for SAE automation levels 3 and 4. A key challenge of STPA is the identification of an appropriate dynamic control structure that is efficient for the purpose at hand. We propose a control structure built around the decision hierarchy of strategical, tactical, and operational decisions, used to structure an ADS including its relations to the user, the environment, and all other traffic actors. More specifically, we show how an analysis based on this control structures at the strategic, tactical, and operational levels can be used to identify safe and unsafe control actions (UCAs) in known scenarios

## INTRODUCTION

It is widely accepted that an automated driving system (ADS) operates in a very complex environment and this one of the reasons why commercial deployments of safe autonomous vehicles has turned out to be much more difficult than expected. Currently there is a international standard ISO 21448, also called the Safety of the Intended Functionality (SOTIF), that addresses the safety of the intended functions of ADSs [1]. An ADS operates in a wide variety of scenarios which must be carefully characterized for a variety of purposes, e.g., conceptual design, implementation, testing, verification, validation, etc. [2]. Depending upon whether scenarios are known or unknown and whether such scenarios cause hazardous behaviour or not, SOTIF classifies scenarios into four areas called Area 1 through Area 4. Safety analysis of each of the SOTIF areas helps determine whether an ADS design has an acceptable level of risk. Recently, there has been much work on system theoretic process analysis (STPA) as a safety analysis method in various contexts, including SOTIF [3-7]. One important step of the STPA method involves the development of control structures [8]. In this paper we identify an effective STPA control structure that would prove useful for the

SOTIF safety analysis of Areas 1, 2, 3, and 4 in the context of an ADS project involving a highway pilot (HWP) feature of an SAE level 3 automation system as defined in the standard SAE J3016 [9]. This paper focuses on the STPA control structure while a future paper will address the safety analysis of SOTIF areas 1,2,3, and 4 based on the proposed control structure.

The contributions of this paper are as follows: a) the development of a detailed STPA control structure that is hierarchical in nature taking into account the three levels specified by the SAE J3016 standard namely the strategical, tactical, and operational control levels, b) a set of unsafe control actions which were identified for the control structure, and c) a discussion on the effectiveness of the STPA Control Structure to characterize SOTIF areas 1,2,3, and 4.

**A. The SAE J3016 Automation and Hierarchical Control Levels**

The SAE J3016 document [9] defines 6 levels of automation that are possible in terms of the performance of lateral and longitudinal automation, the monitoring of the driving environment, the fallback when automation fails (also called the DDT (dynamic driving task) fallback) and the scope of the ODD (operational design domain):

- Level 0 (No automation). As the name implies, at this level there is actually no automation.
- Level 1 (Driver assistance). At this level there is either lateral or longitudinal automation (but not both). A driver monitors the driving environment and must be ready to take over when automation fails. The ODD is limited.
- Level 2 (Partial automation). At this level there is both lateral and longitudinal automation. A fallback driver monitors the driving environment and must be ready to take over when automation fails. The ODD is limited.
- Level 3 (Conditional automation). At this level, the ADS provides lateral and longitudinal automation and in addition it monitors the driving environment. A user must be ready as a fallback when automation fails. The ODD is limited.
- Level 4 (High automation). At this level, the ADS provides lateral and longitudinal automation, it monitors the driving environment, and acts as a fallback when automation fails. The ODD is limited.
- Level 5 (Full automation). At this level, the ADS provides lateral and longitudinal automation, it monitors the driving environment, and acts as a fallback when automation fails. The ODD is unlimited.

While discussing the DDT, the J3016 document makes reference to a three-level control schematic shown in Fig. 1 consisting of three levels: strategic, tactical, and operational [9].

According to J3061, the DDT includes the following sub-tasks:

1. Lateral vehicle motion control via steering (operational).
2. Longitudinal vehicle motion control via acceleration and deceleration (operational).
3. Monitoring the driving environment via object and event detection, recognition, classification, and response preparation (operational and tactical).
4. Object and event response execution (operational and tactical).
5. Maneuver planning (tactical).
6. Enhancing conspicuity via lighting, sounding the horn, signaling, gesturing, etc. (tactical).

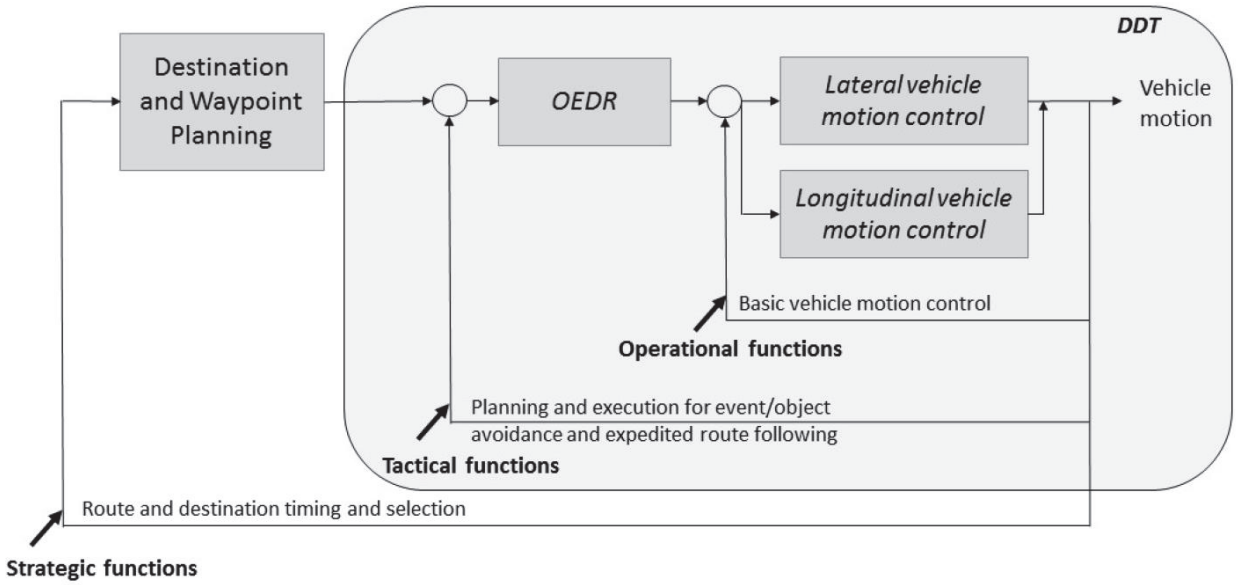



***Figure 1. Schematic view of the driving tasks of a DDT per SAE J3016.***

To enable a DDT with a sufficient level of safety and performance, appropriate models are necessary that include:

1. Models of the driving environment
2. Models for DDT fallback
3. Models for object and event detection, recognition, classification, and response preparation
4. Models for object and event response execution
5. Models for maneuver planning

In this paper, we provide a specific model of the driving environment in the context of a J3016 based hierarchical STPA control structure. We use the control structure together with the driver environment model (DEM) to perform hazard analysis and to identify SOTIF areas 1 and 2 and to provide an in-depth analysis of areas 3 and 4. Although not explicitly addressed, this paper provides discussions on a few aspects of the other models 2 through 5 in the above list.

**B. SOTIF Areas**

The SOTIF standard DIS ISO 21448 [1] classify scenarios into four categories as depicted in the left side of Fig. 2 where only Areas 1 and 2 are known and only Areas 2 and 3 are hazardous. According to this draft international standard, the areas are conceptual abstractions representing a goal of the SOTIF process, which is to:

- Perform a risk acceptance evaluation of Area 2 based on the analysis of the intended functionality.
- Reduce the probability of known scenarios causing hazardous behavior, in Area 2, to an acceptable level of risk.
- Reduce the probability of the unknown scenarios causing potentially hazardous behavior, in Area 3, to an acceptable level of risk.

The presence of unreasonable risk might be evident at the beginning of the development, visualized by too large Areas 2 and 3. The ultimate goal of the SOTIF activities is to evaluate the potentially hazardous behavior present in Areas 2 and 3 and to provide an argument that these areas are minimal, i.e., at or below acceptance criteria, and therefore the residual risk caused by these scenarios is sufficiently low.

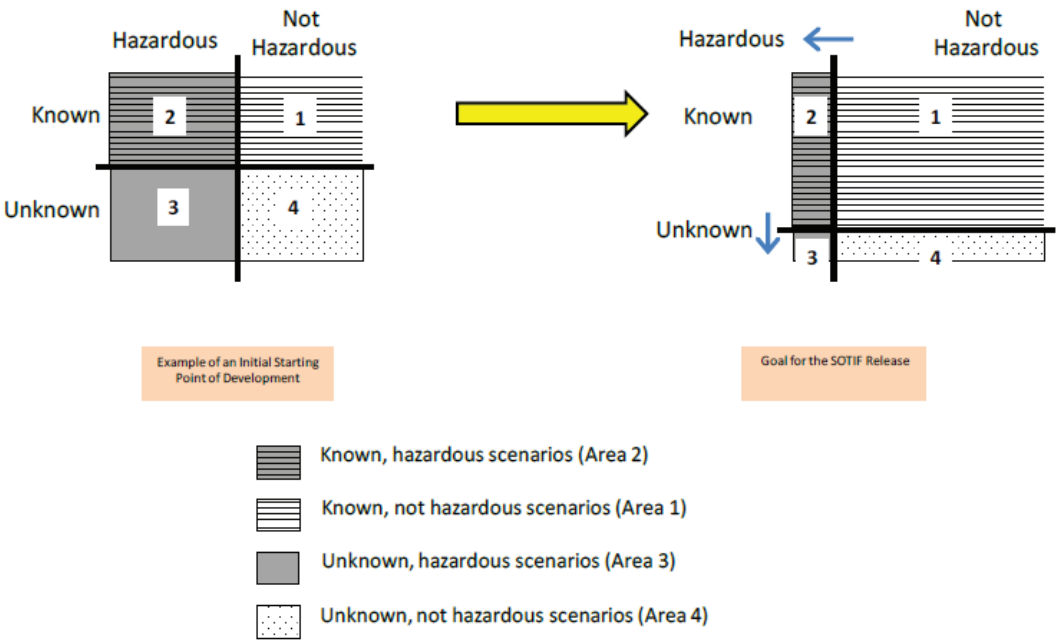



***Figure 2. SOTIF areas and its evolution resulting from the ISO 21448 activities.***

**C. The STPA process**

System theoretic process analysis (STPA) is a safety analysis framework based in control system theory with applications in many industrial areas including automotive. The STPA process consists of 4 steps [8]:

- Step 1. Define the purpose of the analysis
- Step 2. Model the control structure
- Step 3. Identify unsafe control actions (UCAs)
- Step 4. Identify loss scenarios

In step 1, the system under design is characterized as much as possible. Being a framework based on control systems theory, specific control structures are modeled in step 2. Based on the specific control structures the STPA process models hazards as unsafe control actions which are outcomes of the various controllers in the control structure. In step 4, the fundamental question as to how is it possible for the controllers to generate UCAs is answered through the identification of causal factors in the context of specific scenarios. This paper only focuses on STPA steps 2 and 3.

**The STPA Hierarchical Control Structure**

When using methods such as STPA for hazard analysis in an ADS development process, it is important to introduce structure as a means to deal with such complex environment. This structure needs to be detailed enough to enable the capture of what is required by SOTIF; examples of such detail include triggering conditions, insufficiency of specification, performance limitations, and reasonably foreseeable misuse. The structure discussed in this paper is the STPA control structure which is an important step of the STPA process.

In addition to structuring the control, an STPA control structure can be also used to structure additional entities such as:

- Hierarchical control levels
- Information and control flows
- Feedback control loops
- Loss scenarios
- Functional insufficiencies
- Misuse
- Refined hazards

- Safety requirements
- Test scenarios [10]

Furthermore, we need to reduce the scope of the complex environment to only cover what is strictly necessary for the feature in question, e.g., highway pilot. This reduction in scope and complexity will limit, among other things, the number of scenarios and this will enable to perform a more complete safety analysis of the ADS and in turn to characterize SOTIF areas 1, 2, 3, and 4 more precisely.

The implication for an ADS is that on the one hand, the very complex environment including the driver needs to be captured in the control structure, such that the interaction with other traffic actors can be covered. On the other hand, the STPA control structure should also capture the essence of what it takes to act autonomously in the context of the overall driving environment including the main actors such as an operator, a fallback ready user, and other vehicles.

The proposed STPA control structure (i.e., step 2 of the STPA process) is shown in Fig. 3. As depicted in this Fig., in addition to including the hierarchical levels of J3016, the developed STPA Control Structure includes a detailed driving environment model (DEM) to be described in a future paper. Such model will enable a detailed safety analysis with the goal of an accurate characterization of known and unknown scenarios (SOTIF areas 1 to 4). Furthermore, the STPA control structure includes information related to the sensors and perception system, the control algorithms, the actuators, and the controlled process. For clarity, only a few examples of control actions and feedback are depicted in Fig. 3. Note that the controlled process includes the ego vehicle and the physical and driving environment.

Information from the physical and driving environment is captured by appropriate sensors external to the vehicle as part of a perception system composed of cameras, radars, Lidars, IMU (inertial measurement unit) and ultrasonic sensors. The output of these sensors are inputs to a perception fusion system that congregates information about objects in an integrated object model. The HMI block constitutes an interface between the ADS and the operator which in the case of a level 3 ADS is the fallback ready user. There is also a localization and mapping block that is in charge of determining the exact location of the vehicle in real world coordinates by making use of high definition (HD) maps and appropriate GPS, GNSS, and related blocks that is assumed to be available to the ADS. When enabled by the tactical controller a vehicle trajectory is generated and acts as the reference path for the operational controller to control the detailed movement of the ego vehicle in the driving environment. The operational controller ensures that the commanded trajectory is followed as close as possible by using longitudinal and lateral controls. We assume that the ADS is built on top of an already functioning vehicle, thus much of the operational controller is already existing and available.

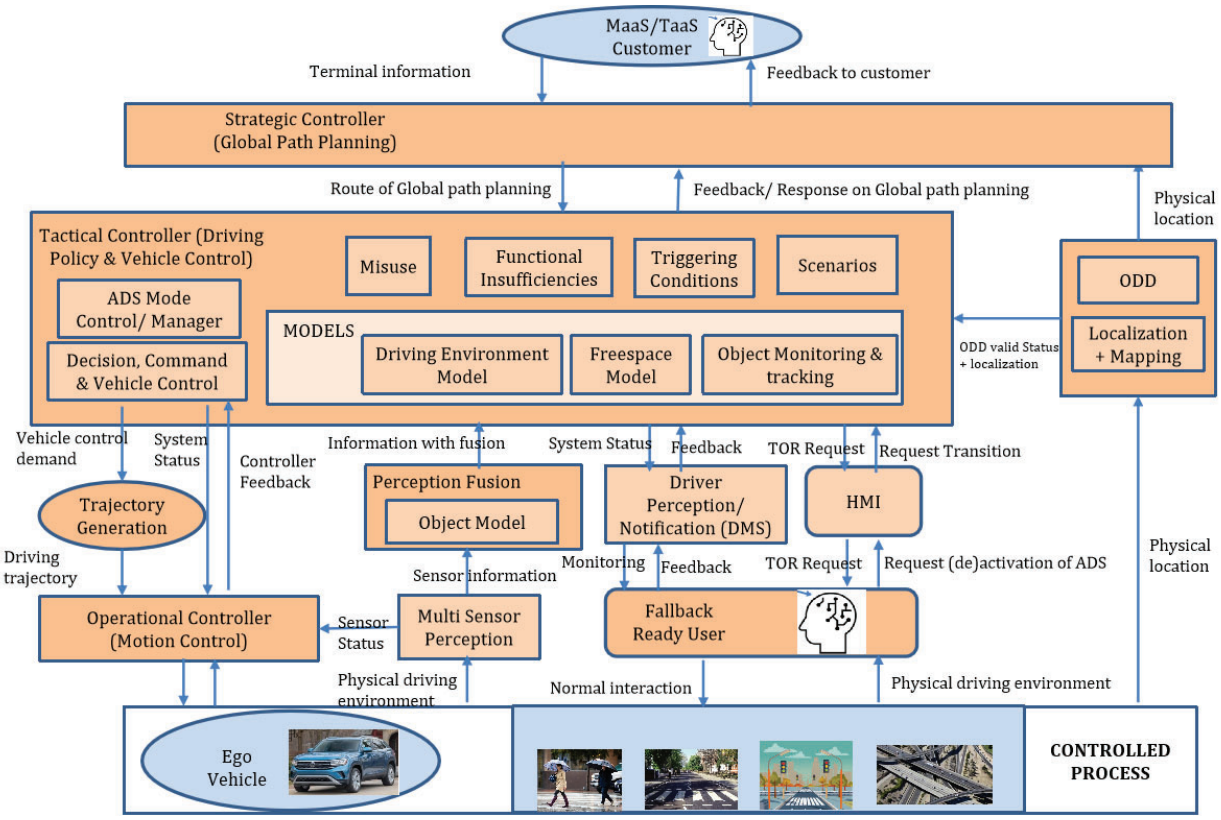



***Figure 3. Proposed STPA control structure for a level 3 automated driving system (ADS). The up arrows (↑) indicate feedback, the down arrows (↓) indicate control actions, and the side arrows (←) indicated other type of information.***

Whereas other authors consider the physical and driving environment as an input to the controllers [10], we put them as part of the controlled process which includes inputs and outputs. There are several reasons for this decision. First, through control actions, the various controllers effect changes on the environment, e.g., a behavioral change. Second, through the ego vehicle it is possible to effect change on the driving environment such as enhancing conspicuity via lighting, sounding the horn, signaling, gesturing, etc. In the future, this degree of control of the environment will increase with the introduction of wireless communications in the context of V2V (vehicle to vehicle), V2X (vehicle to infrastructure), and V2P (vehicle to pedestrian).

