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.

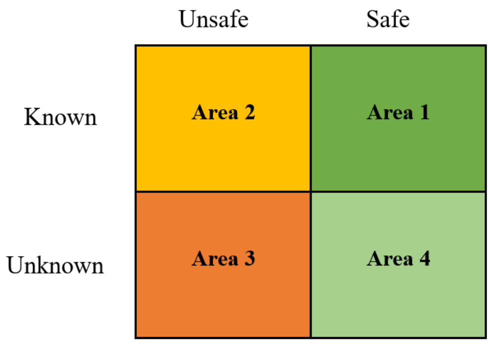
INTRODUCTION

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.



	Unsafe	Safe
Known	**Area 2**	**Area 1**
Unknown	**Area 3**	**Area 4**

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.

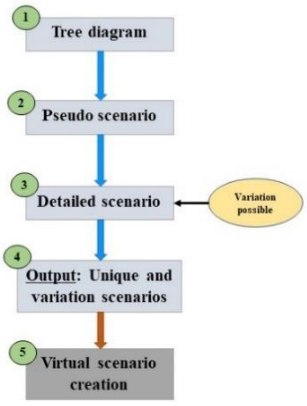


Figure 2. Steps for scenario creation.

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).

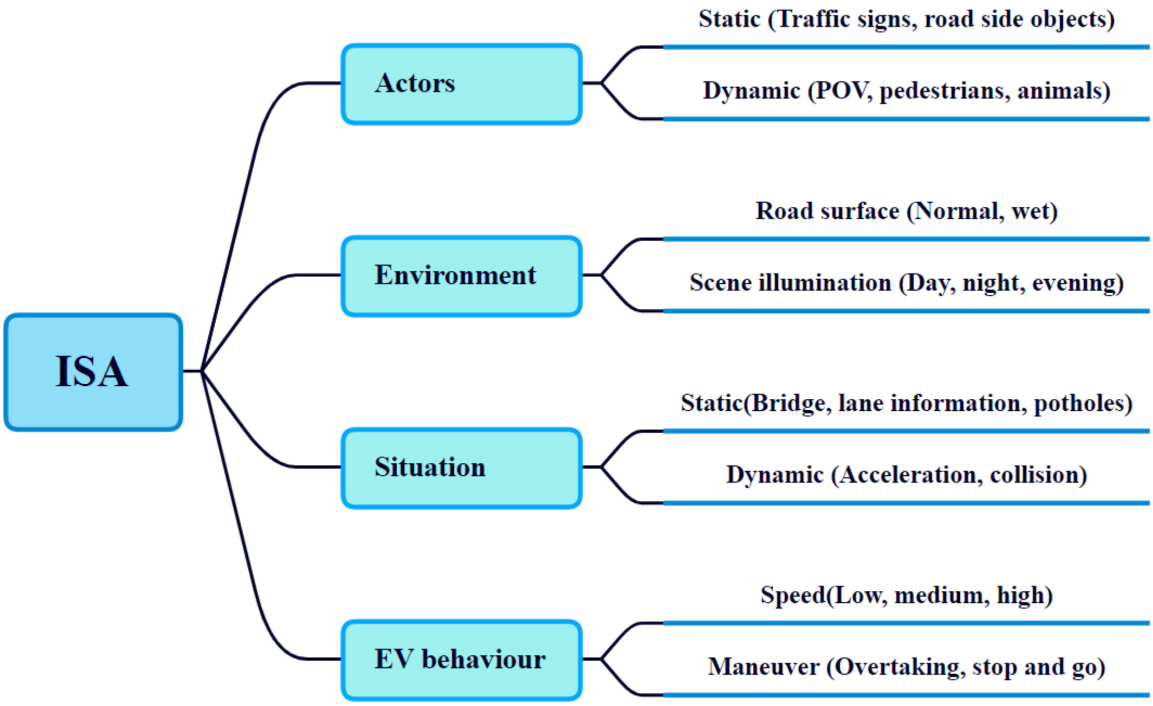


Figure 3. Tree diagram for scenario generation.

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. 2. Traffic sign board present at 200m from origin indicating the speed limit of 40km/h. 3. Length of straight road is 1km.	1. EV travelling at 60km/h. 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.

