A.2.5.2 ISO 26262-3 Hazard analysis and risk assessment (HARA)

The HARA identifies the malfunctioning behaviours of the item and assesses the resulting risk.

EXAMPLE 1 Malfunctioning behaviour of the AEB item:

— UNDESIRED autonomous braking:

  — within specified speed reduction limits: ASIL *X* as a result of the E, C and S evaluation of the hazardous events;

  — outside specified speed reduction limits: ASIL *Y* as a result of the E, C and S evaluation of the hazardous events (with $Y \geq X$);

— TOO LATE or MISSED autonomous braking:

  — due to the high controllability (braking is a regular task of the driver) and the low exposure (emergency braking is a rare event), the hazardous events can be rated as QM.

NOTE (In relation to EXAMPLE 1 above) in other systems with higher levels of driving automation levels, the system can take over the responsibility for the driving task of braking in general, not only for emergency operations. In this case, the above statement might not be valid anymore.

The parameters of the HARA can be impacted by functional modifications motivated by SOTIF.

EXAMPLE 2 AEB function limits the maximum speed reduction while braking autonomously, this increases the controllability of the following vehicles to avoid a rear collision and reduces the severity of a collision.

A.2.5.3 Identification and evaluation of hazards caused by the intended functionality

This activity evaluates the vehicle function according to the following aspects:

— is the specified behaviour of the vehicle function safe?

— what are the undesired behaviours of the vehicle function and are they a source of credible harm?

— what are the risks due to reasonably foreseeable misuse?

EXAMPLE Risk identification and evaluation for AEB:

— Is the specified behaviour at the vehicle level safe in the specified use cases?

  If the specified behaviour can be the cause of an accident, evaluate if there is a more appropriate behaviour in the given context.

  According to the specification of the AEB system, it only intervenes when the collision is unavoidable. In such a scenario, the driver can brake with maximum force. If the driver does not do this, the AEB system takes over this task. This is the best possible behaviour, unless the driver wants to prevent the accident by lateral evasion. In the latter case, braking might even be counter productive, reducing the available lateral acceleration force. Due to this the specified behaviour at the vehicle level is modified: the AEB intervention is suppressed or aborted in case of y Nm steering torque. With this modification the specified behaviour at the vehicle level is considered safe.

  For the sake of simplicity further evaluation of this new add on is omitted in this example.

© ISO 2022 – All rig
This is a preview. Click here to purchase the full publication.

— What are the undesired behaviours of the vehicle function? Are they a source of credible harm?

  — False positive: undesired braking within specified speed reduction limits.

    — The following traffic could not react in time, leading to a rear collision. Here the system introduces a new risk. This undesired behaviour is a source of credible harm and with that, is SOTIF-related.

  — False negative: not braking in case of an imminent collision.

    — The system behaves as a pure assistant, i.e. it does not relieve the driver from the braking task nor will it give the impression of releasing the driver from this task since the driver will never experience the system to brake unless an accident is already unavoidable. From a SOTIF point of view, no new risks are introduced by the system by this undesired behaviour and it is not considered as a source of credible harm. Therefore, this undesired behaviour is not SOTIF-related.

      In other systems it could be possible that the system takes over the responsibility for the driving task of braking. In this case the above statement is no longer valid and this undesired behaviour becomes SOTIF-related.

  — Braking outside specified speed reduction limits

    — The capability to brake within the specified speed reduction limits depends on the accuracy of the vehicle speed measurement and the execution of the actuators.

    — Environmental potential triggering conditions which could lead to a braking outside of the speed reduction limits are conceivable (e.g. wind gust from front, quick increase in upward gradient) but it is assumed that the item's control loop would adapt to them quickly keeping over-braking within irrelevant limits

    — The performance insufficiencies of vehicle speed measurements, the braking control loop and braking actuation are well addressed by established systems. They do not require the SOTIF procedure described in this document. This undesired behaviour is not relevant for this document.

— What are the risks due to reasonably foreseeable misuse?