The operational design domain (ODD) is an important element of the STPA control structure. In this paper, we use the ODD structure proposed by the NHTSA consisting of the following elements [11]: (1) Physical infrastructure, (2) operational constraints, (3) objects, (4) connectivity, (5) environmental conditions, and (6) zones. The physical infrastructure includes such things as roadway types, roadway surfaces, roadway edges, and roadway geometry. Operational constraints include things like speed limit and traffic conditions. Likewise, Objects include things like signage, roadway users, non-roadway users, obstacles, objects, etc. Connectivity includes vehicles, traffic density information, remote fleet management systems, infrastructure sensors and communications. Environmental conditions include weather, weather induced road conditions, particulate matter, and illumination and zones include geo-fencing, traffic management zones, school construction zones, regions, states, and interference zones.

The ODD structure described above is generic to be used by all possible vehicle features. In the specific driver environment model described below, only a few elements of the overall ODD structure is used in order to have a simple and specific DEM that is effective for safety analysis and design of a specific level 3 ADS feature, that of an HWP.

**A. Strategic Controller**

The main task of the strategical decision-level controller is to define the goal of the trip. This includes a negotiation with the mobility-as-a-server (MaaS) / Transport-as-a-Service (TaaS) user, but it also includes the alternatives of never start, and of interrupting a trip changing its strategical decision to a minimal risk condition, MRC. This means that the MaaS/TaaS user might come with preferred trip destinations, but it is the ADS strategical controller that makes the decision of what is a safe strategical control action on this level, i.e. formulates the safe control action for the tactical decision level controller to execute. It is important that the strategical-level controller decision is with the ADS, to be able to avoid any unsafe control action. It is fundamental to formulate constraints on the strategical decision level controller, not to accept any strategically decision that cannot be guaranteed to be able to reach safely. As this is a control-loop responding to feed-back, the strategical decision needs to be reassured constantly, which for example may lead to either suggesting the user to take back the control or to change the ADS strategical decision to an MRC. In the full paper we show the full set of unsafe control actions for the strategical controller, and how these can be connected to a limited set of loss scenarios.

**B. Tactical Controller**

In terms of safety assurance of the HWP feature at an SAE level 3, the tactical controller is the most critical controller in the hierarchy. Although there are hazards at the strategic and operational controller hierarchical levels, the nature of such hazards is different from those of the tactical controller. More specifically, hazards at the strategic controller are out of scope of a DDT and thus of this paper. There are basically two categories of hazards at the operational level; the first category are hazards due to malfunctions and this is addressed by functional safety (i.e., ISO 26262); the second category of hazards are SOTIF in nature and should be addressed in a SOTIF analysis but is out of scope of this paper because the focus is on the tactical controller and an underlying model of the driving environment.

The tactical controller is depicted in Fig. 4 include the following main block categories:

1. Feedback and Inputs
2. Models
3. Decision making (e.g., control algorithms, driving laws)
4. Controller Actions / Execution

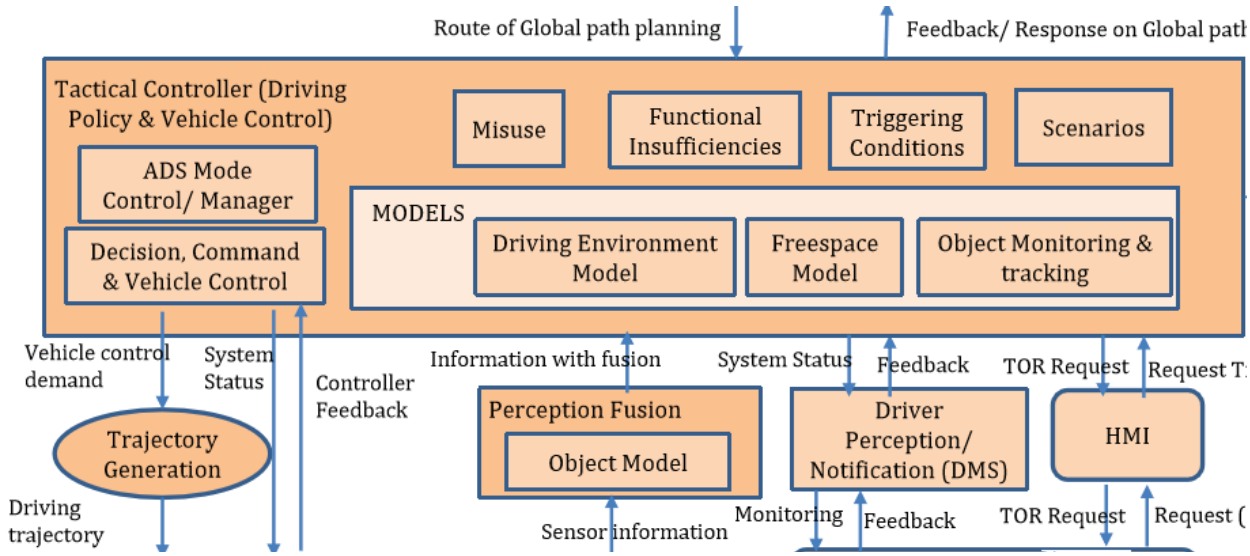



***Figure 4. Constituent components of a tactical controller for a level 3 automated driving system (ADS).***

**C. Operational Controller**

On the operational decision level, we find the traditional controller model, that for an ADS will be to execute a given trajectory. The controller constraints to avoid unsafe control actions, will include what it takes to be sufficiently close to the given trajectory. Whether this trajectory is safe or not, is not a question for the operational level controller where the only task is to execute a trajectory that is deemed safe by the controller on higher level. As for all the controllers, this is a continuous process where new decisions are given and new feed-back from the controlled process appears all

the time. The important thing is that the controller constraints are identified such that the feed-back loops of the controllers can guarantee the ADS to stay safe. By limiting the task for the operational controller to what is complementary to the two other controllers, it is possible to limit the set of loss scenarios, and thus to formulate a feasible verification strategy avoiding the 'billion miles problem'.

**Effectiveness of the STPA Control Structure to characterize SOTIF areas 1,2,3, and 4**

Scenarios are complex entities which are crucial to SOTIF analysis and there has been much discussion and interest in characterizing them. One approach to characterize scenarios is to develop a set of scenarios based on the features and use cases and utilize these scenarios as input for the safety analysis. One issue with this approach is that there is potentially a very large number of scenarios to consider. A related issue is the question as to what extent all scenarios are relevant for safety analysis, particularly the ones that are safety critical). In this context, the scenarios that are relevant but still not part of the analysis, are what constitutes SOTIF area 3. Another approach to characterize scenarios is to consider them not as inputs to the safety analysis but rather as a result of a complex interplay between the environment and the ego vehicle. In other words, scenarios can be viewed as outcomes of dynamic interactions of the STPA control structure and the controlled process which includes the ego vehicle and the physical and driving environment. The question about completeness of the scenarios, is a question about how to reach completeness for the purpose of analysis. If one is not using the scenarios as independent inputs, but as a result of a complex interplay between the environment and the ego vehicle, the problem of reaching completeness is no longer theoretically impossible. In this context, reaching completeness means not leaving anything out of the analysis. In our work we assume the latter approach described above. Regardless, the STPA control structure plays a crucial role in the safety analysis of an ADS in the context of SOTIF areas 1 to 4. Details will be provided in a future paper by the authors.

**Results**

In this section we provide some preliminary results of using the proposed STPA control structure depicted in Figs. 3 and 4 in an actual design of an automated vehicle manufactured by a big OEM. We present results for a HWP (highway pilot) feature at an SAE automation level 3. Through the efficient STPA control structure proposed in this paper we have identified 13 system level hazards and 24 Control flows (considering only the strategic and operational controllers).

A partial list of unsafe control actions includes:

1. HWP ADS does not provide (or providing the incorrect) the longitudinal or lateral control action during cruise control
2. HWP ADS provide longitudinal or lateral control during cruise control when it is not requested
3. HWP ADS does not provide the longitudinal or lateral control action during unplanned situations while driving
4. HWP ADS provide the unnecessary longitudinal or lateral control actions during unplanned situation while driving
5. HWP ADS provides too much or too little longitudinal or lateral control action during unplanned situations while driving
6. HWP ADS provides too early or too late or out of order longitudinal or lateral control action during unplanned situations while driving
7. HWP ADS does not provide the longitudinal or lateral control action while avoiding objects on the highway
8. HWP ADS provide unnecessary longitudinal or lateral control actions while no objects to avoid
9. HWP ADS does not provide the longitudinal or lateral control action while maintaining commanded trajectory
10. HWP ADS provide unnecessary longitudinal or lateral control while maintaining commanded trajectory

**Summary and Conclusions**

We have detailed a hierarchical STPA control structure having three hierarchical levels to generate scenarios suitable for safety analysis of SOTIF areas 1, 2, 3, and 4. Scenarios are complex entities that include features and events occurring over the operating lifetime of the vehicle and also include circumstances in which the hazard can lead to harm. The hierarchical control structure is based on the strategic, tactical, and operational functions defined in SAE J3016. Decomposing the responsibilities of achieving the DDT between the tactical and operational controllers

together with the analysis of the high-level system hazards enable the identification of unsafe control actions which are correlated to SOTIF requirements.

**REFERENCES**


[1] ISO 21448 - Road vehicles— Safety of the Intended Functionality.

[2] Till Menzel, Gerrit Bagschik, and Markus Maurer. Scenarios for development, test and validation of automated vehicles. In 2018 IEEE Intelligent Vehicles Symposium (IV), pages 1821–1827. IEEE, 2018.

[3] A. Abdulkhaleqa, et al., 'A Systematic Approach Based on STPA for Developing a Dependable Architecture for Fully Automated Driving Vehicles', 4th European STAMP Workshop 2016.

[4] Abdulkhaleq, Asim & Wagner, Stefan & Lammering, Daniel & Boehmert, Hagen & Blueher, Pierre. (2017). Using STPA in Compliance with ISO 26262 for Developing a Safe Architecture for Fully Automated Vehicles. arXiv:1703.03657v1 [cs.SE] 10 Mar 2017.

[5] M. Chaal et al., 'A framework to model the STPA hierarchical control structure of an autonomous ship', in Safety Science, Volume 132, December 2020.

[6] Zhang, S.; Tang, T.; Liu, J. A, Hazard Analysis Approach for the SOTIF in Intelligent Railway Driving Assistance Systems Using STPA and Complex Network. Appl. Sci. 2021, 11, 7714. https://doi.org/10.3390/app11167714

[7] S. M. Sulaman, et al, 'Hazard Analysis of Collision Avoidance System using STPA', in Proceedings Information Systems for Crisis Response And Management (ISCRAM) , 2014.

[8] N.G. Leveson, J.P. Thomas, 'STPA Handbook, MIT, March 2018, http://psas.scripts.mit.edu/home/materials/

[9] SAE J3016:APR2021, Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, April 2021.

[10] S. Khastgir et al. 'Systems Approach to Creating Test Scenarios for Automated Driving Systems', in Reliability Engineering & System Safety, volume 215, November 2021.

[11] Eric Thorn, Shawn Kimmel, Michelle Chaka (2018, September). *A Framework for Automated Driving System Testable Cases and Scenarios* (Report No. DOT HS 812 623). Washington, DC: National Highway Traffic Safety Administration.

# New Assessment and Testing Methodology for vehicle type approval

**Carlos Lujan Tutusaus (*), Oriol Flix Viñas, Pablo Rodríguez Corbacho, Núria Cayuela Rafols**

*Applus IDIADA Group, L'Albornar, E-43710 Santa Oliva, Spain (E-mail: carlos.lujan@idiada.com)y*

**ABSTRACT**: In the context of a deep transformation in the automotive technology, specially with the wide introduction of ADAS functions and the first commercially available vehicle with automated functions, the classic type-approval procedures have been challenged and new methodologies are required.

This paper describes the actions being carried out at different levels in order to tackle such challenge, as well as the main future trends with regards to the new assessment and testing methodologies for the type-approval of vehicles and their systems.

**KEY WORDS**: Automated driving, homologation,. testing, simulation, functional safety, SOTIF

## 1. INTRODUCTION

Technological innovations in the field of Connected and Automated Driving have a strong impact in different areas in the automotive industry. Among those areas, the effect on vehicle homologation procedures is game changing, in a way that requires a brand new approach. Traditionally, the homologation process based on the UNECE Regulatory framework has been a single step at the end of the development phase, where regulations normally defined a series of repeatable scenarios to be evaluated, where the effect of the driver is typically supressed by means of the measurement of the inputs on the vehicle commands or by means of the use of driving robots.

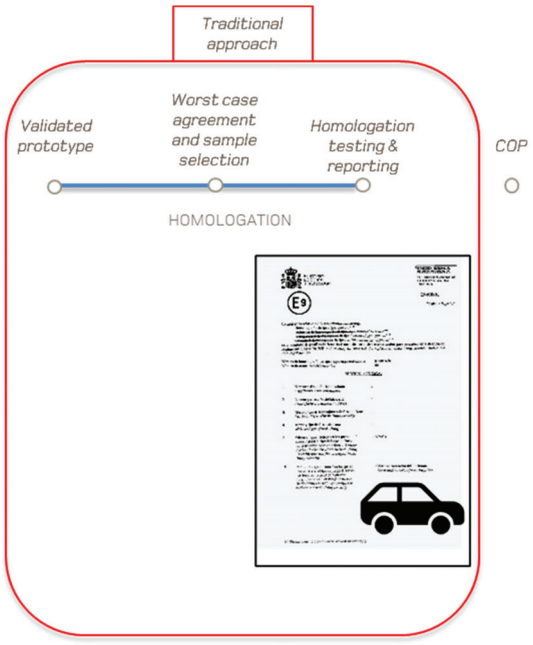



Figure 1 Traditional approach to type approval

In such context, the evaluation process could be scenario oriented: A limited amount of repeateable scenarios where reproduced under controlled conditions, and the performance of the vehicle/system alone was evaluated, in equal conditions.

This approach was initially challenged by the introduction of assisted systems, such as Advance Emergency Brake. Those systems are commanded by Electronic Control Systems which, in some circumstances, may control certain vehicle functions, such as braking or steering. The introduction of those functions required a different approach to the vehicle type approval, in order to evaluate possible failures associated to the Electronic Control Systems.

In such context, concepts such as Functional Safety (FuSa) or Safety Of The Intended Functionality (SOTIF) were introduce as part of the type approval process. This new approach turned the technical evaluation of the compliance from a testing activity in selected scenarios into a combination of testing and assessment of the manufacturer safety concept.

The vehicle is still under control of the human driver at all times, but the reaction of the vehicle may depend on the interventions of complex electronic systems. It is then necessary to guarantee that manufacturers have designed and built the vehicle to take safe decisions both in normal operation and failure conditions.

This methodology was already introduced in Regulation such as UN Regulation N. 13 and UN Regulation N. 13H, where systems like EBS or ESP may activate the braking system without intentional action from the human driver.

## 2. THE CHALLENGE OF AUTOMATED VEHICLES TYPE-APPROVAL

The introduction of the first SAE L3 functions into the market add a new layer of complexity into the type approval methodology. Such technologies replace the human driver during certain dynamic driving tasks, within an unlimited number of scenarios.

This circumstance does not allow the classic strategy of removing the human effect from the test scenarios, and requires a second loop in the modification of the type approval processes, so as to move from an evaluation of the performance to an evaluation of the behaviour of the vehicle.