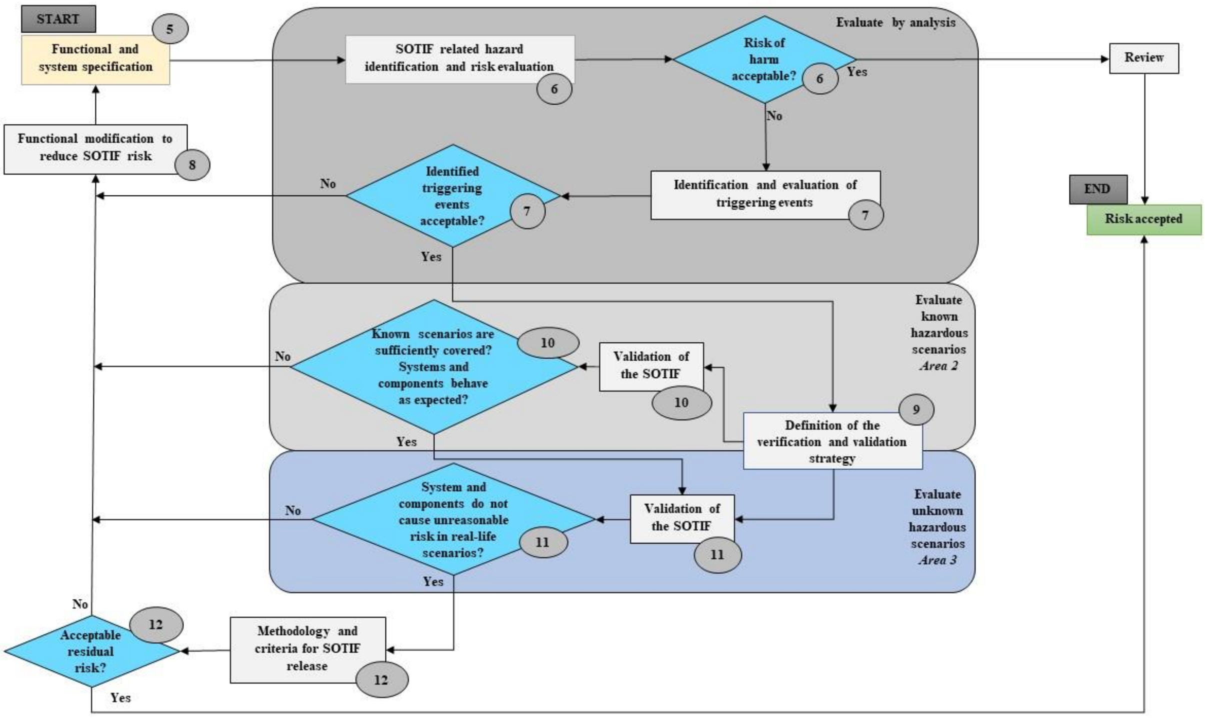


Figure 5. ISO SOTIF flow chart.

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.

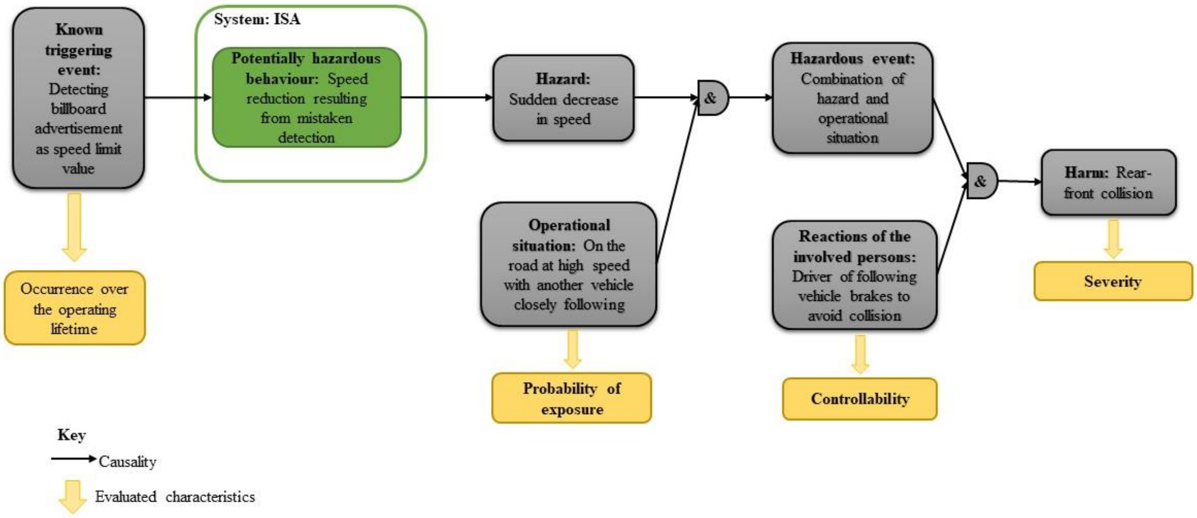


Figure 6. Hazard analysis of ISA according to ISO 26262.