  — Misuse scenario: driver will transfer “braking on object” task to the AEB system.

    — In the user manual, it is clearly mentioned that the system is only assisting the driver and does not prevent the collision, it just reduces the effect.

    — The system brakes in a very uncomfortable manner.

    Therefore, the risk that the driver will transfer the driving task of braking completely to the system is not unreasonable.

    In general, the driver is informed about the limitations of the system (e.g. via the user manual), in order to reduce the likelihood of misuse.

    Care is taken that sales material including advertising and product naming does not lead to incorrect expectations of the user.

A.2.5.4 Conclusion

Care is taken so that the results of the identification and evaluation of hazards caused by the intended functionality and the HARA are consistent. In the example used in A.2.5, this is the case for the malfunctioning behaviour / undesired behaviour “undesired braking” and “Not braking in case of an imminent collision”. Undesired behaviour identified within the identification and evaluation of hazards caused by the intended functionality and malfunctioning behaviour identified within the HARA can lead to the same hazards.

This is a preview. Click here to purchase the full publication.
- All rights reserved

Identification and evaluation of hazards caused by the intended functionality and the HARA do not necessarily always cover the same topics. Evaluating the specified behaviour concerning its safety is a typically SOTIF topic.

Only reasonably foreseeable indirect misuse is considered in ISO 26262 HARA as possible causes of reduced controllability or increased severity when evaluating a hazardous event caused by a malfunctioning behaviour of the item.

Reasonably foreseeable indirect misuse is similarly considered in this document when evaluating a hazardous event caused by a hazardous behaviour of the system. However, this document also considers reasonably foreseeable direct misuse, that is considered as a possible triggering condition.

Some aspects of these activities, for example, the controllability evaluation, can be viewed both as a SOTIF as well as a functional safety topic.

A.2.6 Functional safety concept and SOTIF functional specification

The functional safety concept specifies the fault reaction (e.g. emergency operation, transition into the safe state, etc.). For ADAS and automated driving systems, this fault reaction can also be a SOTIF issue. For these systems, SOTIF determines the necessary functionality in order to execute the specified fault reaction in a safe manner. The task of functional safety is to ensure the availability of the defined necessary functionality in case of a fault (e.g. via fault tolerance) or to ensure that the probability of the fault occurring is sufficiently small (e.g. via fault prevention).

Defining a safe fault reaction itself can be viewed as a SOTIF task as well as a functional safety task.

EXAMPLE In case of an automated driving function: the fault reaction can be for example:

— safe stop in the current lane,

— drive to the next parking lot.

NOTE The consistency of the functional modifications of Clause 8 with the requirements derived from the ISO 26262 series in the functional safety concept can be achieved by proper information exchange and/or reviews.

A.2.7 Technical safety concept and SOTIF

As a result of SOTIF activities the system design might change (e.g. by introducing new sensors), which can have an impact on the technical safety concept.

Also, as a result of functional safety activities, the system design might change (e.g. by introducing new sensors) which can have an impact on the SOTIF.

A.2.8 Safety analysis

The analysis activities to ensure the functional safety and the SOTIF focus on the functional chain and use the same design as a starting point, but have different viewpoints. The analysis for functional safety addresses systematic issues with the implementation of the specified behaviour and random hardware faults of the E/E elements.

The analysis for SOTIF (Clause 7) focuses on functional insufficiencies, their potential triggering conditions and their impact on the vehicle behaviour. In addition, reasonably foreseeable indirect misuse is also considered in this context (Clause 6, Clause 7).

The safety analysis for the ISO 26262 series can be used as an input for the SOTIF analysis and vice versa.

The aspects of the safety of the specified behaviour at the vehicle level and the risk resulting from reasonably foreseeable misuse are unique for the analysis for SOTIF.

© ISO 2022 – All rig
This is a preview. Click here to purchase the full publication.