In this case, there are two main aspects that the traditional approach could not solve efficiently:

a) The driving strategy: In vehicles operating in automated mode, the dynamic driving tasks are responsibility of the vehicle itself, without any human intervention. That means that the vehicle is not only responsible for the performance but also for the decisions on how to react to the inputs, assuming the role of the driver. In such circumstances, a classic type-0 braking test is not representative to evaluate the safety of a vehicle, because a vehicle with a lower mechanical braking performance may follow a more conservative driving strategy, so that will avoid the need for emergency braking in most of the possible scenarios, while a vehicle with a more performant braking system, but with a much more aggressive driving strategy may not be as safe.

b) The number of scenarios: In vehicles corresponding to SAE Level 2 or lower, a reduced number of scenarios is tested to evaluate the safety of its systems. As the human driver influence in the safe operation of the vehicle has a majoritary weight on the overall safety, over the system performance itself, it is possible to evaluate the safety of the system by excluding the human effect, by means of a limited number of test cases under repeteable and controlled conditions. However, if the driver effect can not be excluded, as in the case of automated driving vehicles, it cannot be guaranteed that vehicles which are similar from the mechanical point of view will have similar performance under different scenarios, as the driving strategy may be variable depending on the scenario, affecting the behaviour of the vehicle and, as a consequence, the performance.

## 3. THE RULEMAKING STRUCTURE

The main activities with regards to the definition of a type approval of automated driving vehicles for the European Union market are being developed in two different forums:

### 3.1. European Commission

The European Commission is responsible for the definition of the vehicle type approval within the European Union.

Currently, Regulation (EU) 2018/858 defines the framework for the administrative provisions and technical requirements that road vehicles, separate technical units and components need to comply with, in order to be placed in the market. In addition to that, such regulation establishes also the provisions for other procedures that guarantee a life-cycle compliance, like conformity of production and market surveillance.

On a second level, we can find a series of regulatory tools which support the framework regulation, by means of amending, supplementing or implementing it.

One of the most important regulatory tools is Regulation (EU) 2019/2144, on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users.

This regulation, also known as General Safety Regulation 2 or GSR2 introduces a series of mandatory systems that the vehicles will need to equip from July 2022 onwards. But most important, for the purposes of this paper, it defines a series of requirements that will need to be met by automated and fully automated vehicles.

As an initial step towards allowing the type approval of automated driving technologies, GSR2 does not define the technical specifications in detail, but creates a structure to kick-off the work for the creation of such technical requirements.

### 3.2. UNECE-WP29

One of the principles of Regulation (EU) 2019/2144 is that, for those requirements where there exists an UN Regulation, such Regulation shall be adopted by the European Commission with no need to duplicate efforts.

UN Regulations are developed in the framework of UNECE-WP29, the World Forum for Harmonization of Vehicle Regulations of the UNECE, headquartered in Geneva.

A series of Groups of Experts (GR-) subsidiaries of UNECE-WP29 deal with the different topics which are included within the regulatory framework, as indicated in figure 2.

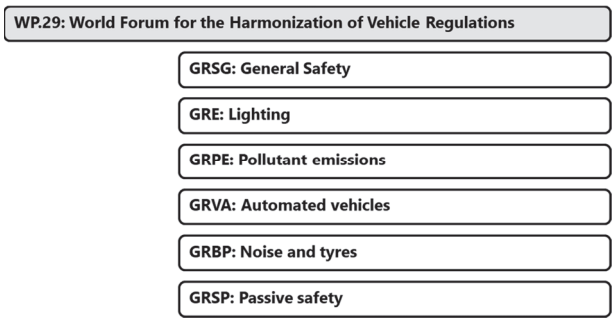



Figure 2 WP29 GR structure

GRVA was newly created in June 2019 to replace the previously existing GRRF (Group of experts on brakes and running gear), as a consequence of the publication of the Framework Document on Automated/autonomous Vehicles by UNECE-WP29 [1].

The framework document primary purpose is to provide guidance to WP.29 subsidiary Working Parties (GRs) by identifying key principles for the safety and security of automated/autonomous vehicles of levels 3 and higher. The framework document also defines the work priorities for WP.29 and indicates the deliverables, timelines and working arrangements for those certain work products related to those priorities.

One of the tasks of the framework document was the definition of a “safety vision”, which included a list of topics which should be taken into account to ensure safety:

a) System Safety: When in the automated mode, the automated/autonomous vehicle should be free of unreasonable safety risks to the driver and other road users and ensure compliance with road traffic regulations;

b) Failsafe Response: The automated/autonomous vehicles should be able to detect its failures or when the conditions for the [ODD/OD] are not met anymore. In such a case the vehicle should be able to transition automatically (minimum risk manoeuvre) to a minimal risk condition

c) Human Machine Interface (HMI) /Operator information: Automated/autonomous vehicle should include driver engagement monitoring in cases where drivers could be involved (e.g. take over requests) in the driving task to assess driver awareness and readiness to perform the full driving task. The vehicle should request the driver to hand over the driving tasks in case that the driver needs to regain a proper control of the vehicle. In addition, automated vehicle should allow interaction with other road users (e.g. by means of external HMI on operational status of the vehicle, etc.)

d) Object Event Detection and Response (OEDR): The automated/autonomous vehicles shall be able to detect and respond to object/events that may be reasonably expected in the [ODD/OD];

e) Operational Design Domain (ODD/OD)] (automated mode): For the assessment of the vehicle safety, the vehicle manufacturers should document the OD available on their vehicles and the functionality of the vehicle within the prescribed OD. The OD should describe the specific conditions under which the automated vehicle is intended to drive in the automated mode. The OD should include the following information at a minimum: roadway types; geographic area; speed range; environmental conditions (weather as well as day/night time); and other domain constraints

f) Validation for System Safety: Vehicle manufacturers should demonstrate a robust design and validation process based on a systems-engineering approach with the goal of designing automated driving systems free of unreasonable safety risks and ensuring compliance with road traffic regulations and the principles listed in this document. Design and validation methods should include a hazard analysis and safety risk assessment for Automated Driving System (ADS), for the OEDR, but also for the overall vehicle design into which it is being integrated and when applicable, for the broader transportation ecosystem. Design and validation methods should demonstrate the behavioural competencies an Automated/autonomous vehicle would be expected to perform during a normal operation, the performance during crash avoidance situations and the performance of fall back strategies. Test approaches may include a combination of simulation, test track and on road testing.

g) Cybersecurity: The automated/autonomous vehicle should be protected against cyber-attacks in accordance with established best practices for cyber vehicle physical systems. Vehicles manufacturers shall demonstrate how they incorporated vehicle cybersecurity considerations into ADSs, including all actions, changes, design choices, analyses and associated testing, and ensure that data is traceable within a robust document version control environment

h) Software Updates: Vehicle manufacturers should ensure system updates occur as needed in a safe and secured way and provide for after-market repairs and modifications as needed

i) Event data recorder (EDR) and Data Storage System for Automated Driving vehicles (DSSAD): The automated/autonomous vehicles should have the function that collects and records the necessary data related to the system status, occurrence of malfunctions, degradations or failures in a way that can be used to establish the cause of any crash and to identify the status of the automated/autonomous driving system and the status of the driver. The identification of differences between EDR and DSSAD to be determined;

The second consequence of the framework document was a redefinition of the structure of informal working groups, task forces and special interest groups, subsidiary of GRVA. Those groups are created under certain terms of reference, as a mandate from GRVA, in order to reach a target within a defined timeframe.

Those working groups develop their activities under the coordination of a chairperson or several chairpersons, with the support of a secretariat and report their results to GRVA.

The frequency of meetings of those working groups is, compared to GRVA, much more frequent, as the technical discussions are held within such forums, while the discussions at GRVA are kept at a higher level, and are focused mainly on decision making rather than the discussion of the details.

The current structure of GRVA and subsidiary working groups can be seen in figure 3, and the direct relationship between the topics described in the safety vision of the framework document and the different working groups is evident.

## 4. VMAD AND THE NEW ASSESSMENT AND TESTING METHODOLOGIES

As stated in the previous section of this paper, one of the topics of the safety vision of the framework document is the validation for system safety. As it was earlier introduced, the automated and autonomous technologies require a new approach to the validation methodology, different from the classical tests for a prototype under repeteable conditions.

The seed for this new technology is the "three pillar approach", firstly introduced in the GRVA discussions upon initiative from OICA.

| GRVA | FRAV: Functional Requirements for Automated and Autonomous Vehicles |
|---|---|
| | VMAD: Validation Method for Automated Driving |
| | CS/OTA: Cybersecurity and (OTA) Software Updates |
| | DSSAD/EDR: Data Storage System for Automated Driving |
| | AEBS/LDWS: Advanced Emergency Braking and Lane Departure Warning |
| | SIG ALKS: Special Interest Group on Advanced Lane Keeping System |
| | ADAS |

Figure 3 Current structure of GRVA working groups, February 2022

The seed for this new technology is the "multi-pillar approach", firstly introduced in the GRVA discussions upon initiative from OICA in 2019 [2]. According to this approach, the use of different tools is required in order to guarantee the safe market introduction of automated and autonomous vehicles:

a) Audit / assessment:

-Understand the system to be certified

-Assess that the applied processes and design/test methods for the overall system development (HW and SW) are effective, complete and consistent

-Assess system's strategies/test performance to address (multiple) fault-conditions and disturbances due to deteriorating external influences; vehicle behavior in variations of critical scenarios

-Simulation: Test parameter variations (e.g. distances, speeds) of scenarios and edge-cases that are difficult to test entirely on a test track

b) Physical CertificationTests:

-Assess critical scenarios that are technically difficult for the system to cope with, have a high injury severity (in case the system would not cope with such a scenario) and are representative for real traffic

-Compare with critical test cases derived from simulation and validate simulation tools

c) Real World Test Drive:

-Assess the overall system capabilities and behavior in non-simulated traffic on public roads and show that the system has not been optimized on specific test scenarios

-Assess system safety requirements like e.g. HMI and ODD

-Assess that the system achieves a performance comparable to an experienced driver

The multi-pillar approach has been further developed under the workframe of VMAD, being renamed as NATM: New Assessment and Testing Methods. For such purpose, and additional level of subgroups, dealing with different specific topics was also created (figure 4):

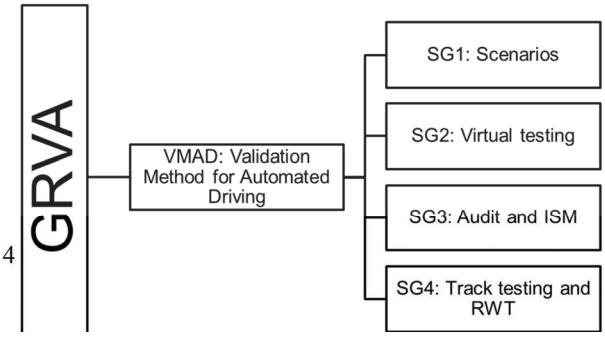



Figure 4 VMAD subgroups

During the 12th Session of GRVA (January 2022), VMAD presented a proposal for a second iteration of the Master Document on NATM [3], which defines the principles of such methodology on the basis of five pillars:

1. Simulation/virtual Testing

It uses different types of simulation toolchains to assess the compliance of an ADS with the safety requirements on a wide range of virtual scenarios including some which would be extremely difficult if not impossible to test in real-world settings. The aspect of credibility of simulation/virtual testing is included in this topic.

2. Track testing

It uses a closed-access testing ground with various scenario elements to test the capabilities and functioning of an ADS.

3. Real world testing

It uses public roads to test and evaluate the performance of ADS related to its capacity to drive in real traffic conditions.

4. Audit/assessment procedures

They establish how manufacturers will be required to demonstrate to safety authorities using documentation, their simulation, test-track, and/or real-world testing of the capabilities of an ADS. The audit will validate that hazards and risks relevant for the system have been identified and that a consistent safety-by-design concept has been put in place. The audit will also verify that robust processes/mechanisms/strategies (i.e., safety management system) that are in place to ensure the ADS meets the relevant safety requirements throughout the vehicle lifecycle. It shall also assess the complementarity between the different pillars of the assessment and the overall scenario coverage.

5. In-service monitoring and reporting

It addresses the in-service safety of the ADS after its placing on the market. It relies on the collection of fleet data in the field to assess whether the ADS continues to be safe when operated on the road. This data collection can also be used to fuel the common scenario database with new scenarios from the field and to allow the whole ADS community to learn from major ADS accidents/incidents.

In order to guarantee the efficiency of those pillars, they need to be supported by a scenario catalogue, descriptions of real-world

driving situations that may occur during a given trip, will be a tool used by the NATM-pillars to validate the safety of an ADS.

This new approach leads consequently to a change in the interaction between Technical Services and vehicle manufacturers. As per the traditional approach (figure 1), it was limited to very late stages of the process, once the vehicle or system had already been validated by the manufacture. However, the new approach requires the type-approval process to be started way in advance, so that the development methodology can be evaluated before the vehicle is ready to be assessed. (figure 5).

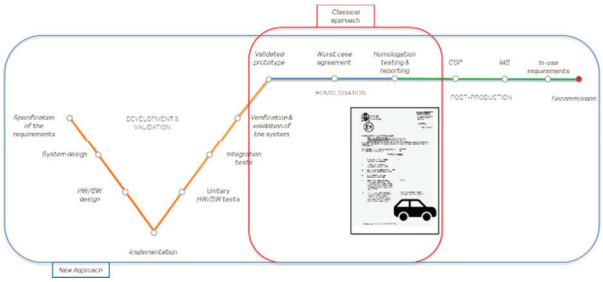



Figure 5 description of the application of NATM within the vehicle life-cycle

## 5. NATM VS OTHER METHODOLOGIES

Type-approval of vehicles and systems is normally the latest step in the life-cycle of the vehicle development. Previously, the manufacturer may have performed its internal validation tests, in order to guarantee the safety of the vehicle, but also some aspects which are not part of the areas of interest of type-approval, such as the feeling or the comfort of the vehicle.

This may have leaded to different approaches to the testing and assessment methods, depending on the stage of development of the vehicle. However, there is a trend for the harmonization of such methods, and it is becoming frequent for manufacturers to use a similar approach for the validation of their vehicles. Additionally, other evaluation frameworks, like EuroNCAP are introducing similar methodologies.

Efforts for harmonization of these methodologies can also be found in EU-funded projects like HEADSTART, which aimed to define testing and validation procedures of Connected and Automated Driving functions including key technologies such as communications, cyber-security and positioning. The tests will be in both simulation and real-world fields to validate safety and security performance according to the key users' needs. Those key users included:

a) Type-approval rulemakers

-New CAV type-approval regulation

-CAV safe market introduction

-Digital driving license

b) EuroNCAP

-New official assessment protocols

-User acceptance

-Safety-aware sales growth

c) Vehicle manufacturers

-New development strategies

-New CAV functions enabler

-Cost and time-to-market reduction

## 6. CONCLUSION

The introduction of automated vehicle technologies introduces a series of challenges to vehicle industry stakeholders, and type-approval is an important one. Guaranteeing that a vehicle is safe to be placed in the market is essential, but it shall be balanced with a certain flexibility to allow the market introduction in a pragmatic and cost effective manner.

The use of innovative methodologies is thus required, as the traditional methods have proven not to be valid for vehicles able to perform dynamic driving tasks on their own.

Rulemaking forums have already stepped forward and developed an innovative methodology that will allow the type-approval of those vehicles, but as a side-effect, all the involved stakeholders will need to adapt themselves to the new tools, time-span and methods introduced by NATM.

Finally, there is also a clear trend for harmonization of the validation methodology along the automotive industry, which reflects the effort to optimize resources and time.

## REFERENCES

[1]https://www.unece.org/fileadmin/DAM/trans/doc/2019/wp29/WP29-177-19e.pdf
[2]https://www.unece.org/fileadmin/DAM/trans/doc/2019/wp29/WP.29-177-20e.pdf
[3]https://unece.org/sites/default/files/2021-11/ECE-TRANS-WP29-GRVA-2022-02e.pdf

**28th ITS World Congress, Los Angeles, September 18-22, 2022**

Paper ID #

# Cyber Security regulation – Practical application from a technical service point of view

**Oriol Flix[1*], Carlos Luján[1], César Elpuente[1]**
1. IDIADA Automotive Technology S.A, Spain (oriol.flix@idiada.com)

**Abstract**
It is widely known that the future of vehicles is a progressive evolution from conventional vehicles to fully autonomous/connected vehicles able to deal with all the situations on the road. This process starts with new ADAS (Advanced Driver Assistance Systems) functions that are gradually taking the control of the vehicle, in controlled situations, over the driver. Based on these new technologies, and always from the safety point of view, the European Union introduced the new General Safety Regulation. This regulation introduces advanced safety requirements that will become mandatory from 2022 for new vehicles types.
One of the regulations that will cause a major impact on manufacturer's internal procedures, but also on the way in which Approval Authorities and Technical Services assess the system, is the regulation on Cyber Security, UN R155, that requires a new approach on how to validate and certify a system

**Keywords:**
Autonomous Driving, Cyber Security, New General Safety Regulation, Advanced Driver Assistance Systems

## Introduction

The main objective of the paper is to analyse the impact of the UN Regulation No 155 on manufacturer's procedures, and to the certification process. The classic certification approach for almost all the safety functions that are legislated, starts when the manufacturer finishes the prototype of this specific system, and together with a documentation package that defines the most relevant aspects of it, characteristics, and design, is sent to the Approval Authority (AA) or Technical Service (TS). The AA or TS will be the responsible to assess and verify if it is valid according to the requirements defined for such specific system in the relevant regulation. This validation process, normally includes the following steps:

1. Verification that the sample provided by the manufacturer is representative of the documentation that defines the system.
2. Verification that the system fulfils the requirements defined by the regulation.
3. Verification of visual means (may be tell-tales, dimensions, masses, …)
4. Testing. Most of the regulations include static and/or dynamic tests that shall be performed in controlled conditions, to ensure the repeatability of the results, with a minimum performance, that is understood as the minimum safety level that shall be provided in order to place the vehicle in the market.