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.

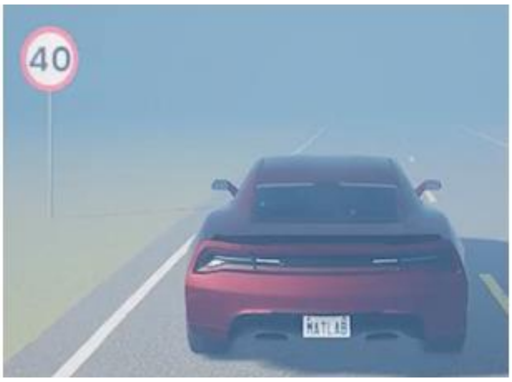


Figure 8. Detection of speed sign by ego vehicle on a foggy road.

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.

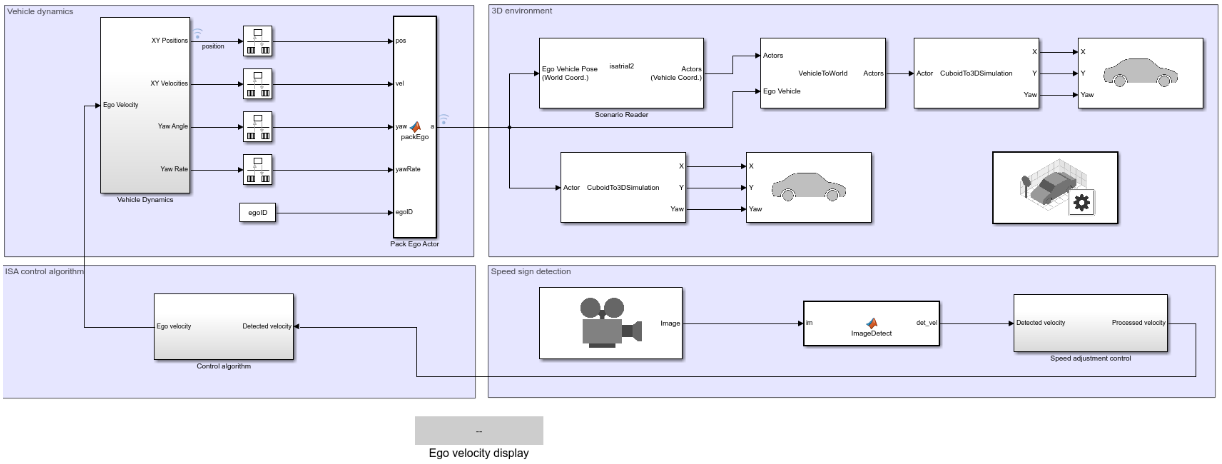
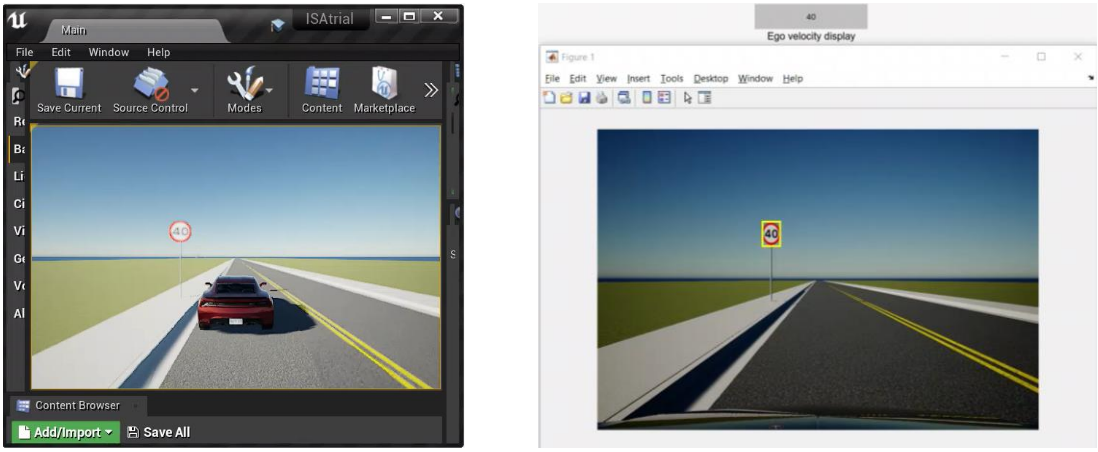


Figure 10. Simulink model of ISA.

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/