A.2.9 Supporting processes

This document does not explicitly formulate requirements concerning the development process itself. The suitability of the development process is important to achieve safety and is addressed by existing standards such as IATF 16949 and the ISO 26262 series. For instance, the supporting processes of ISO 26262-8 are assumed to be adapted, if necessary, and applied to support the achievement of the SOTIF, for example:

— the Development Interface Agreement (DIA) according to ISO 26262-8:2018, Clause 5 is elaborated to also address the SOTIF aspects (see 4.4.2);

— confidence in the use of software tools according to ISO 26262-8:2018, Clause 11 can be applied to the tools relevant to achieve the SOTIF with a few adaptations.

NOTE 1 In addition to explicit tool errors, the capability of a simulation tool to represent the real world within certain tolerances can be of particular relevance in the SOTIF context.

NOTE 2 The accuracy of the real-world data measurement itself can be of particular relevance in the SOTIF context.

A.2.10 Verification and validation

Verification and validation strategy (see Clause 9) as well as the specified test cases (see Clauses 10 and 11) addressing SOTIF-related requirements can also take functional safety requirements into consideration.

As some test cases can address SOTIF as well as functional safety issues, some test cases address aspects of functional safety (e.g. the capability of a safety mechanism to detect and signal a random hardware fault) or SOTIF (e.g. tests to evaluate the sufficiency of the specified behaviour at the vehicle level) alone.

A.3 Simplified SOTIF application examples

Table A.15 provides a comparison of simplified examples of domain relevant SOTIF hazards and mitigations as a function of increasing vehicle autonomy for the reason of comparison of different kinds of functionalities.

This is a preview. Click here to purchase the full publication.
- All rights reserved

Table A.15 — Simplified examples of domain relevant SOTIF hazards and mitigations

	Driver assistance (L1- per Clause 3 Table 2)	Partial driving automation (L2- per Clause 3 Table 2)	Conditional driving automation (L3- per Clause 3 Table 2)	Conditional driving automation (L3- per Clause 3 Table 2)	High driving automation (L4 per Clause 3 Table 2)
System example	**Adaptive cruise control**	**Adaptive cruise control combined with lane keeping**	**Automation for traffic jam convenience**	**Highway co-pilot**	**Robo-taxi**
System description	This function enhances standard automotive cruise control using a sensor to detect a lead vehicle. If the lead vehicle is getting too close the feature will take action by slowing the vehicle to match the speed of the lead vehicle.	This function uses sensors to maintain vehicle position in the centre of the lane and detect a lead vehicle to adjust vehicle speed to maintain a pre-set headway.	This function uses sensors to maintain a safe longitudinal distance from the lead vehicle when in a traffic jam on the highway. It includes steering so as to stay in the lane of travel.	This function uses multiple and diverse sensors to autonomously navigate in traffic, executing all necessary manoeuvres for highway driving.	This function uses multiple and diverse sensors to autonomously navigate in traffic from point A to point B within a defined geofenced area.
DDT- lateral and longitudinal vehicle motion control	Driver and system	System	System	System	System
DDT- OEDR	Driver	Driver	System	System	System
DDT- fallback	Driver	Driver	Fallback-ready user [a]	Fallback-ready user [a]	System
Operational use case(s)	1) Maintain headway to lead vehicle up to set speed 2) When there is no lead vehicle in front of the ego vehicle, maintaining desired speed	1) Following a lead vehicle in lane up to set speed and headway 2) When there is no lead vehicle in front of the ego vehicle, maintaining desired speed and following lane	1) Following a lead vehicle that is operating at or below x km/h at a distance no greater than y m 2) If lead vehicle changes lanes, maintain following the next immediate lead vehicle, or if no lead vehicle present then driver is requested to take back control of the vehicle	All highway related use cases (following, lane keeping, merging, passing, etc.)	All urban and highway related use cases (following, passing, merging, stopping for traffic controls, etc.)

[a] The distinction between the driver and fallback-ready user is that the driver is required to be continuously supervising. While the fallback-ready user might not be supervising the OEDR but is required to take control on request within an appropriate time frame.