The tests to be performed and the acceptance criteria for these regulations is clearly stated, and it is only a matter of having the suitable equipment and trained people to validate it. So, if the value obtained is less or higher than the prescribed by the regulation, the system fulfils (or not) the minimum requirement of safety. The problem arises when the system that is being evaluated cannot be assessed through the typical system inspections and pre-defined tests.
How would you define a specific test for a system, in terms of Cyber Security, if new threats and vulnerabilities are discovered every day?

Similar to what happened with the analysis and assessment of Complex Electronic System, a new certification approach has been developed in order to adapt to this new situation. An approach that still allows to the Technical Services and Approval Authorities the evaluation of Cyber Security in terms of safety for the drivers and other road users. In order to evaluate how the new UN Regulation No 155 has changed this approach both for manufacturers and TS/AA, is important to have a clear idea on why it is so important, application dates, and where the requirements have been created.

**New General Safety Regulation (EU) 2019/2144**

Given the current developments in connected and automated driving, the GSR defines some advanced and intelligent safety features for each category of vehicle of the EU market. Advanced vehicle systems have been proven effective in reducing fatalities, road accidents and mitigating injuries, therefore the regulation looks for a gradual adaptation of the users to automated features by making them mandatory.

Given that connectivity and automation of vehicles increase the possibility of unauthorized remote accessing to vehicle data, and performing illegal modifications of software, the GSR defines that UN Regulations No 155 (Cyber Security) and No 156 (Software updates) should be applied on a mandatory base. Therefore, the GSR defines application dates for all the vehicles, so that it will be mandatory in Europe to fit new vehicles with systems that will protect against unauthorized access. These dates are:

- July 2022 for New Vehicle Types.
- July 2024 for New Registrations.

So, any vehicle sold from July 2024 onwards, shall be protected in terms of Cyber Security.

As said before, the GSR also defines that the new regulation on CS should be created in the UN framework.

**UNECE Structure**

United Nations regulations are regulations that have been accepted and recognized by all the signatories of the 1958 agreement. Moreover, most of these regulations become mandatory under European laws.

Due to the growing importance of the autonomous and connected vehicles, on 2018 WP.29 created a dedicated subsidiary working party called GRVA (Group of Experts on Automated Driving). Considering the main objectives reflected on the framework document for automated vehicles, different informal groups had been established, and continue to be established, in order to address the different topics. The current structure is shown in Figure 2.

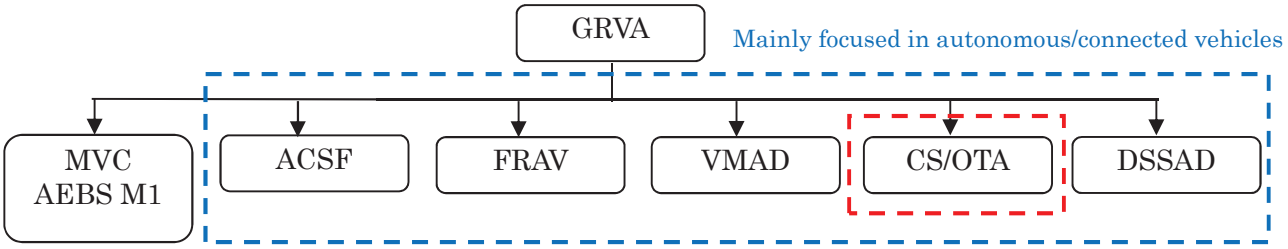



Figure 1. GRVA and subsidiary groups' structure

Under the supervision of the UNECE and the World Forum for Harmonization of Vehicle Regulations (WP.29), GRVA is the group that discusses all the themes belonging to autonomous driving and proposes recommendations or guidelines that will become new UN Regulations.

A framework document presented during 2019 on automated/autonomous driving serves as the basis for further development of a series of vehicle safety topics, always looking for a higher level of safety. The list includes:

- System Safety.
- Failsafe Response.

- Human Machine interface (HMI).
- Object Event Detection and Response (OEDR)
- Operational Design Domain (ODD/OD)
- Validation for System Safety.
- ***Cyber Security***.
- Software Updates.
- Event Data Recorder (EDR)

These priorities are treated or discussed on specific working groups directly dependant of GRVA. As seen, Cyber Security is one of the main topics of the framework document, and the organization dedicated a lot of effort and resources for the development of the regulation between 2019 and 2020.

**CS/OTA (Task force on Cyber Security and Software Updates)**
On top of all the new groups on the autonomous field, Cyber Security and Software Updates task force has evolved quickly due to its high growing importance. This group has been the responsible for developing the technical requirements of such regulations. Given the synergies of Software Updates and Cyber Security in the automotive field, both regulations have been created by the same experts, so they share a similar approach in terms on how to assess the technologies and how they shall be applied by the manufacturer inside of their organizations, for the whole lifecycle of the vehicle (development, production and postproduction).

The first meetings of the group were held at the end of 2018, and the first drafts of the regulations were adopted by the GRVA in March 2020. In between, more that 20 meetings with all the experts took place, given the importance of the topics.
One of the main differences between the two regulations and other vehicles' regulations, is that Cyber Security and Software Updates regulations are accompanied by a master document that pretends to provide guidelines for the TS/AA. The main objective of the guideline (called Interpretation Document), is to provide an explanation of:

- The purpose of the requirement.
- The kind of procedure should be provided by the manufacturer in order to fulfil the requirement.
- Standards, ISO's or similar documents, that could be used as evidence.

So, in short, it is a guideline for the TS/AA, on how to evaluate every single requirement that affects the manufacturer, and what's considered as a minimum level of safety. The use of the guidelines also ensures that all the contracting parties, through their TS and AA, have the same approach on the evaluation of such systems and that there are no different interpretations between them.

What makes these two regulations different, among other conventional regulations, is that both of them are split in two differentiated parts.
First of all, the regulation defines a set of requirements that intended to validate if the manufacturer has a set of processes/procedures in place, that will provide guidance on how to handle Cyber Security/Software Updates during the operational life of vehicles, produced under a vehicle type. The different phases of the lifecycle may have specific activities, procedures, that have to be implemented and analysed.
Focussing on the Cyber Security area, this specific set of procedures that will cover its management is called Cyber Security Management Systems (CSMS). The CSMS is a systematic risk-based approach that defines organisational processes, responsibilities and governance to treat risk associated with cyber threats to vehicles and protect them from cyber-attacks.
As said, contrary to other regulations, this one adds specific provisions in order to ensure that the manufacturer takes into account the Cyber Security of the company and the vehicles that are in use for the whole life-cycle.


Figure 2. CSMS lifecycle covering.

The CSMS of the manufacturer is the first process that shall be evaluated by the TS/AA, given that the obtention of the Certificate of Compliance (CoC) of this system, will allow to the obtention of vehicle type approvals on regards of Cyber Security.
The validity of the CSMS is three years from the obtention of the CoC, and after this period, the system shall be re-evaluated again, to verify that every process is still in place, and has been updated according to the new threats and vulnerabilities. Once the manufacturer has obtained the CSMS, vehicle types can be presented for the certification under the scope of this specific Management System. So, the second set of requirements of the regulation is intended to cover the essential aspects and verifications for the vehicle type. Basically, these requirements are based on the direct application of the processes defined in the CSMS for the whole life-cycle of the vehicle, to the vehicle that is under the type approval. In addition, it is at this point where the tests on the vehicle are performed, according to the vulnerabilities detected, their threats, and the mitigations applied by the manufacturer.

**Technical service point of view**
The overview of the processes, or areas to be assessed in terms of the CS Regulation by the Technical Service, are split as it is shown in Figure 3.

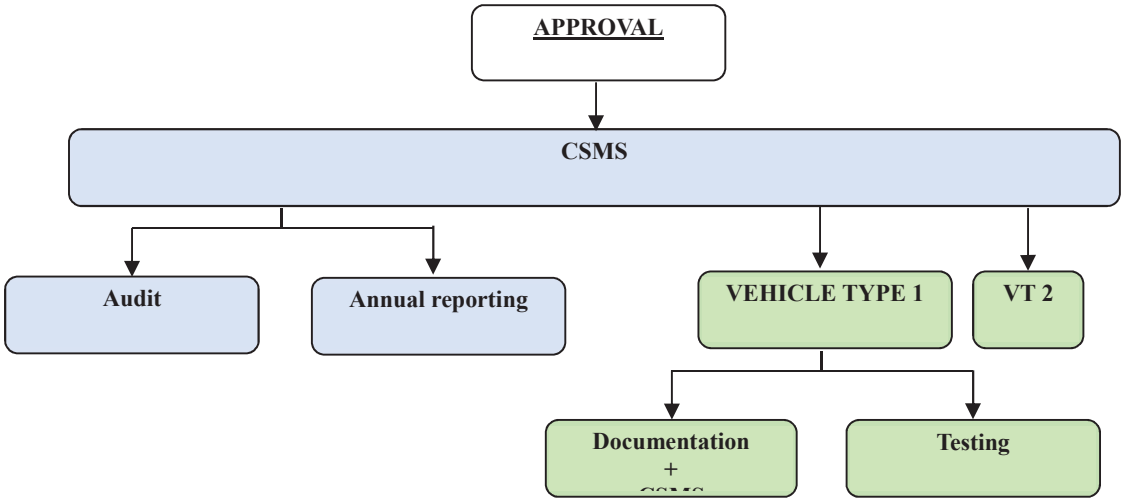



Figure 3. Approval processes of UN R155

The two colours in Figure 3 define the two main areas that are performed for the type approval process by the Technical Service. As it is defined, the Technical Service shall, first of all, assess the whole CSMS of the manufacturer. This is a new concept inside of the certification procedure regarding other regulations. The inspectors shall evaluate if the processes provided by the manufacturer are aligned with what it is expected by the Regulation, and the Interpretation document.

One of the challenges that the TS may have, is that actually, the certification procedure is starting in an early phase of the development of the system. Given that the CSMS is covering all the phases of the lifecycle, it is important to start the first contacts with the manufacturer months before the evaluation of the CSMS, and the obtention of the CoC. Otherwise, if some deviations that directly affect the development process of the vehicle are found when the vehicle is almost in the production line, the mitigations implemented by the manufacturer could cause a big impact in terms of timing, and the development of the architecture of the vehicle.
The assessment of the CSMS should be performed, by experienced persons on type approval and Cyber Security, in the following steps:

- Pre-assessment of the technical documentation: all the non-confidential procedures and processes of the manufacturer can be evaluated before the on-site audit. This first row allows to identify deviations on the procedures from an early phase.
- On-site audit: an audit at the manufacturer's facilities in order to verify that the processes provided in the first stage are actually implemented by all the areas. Additionally, all the information that is considered confidential by the OEM and couldn't be shown before, is evaluated during this phase.
- In case that some deviations are found, a second round of audit may be performed, or a re-evaluation of the technical documentation, with the updates of the manufacturer.
- Issue a test report with the results of the audit, and the fulfillment of the requirements for the CSMS.

Therefore, engineers in charge of these regulations should be more experienced on auditing than testing, also having a background on electronics and Cyber Security.

Once the CoC of the CSMS is issued, an annual reporting from the manufacturer is required for the continuous monitoring of the system: this is intended to ensure that the manufacturer is following the processes defined for the CSMS, and there is evidence of this compliance. After three years from the approval date, a new audit shall be performed in order to obtain the renewal of the CoC.

After the approval of the CSMS is granted, the vehicle manufacturer can obtain vehicle types according to the procedures developed under the management system approved. For this second stage, a new set of requirements focused on the specific architecture that is going to be approved, will apply.
Basically, the requirements are focused on the application of the procedures provided for the CSMS, on the specific vehicle type.

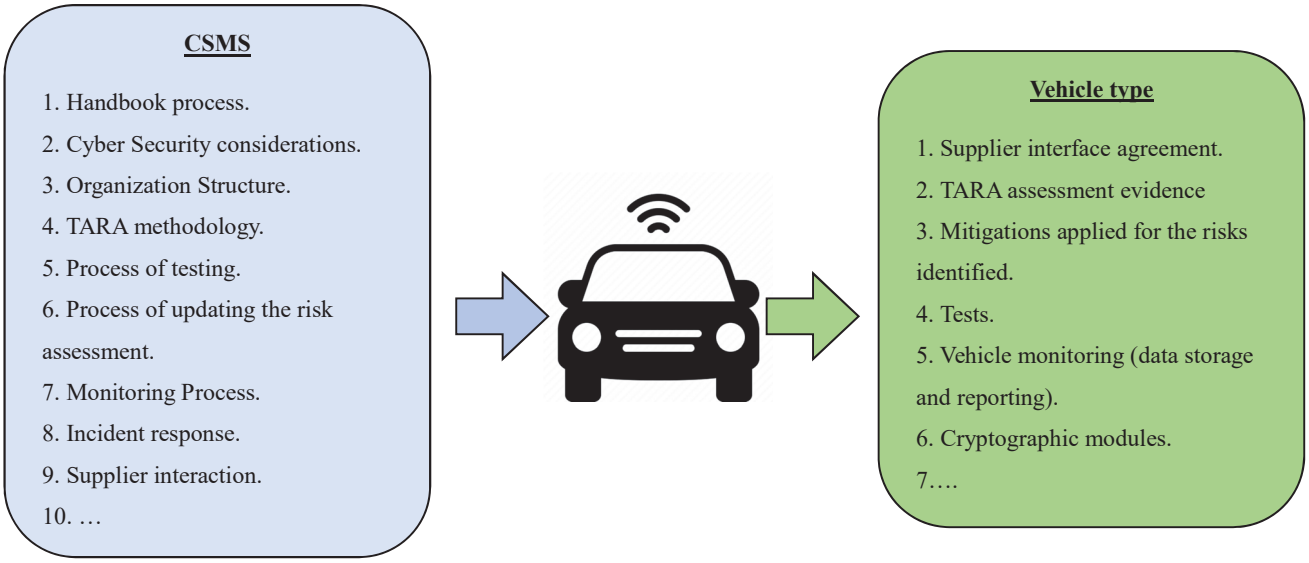


Figure 4. Application of the CSMS to the Vehicle Type.

Thus, for a given architecture, the use of the procedures defined for the CSMS, allows to the manufacturer the identification of threats and vulnerabilities for the vehicle under design. For the identified risks, mitigations are applied, and Cyber Security tests shall be applied in order to verify that the mitigations are suitable according to the safety goals.

What is important for the vehicle type phase, from the Technical Service point of view, is the verification that the defined architecture of the vehicle is covered by the manufacturer's CSMS, and that the processes are correctly applied to ensure the vehicle security during the lifecycle.

Additionally, once the mitigations and tests are defined according to the TARA methodology, the Technical Service is able to witness, or perform by itself, some of the proposed tests, and check that the results are good, and the mitigations are enough for a given risk or threat. Therefore, for the vehicle type certification, the TS need to acquire knowledge for Cyber Security testing, and processes auditing.

**Conclusions**

The path from conventional vehicles to automated and connected vehicles, can not be understood without the evolution and inclusion of new technologies related to complex electronic systems, connectivity between vehicles, infrastructure, and the use of the data obtained onboard and offboard the vehicle. The development of new connectivity technologies and their fitting to the vehicles, also creates new threats and ways to attack the vehicles, obtain confidential data from the users, or create unsafe situations.

For this reason, the European Commission and the World Forum for the Harmonisation of Regulations (WP.29) have developed the set of administrative and technical requirements that a manufacturer and a vehicle shall fulfil in terms of Cyber Security.

Given the complexity of the area, and that the definition of pre-defined tests or mitigation wouldn't be effective for ensuring the security, a new approach for the Type Approval process had to be defined. This new approach leads to a new way to certify, and thus creation of new needs for the Technical Services, which shall evolve quickly and adapt to the new procedures.

**References**


1. European Commission Technical Committee on Motor Vehicles (2019). *Guidelines On The Exemption Procedure For The Eu Approval Of Automated Vehicles*

2. https://www.unece.org/trans/main/wp29/meeting_docs_grva.html

3. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R2144&from=EN

# INFRASTRUCTURE CONNECTIVITY TO IMPROVE AUTOMATED DRIVING SAFETY AND INFORMATION QUALITY

**Ilkka Kotilainen**
**Risto Kulmala**
Traficon Ltd
Finland

**Hironao Kawashima**
Keio University
Japan

**Sven Maerivoet**
Transport & Mobility Leuven Ltd
Belgium

**Siddartha Khastgir**
University of Warwick
United Kingdom

**Steven Shladover**
UC Berkeley
United States

**Jaap Vreeswijk**
**Tom Alkim**
**Anton Wijbenga**
MAPtm Ltd
Netherlands

Paper number 23-0294

## ABSTRACT

All actors in road transport share and aim for the same mutual goal of safe, clean, and efficient Connected and Automated Driving (CAD). The aim of the research was to study how infrastructure connectivity improves Automated Vehicle (AV) safety in three selected motorway environment use cases of traffic jam, adverse weather and static/dynamic road works as well as quality indicators and requirements for the communication. Information priority with safety criticality in mind was assessed for the three actors of road works or (winter) maintenance operator, traffic manager and AV or Automated Driving System (ADS) developer. The results present Operational Domain Design (ODD) and local condition attributes information priority recommendations, ADS developers trust issues when using information via infrastructure communication, information quality recommendations as well as quality monitoring and management methods.

## INTRODUCTION

The safe operation of Automated Vehicles (AV) requires understanding of the conditions in which the Automated Driving Systems (ADS) are capable of operating, i.e., Operational Design Domain (ODD). Because of ADS systems' need of constant monitoring of the current and near future ODD attributes, such as incidents or weather conditions, real-time information is essential to the relevant actors of road works or (winter) maintenance operator, traffic manager and AV (or ADS) developer. This research refers to the automated driving system actor as an ADS developer. However, in practice the primary automated driving system actor ensuring the ODD awareness of the ADS will likely be the fleet operator responsible for the ADS-operated vehicle in question.

Infrastructure communication can be one of the sources of real-time information. Local condition information shared by the local traffic manager may benefit the ADS and vice versa; exchange of information between the actors provides mutual benefits for safe, efficient, and clean automated driving. The values of ODD attributes, which the road operator or traffic manager can regard as local condition attributes, such as weather or traffic

flow conditions that the ADS cannot measure or sense by itself, may be provided by off-board sensor infrastructure. The real-time sharing of ODD related data can be accomplished with a concept that we call the Distributed ODD Awareness (DOA) Framework.

We wished to study how infrastructure connectivity improves AV safety in three selected use case scenarios, and the related quality indicators and requirements for the communication. To improve the safety of AV with connectivity, the right kind of information needs to be available at the right time for the vehicle to help its decision making and manoeuvre. The right kind of information relates to what kind of information is needed by the vehicle and what is the source of the information. Furthermore, even with the right kind of information from a reliable source, the information needs to be delivered on time and the quality must be sufficiently high. Therefore, four research questions were formulated to further specify the aim of the research:

1. What kind of information is to be transmitted in the interaction (in both directions) between the traffic management centre (TMC) and vehicle?
2. Which information is to be provided by the National Road Authorities (NRA)/roadside and which information can be obtained by the sensors of the moving vehicle itself?
3. When and how should such information be available?
4. How to define and measure the quality/correctness of such information?

## METHODOLOGY

The research was part of the Traffic Management for Connected and Automated Driving (TM4CAD) project funded by the Conference of European Directors of Roads' (CEDR) Call 2020 Impact of Connected and Automated Driving (CAD) on Safe Smart Roads, aiming to prepare the national road authorities for the future challenges of connectivity, digitalization, and automation [1]. Qualitative methods of research project members' expert analysis, literature review, survey, workshop, and feedback review were used.

The expert analysis and literature review of ODD information needs, and importance were completed for three actors: road works or (winter) maintenance operator, traffic manager and ADS developer. The actors were selected based on their close collaboration with road operator or AV as well as their status as a data provider and consumer for the local condition and ODD attribute information. Three use cases of traffic jam, adverse weather and static/dynamic road works were selected based on their relevance in highway and motorway environment as well as evaluated increased information need by the ADS in such environment. The use cases vehicles are cars with connectivity and access to infrastructure communication via various technologies, but other motor vehicles with similar equipment would be applicable as well. The vehicles were assumed to have SAE Level 3 or 4 automated driving capability for the highway auto pilot type use case. The following ODD attribute clusters used in the analysis were taken from the project's earlier analysis of the attributes: physical attributes of the roadway and its environs, digital infrastructure support, dynamically varying ambient environmental conditions, and operational attributes of the roadway [2].

The prioritisation of the ODD (or local condition) information needs of the three actors were assessed based on three criteria. First, expert assessment was completed for information need importance in the three use cases for the three actors in four levels of none, low, medium, or high. Then an average was calculated for each of the actors, and the aggregated information need importance (or priority) for the actor was qualitatively analysed to avoid any bias between the scenarios. Secondly, ODD attribute safety criticality was assessed as if the information would not be available, and then its impact to the actor in similar four levels from no safety impact to high impact. Third, additional/reduced costs for the actor were assessed. Finally, an overall information priority was qualitatively assessed for each of the ODD attributes (local condition) based on

- three actors of maintenance operator, traffic manager and automated vehicle or Automated Driving System developer,
- actor's need for the information and information safety criticality,
- three scenarios of traffic jam, adverse weather area and static/dynamic road work zone.

Two workshops were held, one together with the automated vehicle industry members and the other with CEDR Connected and Automated Driving (CAD) Working Group Road authority members to validate the ODD attribute prioritisation of information needs results. Furthermore, discussions were held, and written feedback collected from the CEDR CAD Working Group. Before the AV industry members workshop, a survey was conducted to collect feedback of the information priority analysis and to refine the content of the workshop. The survey was circulated via the Hi-Drive consortium (Hi-Drive 2022) involving all major vehicle manufacturers

and ADS developers in Europe; as the consortium is research oriented the views do not present the views of the vehicle manufacturers, but more of individual ADS use case developers.

## RESULTS

### Infrastructure connectivity and information priority

The results concerning the ODD (local condition for the road operators and traffic managers) attributes' information priority levels are presented in Tables 4.-7. (Appendix of paper) where each of the previously mentioned four ODD attribute clusters are presented. The following is a summary of the analysis, pre-workshop survey, workshops, and written feedback results, aiming to validate the information priorities and limitations.

The assessed information priority among the three actors and use cases was most of the time comparable to the evaluated safety criticality of the information. Therefore, if the information was safety critical, it was most likely to be considered priority information as well.

Aiming to validate the information priority results, an online survey was sent to the ADS developers before the workshop. Total of 8 responses were received. The developers were requested to answer whether they agree or disagree with the ODD attributes' prioritisation presented to them (Appendix 1). Provision of no response for an attribute would indicate agreement with the analysis of the researchers. In case of disagreement, the developers were requested to specify whether the attribute in question should have, on average, a low, medium, or high priority instead. Also, an open field response option was provided to enable respondents to further elaborate the answer. The survey results were further reflected in the workshops and written feedback. [3]

The survey results indicated mostly agreement with the researchers' analysis as over half of the respondents were in full agreement with the analysis of information priority levels and the feedback indicated high priority in general for most of the ODD attributes. [3]

One survey respondent's answer included over 90 % of the attribute's priority level being low. Also, some of the survey's open-field answers and discussion in the workshop among the ADS developers supported this feedback. The survey and workshop feedback stated, that use of external information requires not only trustworthiness of data both in terms of correctness and cybersecurity but also resolving any liability issues. For example, even if external information contributes to a crash of the vehicle in automated mode, the responsibility still resides with the ADS developer. [3]

Regarding the individual attributes, the remote human support ODD attribute (such as remote supervision of the automated vehicle), which was evaluated as high priority information in the research analysis, was considered low priority by half of the developers in the survey. Written and workshop feedback indicates that remote human support was partly considered being a more distant future service. Also, attributes that had slight deviation of priority level compared to the analysis were GNSS coverage unavailability, wind speed range, special challenging lightning conditions, wet pavement surface and road surface friction. For example, sudden wind speed changes can be very local and therefore changing in different parts of road sections as indicated in some of the comments and discussions. Other comments suggested that landmarks and GNSS positioning on the other hand would require highly accurate digital maps in order to provide benefits. The quality of pavement marking visibility was raised as an example by both the ADS developers and road authorities on how the ADS development is a constantly changing dynamic domain and reducing the importance of some attributes that were earlier identified as very important. [3]

### Data and information quality

The Distributed ODD Awareness (DOA) framework's quality criteria and needs for the traffic information for the three use cases were extracted after analysis from the European ITS Platform projects (EU EIP) [4], EU EIP C-ITS quality package [5], and Finnish Transport Infrastructure Agency reports [6]. The proposed quality criteria with explanation are presented in the Appendix 2 Table 8.

After the quality criteria analysis, tentative quality needs of the three use cases for the DOA framework were analysed. Finally, quality recommendations for the three use cases, presented in Table 1. below, were given. The recommendations are targeting a future situation when enough SAE Level 4 CAD vehicles are operating on the road to provide reasonable quality vehicle probe data. Therefore, the quality recommendations may be higher than the quality levels that road operators can provide today. [3]

*Table 1 Quality recommendations for the Distributed ODD Awareness framework concerning various variables.*

| Quality Criteria for Distributed ODD Awareness Framework | Traffic jam | Adverse weather | Road works |
|---|---|---|---|
| **Geographical coverage** | 100% on designated motorways with high traffic volumes | 100% on designated highways with frequent weather issues | 100% on highways at road works locations |
| **Availability** | 99% | 99% | 99% |
| **Performance conditions** | -50…+60℃ | -50…+60℃ | -50…+60℃ |
| **Coverage of data types** | traffic flow speed, occupancy | visibility, precipitation intensity and state of matter, road surface condition, wind (gust) speed, friction | location, status, local traffic management, lane availability, detour, trajectory |
| **Timeliness (start)** | < 2 min | <5 min | < 2 min |
| **Refreshment rate** | < 2 min | < 20 min | < 5 min |
| **Data transfer delay** | < 100 ms | < 100 ms | < 100 ms |
| **Timeliness (update)** | < 2 min | < 5 min | <2 min |
| **Latency (content side)** | <1 s (C-ITS)<br><10 s (NAP)<br><1 min (NAP event info) | <1 s (C-ITS)<br><10 s (NAP)<br><1 min (NAP event info) | <1 s (C-ITS)<br><10 s (NAP)<br><1 min (NAP event info) |
| **Location accuracy** | 10 m | 100 m | 10 cm (trajectory) … 10 m (others) |
| **Monitoring point density** | each link between major intersections | critical microclimate spots, otherwise 50 km | start and end of road works |
| **Measurement accuracy** | depends on indicator | depends on indicator | depends on indicator |
| **Reporting accuracy** | ± 5% | ± 10% | ± 5% |
| **Error Rate** | < 5% | < 8% | < 5% |
| **Classification correctness (non-false positives)** | 96% | 92% | 99% |
| **Event coverage (true positives)** | 94% | 90% | 98% |
| **Missed events (false negatives)** | 4% | 5% | 2% |
| **Report coverage** | 97% | 97% | 97% |

The road operators have compiled the quality monitoring and management methods currently used for the information services used by them or utilising their own information systems in the EU EIP Quality Package [4]. The methods compiled are listed below in Table 2. [3]

***Table 2 Quality recommendations for the Distributed ODD Awareness framework concerning various variables.***

| Nr | Method | Objective | | | | Coverage of value chain | | | | Assessment / assu-rance | | Event / status | | Type of service / equip-ment | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Assessment of service | Acceptance testing | Feasibility / testing new procedure of algorithm | Internal quality control / monitoring | Content detection | Content processing | Service provision | Service presentation | Quality assurance | Quality assessment | Event | Status | Equipment | Process |
| **1** | Continuous monitoring of equipment performance and availability | X | X | X | X | X | | | | X | | X | X | X | |
| **2** | Manual verification of events or conditions | X | X | X | X | X | X | X | X | | X | X | | X | X |
| **3** | Reference testing of data collected | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| **4** | Time-space oriented reference test methods | X | | | X | X | | X | | | X | X | | | X |
| **5** | Monitoring of data completeness and latency | X | | | X | X | X | X | | X | X | X | X | X | X |
| **6** | Regular sampling of message or data content comp-leteness and correctness | | | | X | | X | | | X | | X | | | X |
| **7** | Verification and calibration of traffic / weather conditions prognosis | X | X | X | X | | X | X | X | X | X | X | X | | X |
| **8** | Surveys of perceived quality by users | X | | | X | X | X | X | X | | X | X | X | X | X |
| **9** | Collection of direct user feedback | X | | | | X | X | X | X | X | | X | X | X | X |
| **10** | Monitoring of service use statistics | X | | | | | | X | X | X | X | X | X | | X |

**DISCUSSION**

The first research question of the study was ´what kind of information is to be transmitted in the interaction (in both directions) between traffic management centre (TMC) and vehicle? ´ The results are presented in the Appendix 1 Tables 4.-7. where information to be transmitted as a priority has an attribute information priority level HIGH. According to the survey, which was distributed to the Automated Driving System (ADS) developers before workshop, over half of the ADS developer respondents agreed with the information priority

level analysis. Uncertainty and the dynamic nature of the AV development was reflected some responses, where some uncertain future developments were considered less important for that reason.

The second research question was 'which information is to be provided by the National Road Authorities (NRA)/roadside and which information can be obtained by the sensors of the moving vehicle itself?'
The ADS developers indicated trust concerns on infrastructure communication data reliability and possible liability issues if an accident happens due to faulty information. Therefore, infrastructure information quality can have high importance, but possible backup and redundancy of the infrastructure information monitoring would be required. If the information would come from inside the vehicle sensor range, it could be used for redundancy. On the other hand, information coming from outside of the vehicle's sensor range could be used to extend the geographical area of the ODD if the ADS is convinced of the veracity and reliability of the information. Also, the dynamic nature of weather conditions and possible variations in measuring these conditions such as the pavement friction and wet conditions also relates to the first mentioned trust issues with the information. [3]

The long-term assessment of the importance and need of the ODD attributes is considered difficult due to the wide range of the attributes and possible data fusion between attributes, i.e., when multiple data attributes are combined to produce more accurate information for the use of ADS decision making. Also, governance and harmonisation of data exchange between the actors need to be considered. The best indication of the current and possible future development can be gathered from the latest development projects addressing the key challenges currently hindering the progress of developments in vehicle automation and ODD continuity. [3]

The third research question was ´when and how should such information be available? ´ Table 3. below presents the time-related quality recommendations picked from the Results chapter's table 1. The overall DOA information exchange was evaluated of being available for Level 3 and 4 vehicles for 99% of the time in the future with considerable traffic flow penetration of such vehicles. [3]

***Table 3 Time-related quality recommendations for the Distributed ODD Awareness framework in the future concerning various use cases on highways and motorways.***

| **Quality Criteria for Distributed ODD Awareness Framework** | **Traffic jam** | **Adverse weather** | **Road works** |
|---|---|---|---|
| Availability | 99% | 99% | 99% |
| Timeliness (start) | < 2 min | <5 min | < 2 min |
| Refresh interval | < 2 min | < 20 min | < 20 min |
| Data transfer delay | < 100 ms | < 100 ms | < 100 ms |
| Timeliness (update) | < 2 min | < 5 min | <2 min |
| Latency (content side) | <1 s (C-ITS)<br><10 s (NAP)<br><1 min (NAP event info) | <1 s (C-ITS)<br><10 s (NAP)<br><1 min (NAP event info) | <1 s (C-ITS)<br><10 s (NAP)<br><1 min (NAP event info) |

The fourth research question was ´how to define and measure the quality/correctness of such information? ´ The quality recommendations followed the EU EIP Quality Package [4], which can be found from the Appendix 2 Table 8. As discussed above, the data quality has an important role on possible ADS developers' trust issues towards the infrastructure communication and should therefore be further developed and tested in future.

Limitations of the survey answers include some of the open field written answers that highlighted urban use case examples and role of the road operator. The research and survey scope were oriented only to highway and motorway use cases and the ADS developers' views. Also, difficulties and cost for providing each of the individual ODD attribute information elements was reflected, which were not considered part of the information priority analysis. [2]

## CONCLUSIONS

The study investigated how infrastructure connectivity could contribute toward improving AV safety in three selected use case scenarios of traffic jam, adverse weather and static/dynamic road works, and quality indicators and requirements for the communication. Three actors were selected for the use case evaluation: road works or (winter) maintenance operator, traffic manager and ADS developer.