© ISO 2022 – All rig
This is a preview. Click here to purchase the full publication.

Table A.15 *(continued)*

	Driver assistance (L1- per Clause 3 Table 2)	**Partial driving automation (L2- per Clause 3 Table 2)**	**Conditional driving automation (L3- per Clause 3 Table 2)**	**Conditional driving automation (L3- per Clause 3 Table 2)**	**High driving automation (L4 per Clause 3 Table 2)**
Operational design domain	The system is operational when vehicle is operating at or above x km/h.	The system is operational when vehicle is in a detected lane and is operating at or above x km/h.	The system is operational when the vehicle is within the geo-fence (mapped area), in a valid lane, and operating below x km/h in most environmental conditions (the feature is assumed to disengage in case of adverse environmental conditions such as thick fog, heavy rain, etc.).	The system is operational on mapped highways in most environmental conditions (feature is assumed to disengage in case of adverse environmental conditions such as thick fog, heavy rain, etc.).	The system is operational in a geo-fenced mixed highway and urban area in all environmental conditions except extreme weather (as defined in the specification).
Example of an intended behaviour/functionality	Maintain a safe headway with the lead vehicle. If the lead vehicle is getting too close, the feature will apply an appropriate brake force to maintain a safe headway. If it detects that the lead vehicle is far off, the feature will apply an acceleration until the user's pre-set speed is reached.	Maintain lane boundaries and maintain a safe headway with the lead vehicle. If the lead vehicle is getting too close, the feature will apply an appropriate brake force to maintain a safe headway. If it detects that the lead vehicle is far off, the feature will apply an acceleration until the user's pre-set speed is reached. Lateral control is applied to stay in lane.	The system requests that the user takes control in case of adverse environmental conditions like thick fog (user expected to take control before exiting the ODD).	Execute a zipper merge making lateral manoeuvres while leaving appropriate time and space for others.	Exhibit caution in occluded areas.

[a] The distinction between the driver and fallback-ready user is that the driver is required to be continuously supervising. While the fallback-ready user might not be supervising the OEDR but is required to take control on request within an appropriate time frame.

This is a preview. Click here to purchase the full publication.
- All rights reserved

Table A.15 *(continued)*

	Driver assistance (L1- per Clause 3 Table 2)	**Partial driving automation (L2- per Clause 3 Table 2)**	**Conditional driving automation (L3- per Clause 3 Table 2)**	**Conditional driving automation (L3- per Clause 3 Table 2)**	**High driving automation (L4 per Clause 3 Table 2)**
An example of SOTIF hazard requiring mitigation	System brakes when approaching a bridge perceiving it incorrectly as a static metal object in the roadway.	Ego vehicle and lead vehicle are operating in a merge lane. The lead vehicle merges into the intended lane and the ego vehicle now no longer detects a lead vehicle so it begins to accelerate to the previously pre-set cruise control speed. The ego vehicle driver is unable to merge into the intended lane before the merge lane ends and goes off the road.	The fallback-ready user does not take control when requested because the user did not observe the visual alert and the system enters a heavy fog area where it cannot perceive objects with acceptable precision.	Vehicle failed to merge successfully due to the inability to detect a vehicle with lighting and colouring that spoofed the automated system into misclassifying the vehicle as nominal skyline.	A large vehicle in the adjacent lane occludes a traffic light, the robo-taxi does not perceive the traffic light and proceeds into the intersection when the light is red.
An example of SOTIF mitigation	Software algorithm is enhanced to differentiate between vehicles and road infrastructure (i.e. steel bridge, steel covering).	The feature has limited acceleration authority.	The vehicle is designed to be able to detect the impeding heavy fog condition and provide a visual alert to the fallback-ready user. If the fallback-ready user does not take control, the system uses other methods to notify the driver by stimulating other driver senses such as audio, touch, kinematic (such as short brake pulses).	An orthogonal and independent collision mitigation algorithm that is separately evaluating the raw sensor data verifies that the generated path is collision free before it is accepted by the lower level controllers.	The vehicle rationalizes map data with perception data to look for a traffic light state before proceeding into an intersection and understands that the presence of the large vehicle is creating an occlusion of the traffic light. An appropriate behaviour is chosen.