The main findings of the research can be found from the Appendix 1 Tables 4.-7. where the assessed ODD attributes' priority levels are presented: attributes with 'HIGH' priority level were considered important information to transfer. The evaluated priority attributes were also consistently being evaluated as safety critical. Also, survey and workshop inputs and the ADS developers supported the results as a majority of the answerers agreed with the research evaluation.

According to the AV industry feedback in the survey and workshop, the vehicle manufacturers and ADS developers mainly rely on the information that the vehicle's own sensors provide. This is done especially for road safety and liability reasons. Any external ODD or local condition information from infrastructure can bring redundancy, i.e., backup for the automated driving systems, but the trustworthiness of the information is a concern because the manufacturer bears the responsibility of the outcome of using the information when the vehicle is used in the automated mode. [3]

## ACKNOWLEDGEMENTS

The research was part of the Traffic Management for Connected and Automated Driving (TM4CAD) project funded by the Conference of European Directors of Roads (CEDR) Transnational Research Programme (TRP) Call 2020 Impact of CAD on Safe Smart Roads.

## REFERENCES

[1] CEDR Research Call 2020 [website]. 2020. "CEDR Research Call 2020 is open!" Available online: https://www.cedr.eu/17852/cedr-research-call-2020/

[2] Khastgir, S., Shladover, S., Vreeswijk, J., Kulmala, R. and Wijbenga, A. 2022. "Report on distributed ODD awareness, infrastructure support and governance structure to ensure ODD compatibility of automated driving systems." TM4CAD Deliverable D2.1. March 2022. Available online: https://tm4cad.project.cedr.eu/deliverables/TM4CAD%20D2.1_submitted.pdf

[3] Traffic Management for Connected and Automated Driving (TM4CAD) Deliverable D3.1. 2022. Information exchange between traffic management centres and automated vehicles – information needs, quality, and governance. Version 0.95 (unpublished). 8 October 2022.

[4] Kulmala, R., Öörni, R., Laine, T., Lubrich, P., Schirokoff, A., Hendriks, T. and Rystrøm, L. 2019. "Quality of Safety-Related and Real-Time Traffic Information Services. Quality package." European ITS Platform, EU EIP SA 4.1: Determining Quality of European ITS Services. 81 p. Version: 2.0, May 15, 2019.

[5] Lubrich, P., Geissler, T., Öörni, R. and Rystrøm, L. 2022. "C-ITS Quality Package." Version 1.0, January 21, 2022. European ITS Platform, EU EIP SA 4.1: Determining Quality of European ITS Services. 73 p. Available online: https://www.its-platform.eu/wp-content/uploads/ITS-Platform/AchievementsDocuments/Quality%20Frameworks/EU%20EIP%204.1_C-ITS%20Quality%20Package%20v1.0_20220121.pdf

[6] FTIA. 2022. "Tieliikenteen vaihtuvan ohjauksen ja seurantajärjestelmien palvelutasot [Service levels for dynamic road traffic management and monitoring systems; In Finnish]." Väylävirasto – Finnish Transport Infrastructure Agency. Väyläviraston julkaisuja 10/2022. 82 p. Available online: https://www.doria.fi/bitstream/handle/10024/183717/vj_2022-10_tieliikenteen_vaihtuvan_ohjauksen_web.pdf

**APPENDIX 1**

***Table 4 Priority levels of physical attributes of the roadway and its environs.***

| **Physical attributes of the roadway and its environs** | **Priority level** |
|---|---|
| Locations of road boundaries | HIGH |
| Zone boundaries | HIGH |
| Roadside landmarks | HIGH |
| Special-purpose localization references | LOW |
| Quality of pavement marking visibility | HIGH |
| Load-bearing capacity of roadway or bridge structures | MEDIUM |
| Road surface damage | MEDIUM |
| Game fence locations and condition | LOW |
| Vegetation obscuring sight angles or visibility of signs | MEDIUM |
| Road geometry constraints | HIGH |
| Road shoulder conditions on both sides | HIGH |
| Notifications of locations with occluded visibility | HIGH |

***Table 5 Priority levels of digital infrastructure support variables.***

| **Digital infrastructure support** | **Priority level** |
|---|---|
| Variable message sign contents | HIGH |
| Locations where V2I/I2V communications are available | HIGH |
| Locations where GNSS differential correction signals are available | MEDIUM |
| Locations where GNSS coverage is NOT available now, by GNSS service | MEDIUM |
| Electronic toll collection systems and their associated pricing | LOW |
| Locations of incidents that represent traffic impediments or safety hazards | HIGH |
| Emergency vehicle locations and direction/speed of travel of each one | MEDIUM |
| Current average traffic speed and density by lane and road section | HIGH |
| Current percentage of heavy vehicles in traffic stream, by lane and road section | LOW |
| Special events creating abnormal traffic conditions and their locations | HIGH |
| Temporarily blocked or closed road locations | HIGH |
| Locations with high density of pedestrians | LOW |
| Locations with high density of cyclists or users of micro-mobility devices | LOW |
| Highway shoulder locations occupied by vehicles or debris | HIGH |
| Locations with dynamic traffic access changes | HIGH |
| Remote human support | MEDIUM |

*Table 6 Priority levels of dynamically varying ambient environmental condition variables.*

| Dynamically varying ambient environmental conditions | Priority level |
|---|---|
| Wind speed range | MEDIUM |
| Visibility range with rain/snow/sleet/hail in visible light spectrum | HIGH |
| Visibility range with rain/snow/sleet/hail in lidar infrared spectrum | HIGH |
| Rainfall rate in mm/hr | HIGH |
| Snowfall rate in qualitative ranges | HIGH |
| Visibility range with other particulate obscurants in visible light spectrum | HIGH |
| Visibility range with other particulate obscurants in lidar infrared spectrum | HIGH |
| Predicted significant changes in key weather attributes | HIGH |
| Qualitative ambient lighting conditions | LOW |
| Quantitative ambient lighting conditions | MEDIUM |
| Special challenging lighting conditions | MEDIUM |
| Electromagnetic interference | HIGH |
| Wet pavement surface | HIGH |
| Ice on pavement surface | HIGH |
| Cold pavement surface (potential for ice if wet) | HIGH |
| Road surface friction | HIGH |
| Light to moderate snow/slush accumulation on surface | HIGH |
| Heavy snow/slush accumulation on surface | HIGH |
| Light to moderate flooding (puddles) on surface | HIGH |
| Heavy flooding – potentially impassable to low-profile vehicles | HIGH |

*Table 7 Priority levels of operational attributes of the roadway.*

| Operational attributes of the roadway | Priority level |
|---|---|
| Temporary static signs | HIGH |
| Maintenance vehicles using portions of carriageway | HIGH |
| Work zones | HIGH |
| Incident recovery events (crash scenes, crime scenes, dropped loads, landslides, avalanches…) | HIGH |
| Availability of specific C-ITS information services | HIGH |
| Availability of real-time merging guidance or assistance at motorway interchanges or entrance ramps | HIGH |
| Real-time lane-specific speed limit information availability at specific locations. | HIGH |
| Obstacles or debris on road surface | HIGH |
| Roadside objects that change their locations over time, such as parked vehicles or trash cans | MEDIUM |
| Routing advisory information | MEDIUM |
| Traffic rules and regulations in digital form, updated in real time | HIGH |

**APPENDIX 2**

***Table 8 Proposed quality criteria for the Distributed ODD Awareness framework and the data exchanged.***

| Definition of Quality Criteria for Distributed ODD Awareness Framework | | Applicable for | | |
|---|---|---|---|---|
| | | **Event Information** | **Status-Oriented Information** | **DOA Framework** |
| **Geographical coverage** | Percentage of the road network or link covered by the (content provision) service | - | - | X |
| **Availability** | Percentage of the time the (content provision) service is available | - | - | X |
| **Performance conditions** | The conditions in which the system operation and performance is guaranteed | - | - | X |
| **Coverage of data types** | Data or sensor types required | - | - | X |
| **Timeliness (start)** | The time between the occurrence of an event and the acceptance* of the event | X | - | |
| **Refreshment rate** | Time interval for refreshing / updating the status reports coming from a data sender | - | X | |
| **Data transfer delay** | The time from transmission of data from monitoring station to the receipt of data at server | X | X | |
| **Timeliness (update)** | The time between the end or (safety) relevant change of condition and the acceptance* of this change | X | - | |
| | The average age of the sensor data used in the most recent reporting period | X | X | |
| **Latency (content side)** | The time between the acceptance of the event or its end or (safety) relevant change of condition and the moment the information is provided by the content access point | X | - | |
| | The time between the calculation of the reporting data and the moment the information is provided by the content access point | - | X | |
| **Location accuracy** | The relative accuracy of the referenced location with respect to the actual location of the actual event | X | X | |
| **Monitoring point density** | Minimum density of monitoring stations on road section or maximum link length for link-related data in operating environment | X | X | |
| **Measurement accuracy** | Minimum accuracy for displaying data monitored | - | X | |
| **Reporting accuracy** | The relative accuracy of the reported quantity (speed or travel time) versus the actual value (average experience of road users in a given reporting period) | - | X | |
| **Error Rate** | Percentage of published status reports which fall below a minimum accuracy | - | X | |
| **Classification correctness (non-false positives)** | 100% - percentage of the published events which are known to be not correct (concerning actual occurrence of this event type / class), and which result in a consequence for the user behaviour | X | - | |
| **Event coverage (true positives)** | Percentage of the events which are known to be correctly detected and published by type / class, time and location (i.e. detection rate) | X | - | |
| **Missed events (false negatives)** | Percentage of occurred events that were not published (and perhaps not even detected) | X | | |
| **Report coverage** | The percentage of reporting locations for which a status report is received in any given reporting period | - | X | |

# TRANSFER OF RECONSTRUCTED REAL-WORLD ACCIDENT DATA INTO SCENARIO CATALOGUES FOR THE DEVELOPMENT AND TEST OF ADAS AND ADS

**Marcus Petzold**
**Thomas Unger**
**Henrik Liers**
Institute for Traffic Accident Research at Dresden University of Technology (VUFO)
Germany

Paper Number 23-0320

## ABSTRACT

The development and test of ADAS and Automated Driving Systems (ADS) require appropriate scenario data. To ensure the correct functionality and functional safety of such systems, an incredible amount of scenarios is necessary, containing normal, critical, and accident situations. These scenarios are usually used for virtual simulations. However, selected scenarios should be also physically tested on proving grounds. We developed a method to extract and describe maneuver-based and parameterized scenario catalogues for development and test of ADAS and ADS.

We used real accident data from GIDAS (German In-Depth Accident Study). The focus was on car accidents in urban areas as the complexity in urban traffic is much higher than on highways (heterogeneous infrastructure, large variety of road users and behavior).

At first, we clustered the (weighted) GIDAS accidents into different scenario groups. Then, we identified relevant parameters that are necessary for the description of the static and dynamic content of scenarios. The static content was extracted within the “environment analysis”. With this, the scenarios can be parameterized in terms of weather and lighting conditions, road layout (e.g. number of lanes, road width etc.).

For the “dynamic analysis” we additionally used the GIDAS-PCM, containing reconstructed maneuvers, time- and location-resolved trajectories, accident sequences. Here, we generated statistical descriptions about speeds, trajectories, braking or steering maneuvers.

Finally, some concrete example scenarios have been transferred to IPG CarMaker and OpenDRIVE / OpenSCENARIO files.

With the developed method it is possible to transfer thousands of single traffic events and/or accidents with concrete characteristics into generic (test) scenarios. Within the project, scenario groups have been created using a maneuver-based approach. There are currently four main categories (following in one lane, crossing scenarios, turning scenarios, and lane change) which are further divided into sub-maneuver groups.

The created parameter sets per scenario group contain several static and dynamic parameters. These distributions can be used by system engineers for virtual simulation runs (e.g. with randomly varied scenarios) but also by test engineers to parameterize physical tests. The approach was already tested with partners with demonstrations in physical tests.

The implementation in concrete formats (IPG CarMaker, OpenX) showed that an automated transfer is not possible at the moment due to the complexity and multitude of implementation options. The developed method works for accident data out of GIDAS and was already tested in physical tests. However, the method was not yet applied to normal/critical situations but this should also work with the presented static and dynamic parameter sets. Another limitation is the lack of automatic data transfer from the PCM format into the open ASAM standards (OpenX).

As scenario catalogues are essential for virtual simulations as well as for physical tests of ADAS and AD functions the presented method helps to provide appropriate scenario data out of real-world accidents. The big advantage is that the created parameter sets and scenarios base on reconstructed accident data and can be used independently from certain software solution or format.

## PREFACE

The methodology of the scenario catalogue generation was developed as part of the BMVI-funded project *„Ervast - Einsatz dynamischer Verkehrselemente für die Prüfung automatisierter Fahrfunktionen"*.. Project goals were:

- Development of test technologies and tools
- Manufacturer and vehicle model-independent testing of automated and connected assistance and driving functions
- Verification of correct and reliable environment detection, e.g. by means of dynamic traffic elements

## RESEARCH QUESTIONS / OBJECTIVES

For the development and testing of ADAS and automated driving systems (ADS), appropriate scenario data is required. To ensure the correct functionality and functional safety of such systems, an incredible amount of scenarios is required, including normal, critical and accident situations. These scenarios are typically used for virtual simulations. However, selected scenarios should also be physically tested on a test site. We have developed a method for extracting and describing maneuver-based and parameterized scenario catalogues based on real accident data, which can be used to answer the following research questions:

- Which speed ranges should be considered?
- Which trajectories of motion should be tested?
- Which space requirements are needed for different scenarios?
- Which dynamic requirements can be derived for the target?

## OVERVIEW OF DATA SOURCES

In order to adequately test automated and connected driving functions, a vehicle model-specific design of the test scenario is necessary. These test scenarios must be generated for the investigation of the system's or function's effectiveness. In the project, in addition to existing homologation regulations (e.g. ECE regulations) or test protocols (e.g. NCAP), real driving data and accident data were also applied and processed for scenario generation.

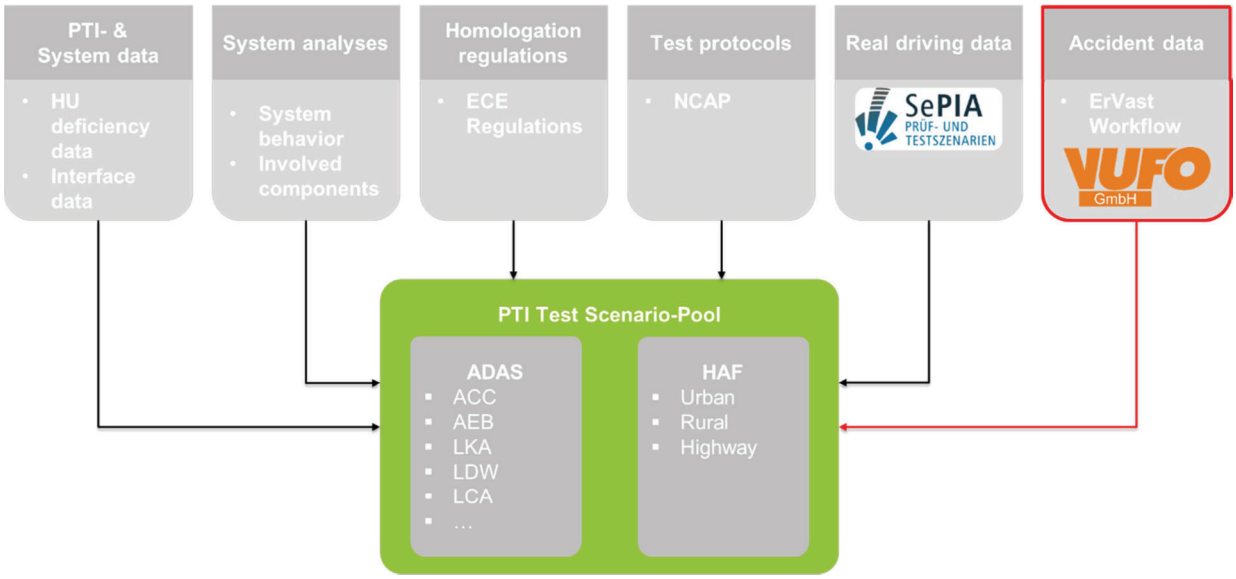



***Figure 1:*** **Overview of data sources**

The goal of the scenario generation is to develop relevant and representative scenarios for the PTI test scenario pool. It is important that on the one hand a parameter set is created for a test scenario, which the testers can apply in a real test scenario. For example, do define the speed range in which the test takes place, or should a steering and/or braking maneuver must be initiated. On the other hand, it is necessary to simulate the scenarios virtually, for example to determine the space requirements for selected scenarios, to virtually secure the test scenario (feasibility), or to control the target carrier. In this paper we present some methodologies for the transfer of test scenarios from different data sources. The main focus is the scenario generation based on real accident data.