[a] The distinction between the driver and fallback-ready user is that the driver is required to be continuously supervising. While the fallback-ready user might not be supervising the OEDR but is required to take control on request within an appropriate time frame.

© ISO 2022 – All rig
This is a preview. Click here to purchase the full publication.

With respect to verification and validation there are many commonalities regardless of level of driving automation.

Evaluation of the SOTIF mitigation measure regarding the known potentially hazardous scenarios:

1) analytical efforts to expose new potential triggering conditions;

2) exercising the feature in the context of the known scenario where the mitigation is demonstrated.

This can be achieved using a combination of sub-system and system level testing on a closed course, simulation, or open road.

Evaluation of the SOTIF mitigation measure regarding the unknown potentially hazardous scenarios:

a) analytical efforts to influence the V&V strategy to expose undiscovered potential triggering conditions;

b.) exposure across the ODD in closed course, simulation, and open road continues to achieve the validation target in order to show that the residual risk of unknown potentially hazardous scenarios is acceptable.

When expanding an ODD (such as exporting feature to other cities or countries) the changes within the ODD and OEDR are identified and evaluated. This can lead to the necessity to repeat test and simulation activities.

This is a preview. Click here to purchase the full publication.
- All rights reserved

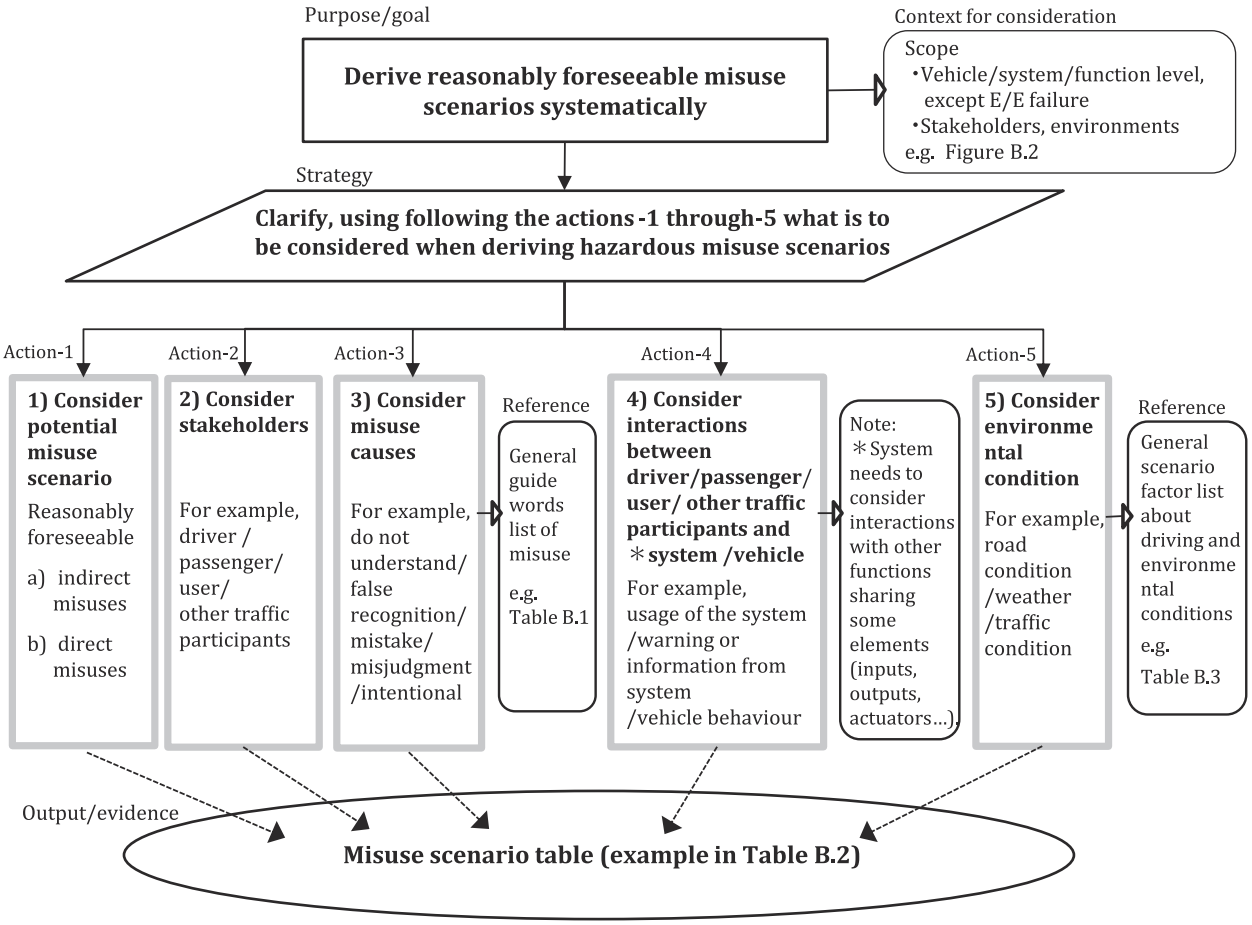
Annex B
(informative)