**Real driving data**
For the development of scenarios for testing automated driving functions, the normal driving behavior of today's drivers in real road traffic is the relevant reference value. In the SePIA project, standardized processes for generating test scenarios based on real driving data were generated in this context. The results obtained in this process provided valuable input for the creation of the scenarios in the ErVast project. Examples of simple scenarios for automated driving functions are intersection scenarios without traffic signals or traffic signs, or approaching traffic signals.

**Test protocols, homologation regulations and standards**
Some test procedures for assisting vehicle systems already exist. In both, the type approval process and in consumer protection programs (e.g. EuroNCAP), scenarios are described and test conditions are formulated in protocols. Within the scope of the project, these data were also used as a basis. An analysis of the test protocols was carried out with the aim of obtaining the relevant parameters for the test scenarios and test conditions and transferring them to the project format. One difficulty for the ErVast approach here was the large variance in functionality of systems from different vehicle manufacturers. Due to the increasing regulation of system functionalities and the resulting standardized functionality, test scenarios can also be derived across vehicle models.

**PTI system data, System analyses**
In order to be able to provide the testing organizations with specifications for the performance of the general inspection, detailed knowledge of the electronic systems installed in the vehicle, vehicle diagnostic data, and information about the installed components is essential. The provision of this data by vehicle manufacturers is ensured throughout Europe via regulation. The expertise in handling this data could be used in the project. A meta-analysis of component location plans and usable diagnostic data via the electronic vehicle interface was carried out as a basis for the development of test concepts.

**Real accident data from in-depth investigations**
The main focus of this paper is the scenario generation based on real accident data. The GIDAS (German In-Depth Accident Study) database was chosen as basis, since this database has a very high level of detail with approximately 38,300 accidents (as of June 30, 2020) and about 3,500 single information per traffic accident. The database contains, for example, information on the accident environment (e.g. location, road type and markings, weather data), as well as reconstruction data for the participants (e.g. speeds, accelerations, maneuvers) which are of crucial importance for the scenario generation. Furthermore, it is possible to derive representative statements for the German accident scenario by applying a weighting procedure. The coupling to the simulation database GIDAS-PCM (Pre-Crash-Matrix) offers the possibility to analyze detailed time- and location-resolved information about the trajectories of the accident participants [2].

## METHODS

At the beginning, the accidents in GIDAS were weighted towards the German accident occurrence of 2019. Then, an analysis was performed based on the accident type, as well as a classification into scenario groups. The scenario groups were composed as follows. The project focused on urban accidents. As the scenarios should be used for PTIs of passenger cars, at least one passenger car must be involved in the accident. Furthermore, assistance systems that react to another road user should be examined. Thus, at least one other road user must be involved in the accident. These filter criteria limit the GIDAS data set within the project and lead to a first approach of an accident-based test scenario catalogue, which is illustrated in *Figure 2*.

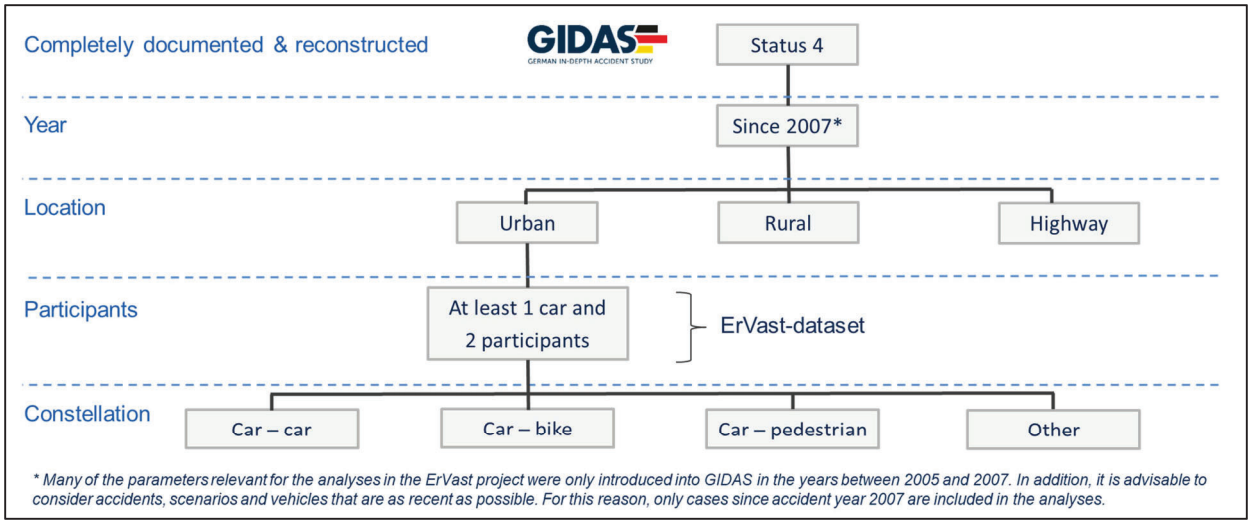



***Figure 2:*** **Filter criteria and categorization of accidents**

In the next step, the accident types of the ErVast data set were analyzed and evaluated. The following figure shows an overview of the 10 most frequent accident types for passenger cars in urban accidents.

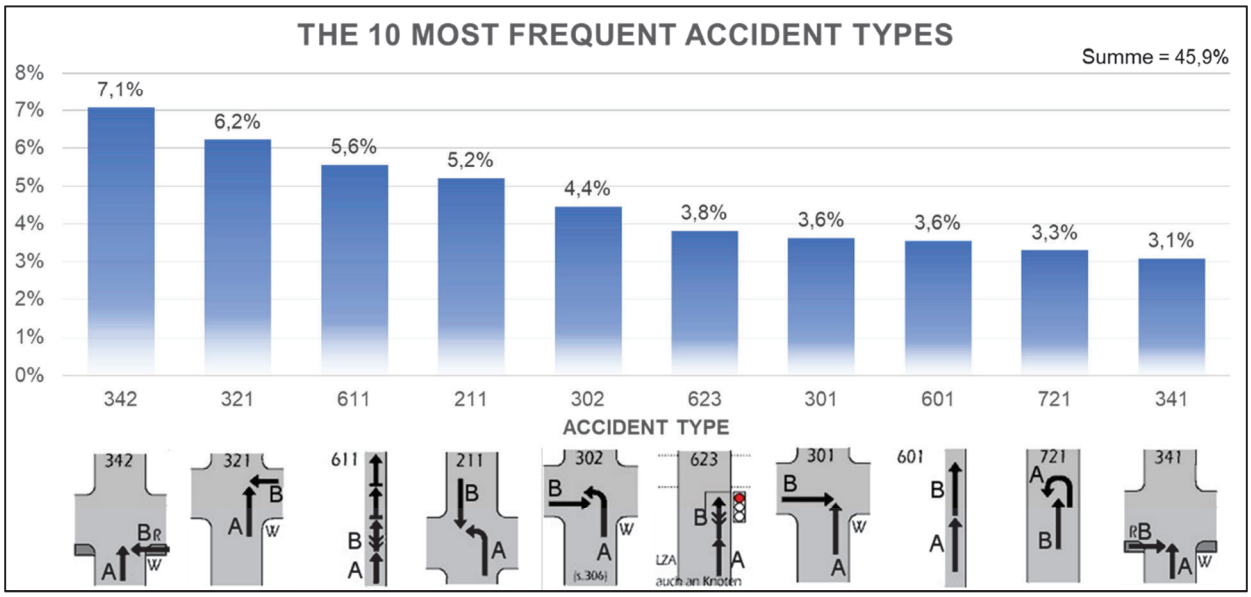



***Figure 3:*** **10 most frequent accident types in the considered dataset of urban car accidents**

It can be seen that the analysis of the top 10 accident types already addresses almost half of all accidents (45.9%) in the ErVast dataset. In addition, the figure shows a great variety in the definitions of the accident types. For example, accident type 342 represents a passenger car and crossing bicyclist, accident type 321 includes a crossing of two participants regardless of the type of involved road users, and accident type 611 describes a longitudinal traffic accident, which is also independent of the road user types. For further analyses, it is therefore necessary to divide the data set according to the type of road user. The focus was on test scenarios for passenger cars (cars), so the data set was limited to the constellations "Car - car", "Car - bike", "Car - pedestrian" and "Other".

In a further step, additional corresponding accident types were identified in GIDAS for the identified scenario groups and added to the groups. The method is summarized in the following figure.

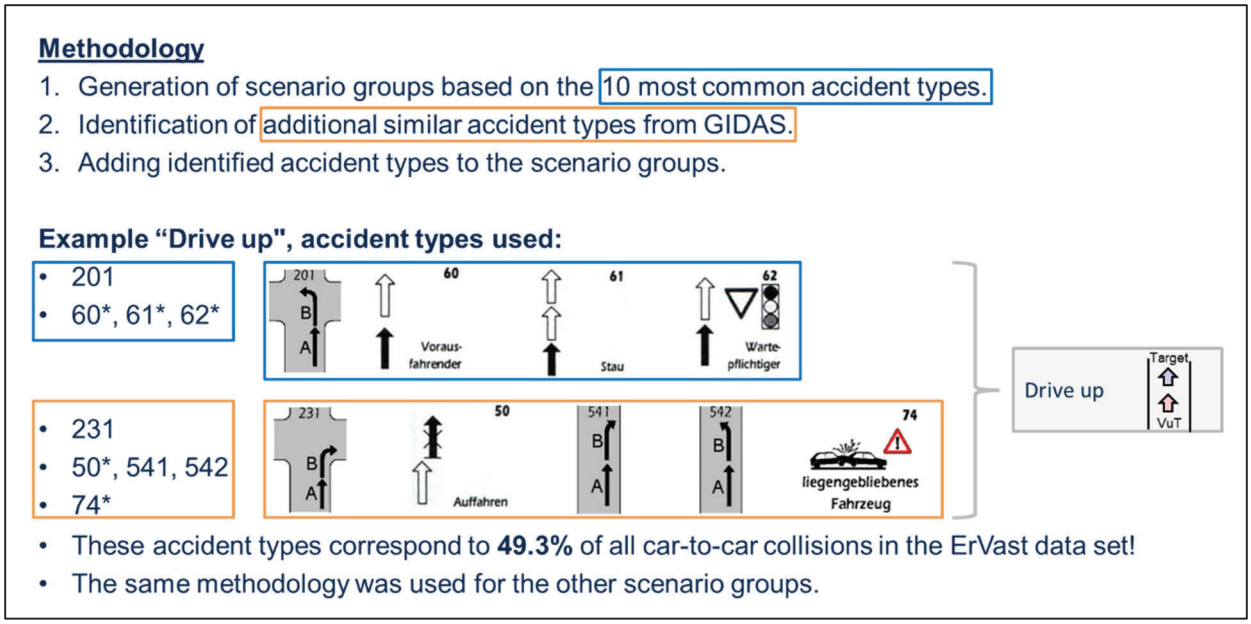



*Figure 4:* **Methodology for the generation of the accident-based test scenario catalogue**

The analyses within the scope of the project lead to the following test scenario catalogue:

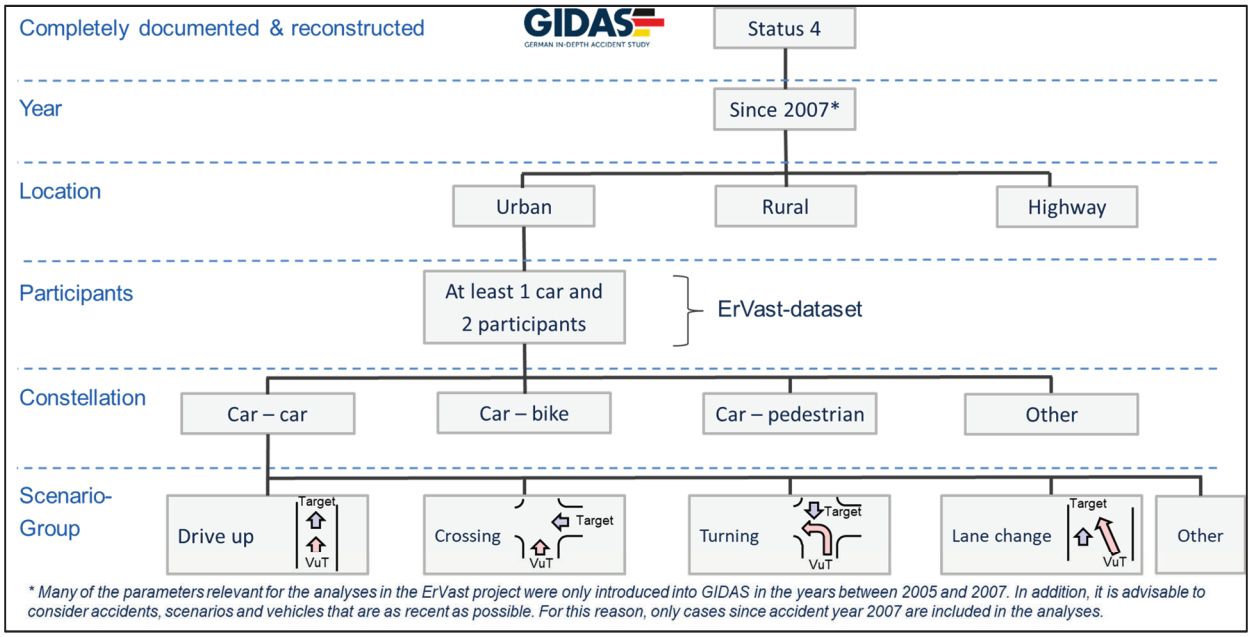



*Figure 5:* **Accident-based test scenario catalogue**

For in-depth analyses and to be able to derive test scenarios (especially maneuvers and associated dynamics data) based on real accident data, it is necessary to use another database, the GIDAS-PCM. This database contains reconstructed, time-dependent motion trajectories of the accident participants based on the accidents of the GIDAS database. The accident trajectories of the involved participants in the initial collision are considered. Based on the time- and location-resolved trajectories and the corresponding stored data of the accident participants, this database is suitable for a detailed dynamics analysis of the scenario groups. At the time of the project, the GIDAS-PCM contained approximately 10,300 accident scenarios. For car-vehicle collisions, a total of 1,951 cases could be identified for the analysis.

For the respective scenario groups, it was necessary to create further clusters for a more detailed description of the accident scenarios to analyze them with regard to characteristic features. For this step it was necessary to develop a maneuver catalogue with defined limits. In *Figure 6* the maneuver catalogue is shown.

| MID | lateral | longitudinal | Motion | MID | lateral | longitudinal | Motion | MID | lateral | longitudinal | Motion |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Straight | Forward | Constant | 8 | Left | Forward | Constant | 14 | Right | Forward | Constant |
| 2 | Straight | Forward | Accelerated | 9 | Left | Forward | Accelerated | 15 | Right | Forward | Accelerated |
| 3 | Straight | Forward | Decelerated | 10 | Left | Forward | Decelerated | 16 | Right | Forward | Decelerated |
| 4 | Straight | Backward | Constant | 11 | Left | Backward | Constant | 17 | Right | Backward | Constant |
| 5 | Straight | Backward | Accelerated | 12 | Left | Backward | Accelerated | 18 | Right | Backward | Accelerated |
| 6 | Straight | Backward | Decelerated | 13 | Left | Backward | Decelerated | 19 | Right | Backward | Decelerated |
| 7 | - | - | Standstill | | | | | | | | |

***Figure 6:*** **Maneuver catalogue**

The maneuver catalogue describes the movement and the direction (longitudinal/lateral) of a participant and assigns it to a maneuver identifier (MID). Thus, it is possible to assign a MID to each participant, at each time step, in the GIDAS-PCM. The goal is to subdivide a scenario group into maneuver variants to analyze and describe the maneuvers separately for the VUT and target. By analyzing the single maneuvers and also their combination these results could be done. Figure 7 shows an overview of the additional maneuver variants.

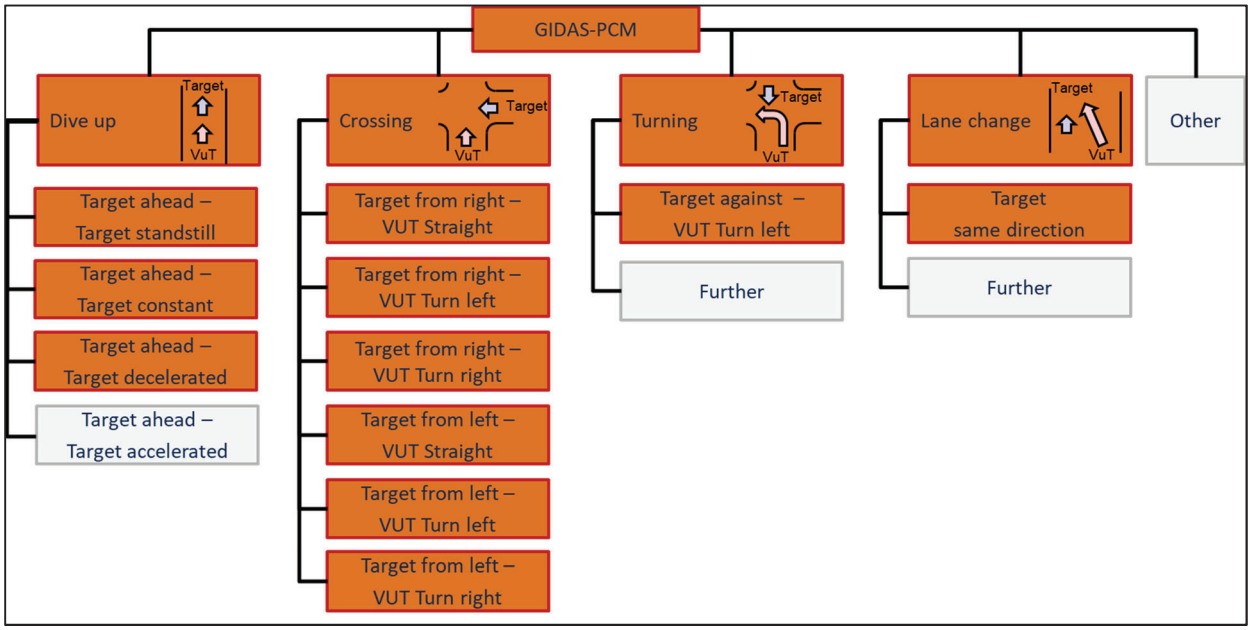



***Figure 7:*** **Maneuver variants in the scenario groups**

In the figure above, the analyzed scenarios are shown in orange. Scenarios with a gray background were not considered. For all clusters and their corresponding cases a clear assignment of the VUT and the target is included. This allows for the separate dynamics and environment analyses.

In the next step, the GIDAS-PCM was analyzed with respect to the following parameters:

- Trajectories
- Speeds
    - Start speed: Start of simulation
    - Initial speed: speed before critical scenario
    - Collision speed
- Vehicle accelerations
- Vehicle alignment
- Center of gravity positions of the vehicles
- Distances covered in the GIDAS-PCM

The analysis of dynamic parameters does not provide all necessary information and general conditions for the tests. Thus, an additional analysis regarding environmental aspects was done. Therefore, the same basic (GIDAS) master-dataset was used.

With the environment analysis, general information and conditions for the entire scenario can be extracted, e.g. lighting conditions, surrounding infrastructure, road layout etc. In addition, statements can be made which only apply to the VUT or only to the target, e.g. number of lanes or road width. The following variables were investigated.

- Lighting conditions
- Infrastructure
- Number of lanes
- Lane layout
- Road and lane width
- Marking lane
- Road condition and surface
- Type of traffic regulation
- Maximum permitted speed / type of speed limit
- Visual obstruction / type of visual obstruction

**RESULTS**

All analyzed parameters were stored in the form of diagrams and data tables and serve as parameter sets for the creation of real and virtual test scenarios. The following figure shows some evaluation examples for a crossing scenario.

**The left diagram in**

*Figure 8* shows the trajectories of the two relevant road users. The colors represent the frequencies of different trajectories (red: very frequent; blue: rare). The second diagram (mid, left) shows boxplots with the relevant speed distributions of the vehicles (blue: Target vehicle, red: VUT) for three different sub-scenarios (I: VUT is driving with constant speed, II: VUT is starting and accelerating, III: VUT is decelerating prior to the collision). The third diagram (mid, right) shows a distribution of the different road elements where the considered crossing accidents happened (e.g. X-Crossing, T-junction, property exit). The right diagram displays another infrastructure parameter which is very relevant for the definition of actual test scenarios. It shows the distribution of the road width in boxplots.

These four diagrams show only a small part of the variety of analyzed parameters. Besides the dynamic parameters and infrastructure variables mentioned above, there are many more parameters characterizing available.

With such results it is now possible to derive a variety of relevant test scenarios. On the one hand side, legislation and homologation authorities or test organizations can choose the "median scenario", using the median values from the boxplots and the "average conditions". On the other hand side, corner cases could be defined by using the outermost values of each distribution, e.g. by consumer protection agencies that want to promote the most effective systems and functions in the market.

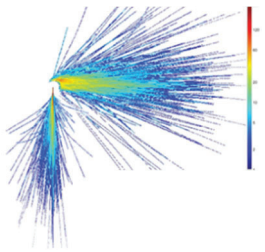
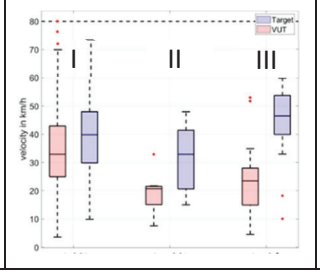
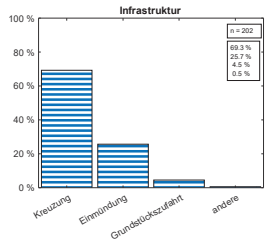
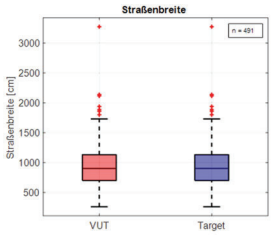
| Trajectories | Initial speed | Infrastructure element | Road width |
|---|---|---|---|
|  |  |  |  |

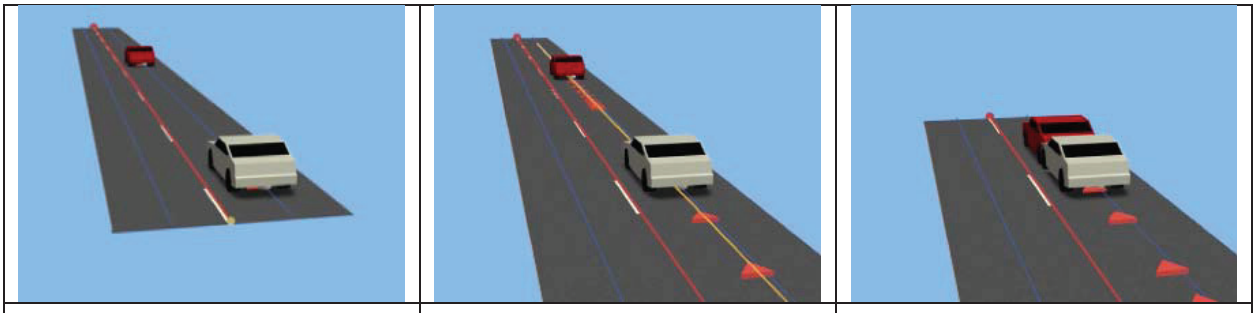
***Figure 8:*** **Results of parameter analyses for a crossing scenario**

Based on the created parameter sets, the transfer from concrete (real) accidents to generic test scenarios was done. Additionally, some selected scenarios have been further processed to demonstrate the complete tool chain from scenario extraction to the transfer in usable format for test beds.

Therefore, three different scenarios were selected for a transfer to CarMaker and OpenDRIVE / OpenSCENARIO:

- Rear-end collision - Target ahead, target decelerating
- Lane change - Target in same direction
- Left turn across path (LTAP) - Target in oncoming lane, VUT turs left

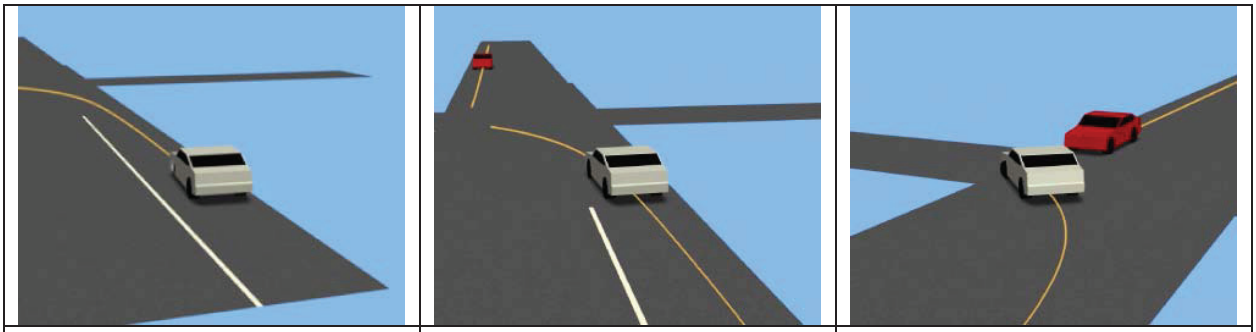
The following figure shows the rear-end collision scenario as OpenDrive / OpenSCENARIO in ESMINI.



| T=0s | T=4,8s | T=9,8s |
|---|---|---|

***Figure 9:*** **"Rear-end collision"-Scenario w/o ADAS / ADS as OpenDRIVE / OpenSCENARIO in ESMINI**

The following figure shows the LTAP scenario as OpenDRIVE / OpenSCENARIO in ESMINI.



| T=0s | T=4,8s | T=9,8s |
|---|---|---|

***Figure 10:*** **"LTAP"-Scenario w/o ADAS / ADS as OpenDRIVE / OpenSCENARIO in ESMINI**

Based on the median values of the data analyses, CarMaker, OpenDRIVE and OpenSCENARIO files could be created and successfully embedded in the further tool chains for all three scenarios. Furthermore, a variation of the dynamic values for the scenario "Rear-end collision" was carried out in CarMaker. Three variations were made to the scenario, with one parameter being changed for each variation:

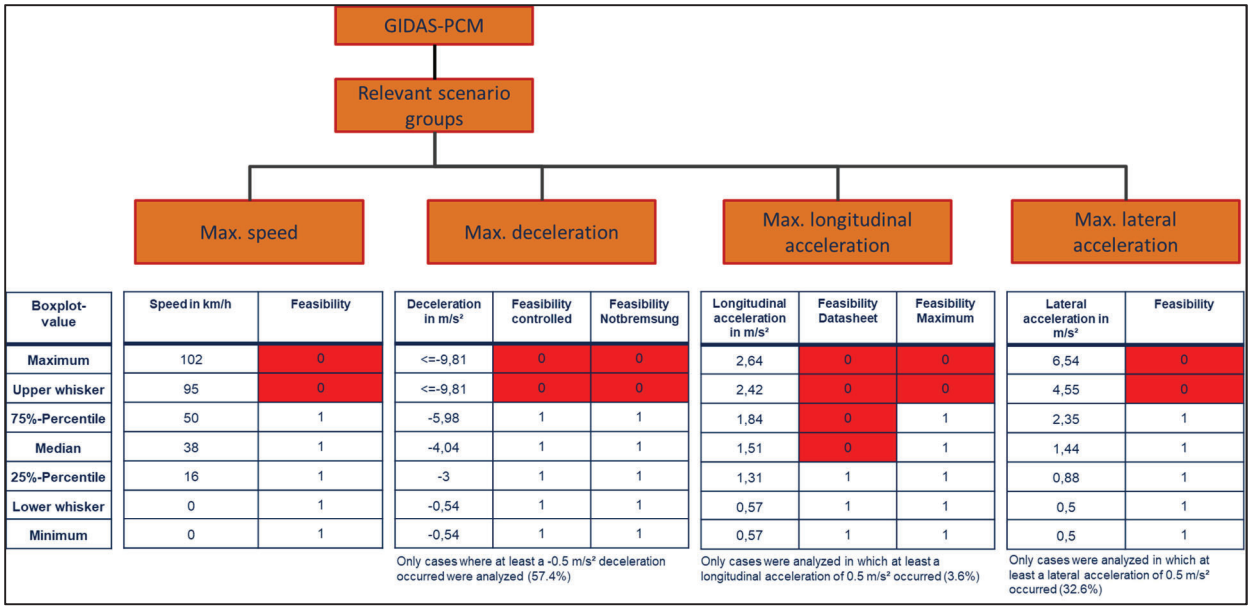
- Deceleration of the target vehicle
- Initial speed of the VUT
- Variation of the trajectories

The decisive factor after the variation is the testing of the newly generated scenario. The goal of this test is collision avoidance through a specific system intervention. The simulation could be carried out successfully for the three variations in CarMaker.

Finally, it was checked whether the values of the dynamics analysis could be realized with the target carrier. For this purpose, the technical data of the target carrier were compared with the boxplot values of the dynamics analysis of the entire ErVast data set and then with the entire GIDAS-PCM 2020-1 data set. For this purpose, the maximum of the following parameters was considered:

- Speed
- Deceleration
- Longitudinal acceleration
- Lateral acceleration

The figure below shows the results of the analysis of the ErVast dataset. In the "Feasibility" column, the variable "0" stands for not feasible and "1" for feasible in terms of the technical abilities of the target.




| Boxplot-value | Speed in km/h | Feasibility |
|---|---|---|
| Maximum | 102 | 0 |
| Upper whisker | 95 | 0 |
| 75%-Percentile | 50 | 1 |
| Median | 38 | 1 |
| 25%-Percentile | 16 | 1 |
| Lower whisker | 0 | 1 |
| Minimum | 0 | 1 |

| Deceleration in m/s² | Feasibility controlled | Feasibility Notbremsung |
|---|---|---|
| <=-9,81 | 0 | 0 |
| <=-9,81 | 0 | 0 |
| -5,98 | 1 | 1 |
| -4,04 | 1 | 1 |
| -3 | 1 | 1 |
| -0,54 | 1 | 1 |
| -0,54 | 1 | 1 |

Only cases where at least a -0.5 m/s² deceleration occurred were analyzed (57.4%)

| Longitudinal acceleration in m/s² | Feasibility Datasheet | Feasibility Maximum |
|---|---|---|
| 2,64 | 0 | 0 |
| 2,42 | 0 | 0 |
| 1,84 | 0 | 1 |
| 1,51 | 0 | 1 |
| 1,31 | 1 | 1 |
| 0,57 | 1 | 1 |
| 0,57 | 1 | 1 |

Only cases were analyzed in which at least a longitudinal acceleration of 0.5 m/s² occurred (3.6%)

| Lateral acceleration in m/s² | Feasibility |
|---|---|
| 6,54 | 0 |
| 4,55 | 0 |
| 2,35 | 1 |
| 1,44 | 1 |
| 0,88 | 1 |
| 0,5 | 1 |
| 0,5 | 1 |

Only cases were analyzed in which at least a lateral acceleration of 0.5 m/s² occurred (32.6%)

***Figure 11:*** **Overview about the dynamic feasibility of the target**

## DISCUSSION

The results show that not all possible dynamics quantities can be mapped with the target carrier, but a large portion of the data can.

It was shown that a broad data basis could be used to derive test scenarios for several applications, e.g. test and validation of ADAS and AD functions but also for scenario testing within future PTI. The various data sources partly address overlapping focal points of the test, so that it is not possible to derive the required scenarios unambiguously.

In the field of accident analysis, it was shown that the methodology used is suitable for developing scenarios for testing critical driving conditions. These can be used, for example, for testing ADAS systems such as Autonomous Emergency Braking (AEB) systems.

## LIMITATIONS

It became apparent that a fully automated transfer of logic or concrete scenarios is not possible yet. This is due to the large complexity and the large number of implementation options. This means that some manual effort in combination with expertise is necessary for a meaningful application and further processing of the parameter sets with regard to the transfer into simulation formats (CarMaker, OpenDRIVE, OpenSCENARIO).

Currently, VUFO is further working on a method to transfer accident scenarios automatically from GIDAS-PCM into OpenDRIVE and OpenSCENARIO. Some hundred (less complex) cases (accidents from GIDAS, based on in-depth investigation and accident reconstruction) could be already transferred.

## REFERENCES

[1] **The Research Association of Automotive Technology (FAT), Federal Highway Research Institute (BASt).** German In-Depth Accident Study (GIDAS). Retrieved from www.gidas.org. 2022

[2] **Schubert, A., Liers, H., Petzold, M.** The GIDAS Pre-Crash-Matrix 2016 - Innovations for standardized pre-crash-scenarios on the basis of the VUFO simulation model VAST. 7th International Conference on ESAR "Expert Symposium on Accident Research", Hannover, June 09/10, 2016.