Guidance on scenario and system analyses

B.1 Method for deriving SOTIF misuse scenarios

B.1.1 Overview

For systems that are SOTIF-related, it is important to consider potential reasonably foreseeable misuse when performing the safety analysis. Scenarios containing SOTIF-related misuse can be derived from various sources, such as: lessons learnt, expert knowledge, brainstorming by designers, etc. B.1 gives an example methodology for systematically deriving SOTIF-related misuse to support the SOTIF safety analysis. The concept overview of this example methodology is given in Figure B.1 and an example of a SOTIF-related misuse is outlined. The approach to the human factors analysis is described in Reference [16].



NOTE For the meaning of the symbol shape of each element in Figure B.1 refer to Table A.1.

Figure B.1 — Systematic derivation of SOTIF-related misuse scenarios (example)

Points to consider and an example scenario factor table for scenarios containing SOTIF-related misuses are described in B.1.2.

© ISO 2022 – All rig
This is a preview. Click here to purchase the full publication.

B.1.2 Flow of safety analysis method for misuse

The points that can be considered when deriving the SOTIF-related misuses are described below.

1) Potential misuse scenario

   Consider the two types of misuse cases:

   — "reasonably foreseeable indirect misuses", are considered in combination with potentially hazardous system behaviour when identifying hazardous events; and

   — "reasonably foreseeable direct misuses", which could directly initiate a hazardous behaviour, as a potential triggering condition.

2) Stakeholders

   Consider who initiates the SOTIF-related misuse that leads to the hazard (e.g. driver, passenger, user, other traffic participants).

3) Misuse causes

   When considering the SOTIF-related misuse causes, general guide words derived from the typical human misuse process (recognition, judgment and action) can be useful.

   Examples of possible guide words are described in Table B.1.

Table B.1 — Guide words for human error

Process	Guide word	Example
Recognition	1. Does not understand	Cannot operate correctly due to complicated usage or insufficient information.
	2. False recognition	Cannot recognise correctly due to being overloaded with information.
Judgment	3. Judgment error/misjudgement	Misjudgement due to wrong impression or misunderstanding (e.g. changing the environment of a GNSS antenna by mounting a bike rack).
Action	4. Slip/mistake	Mistake due to loss of concentration (distraction, drowsiness, automation complacency, etc.).
	5. Intentional	Violation of social rules, commonly accepted human behaviour, correct operation (according to user manual).
	6. Unable	Difficult to operate

4) Interactions between the driver/user, system and vehicle

   A possible cause of misuse might be miscommunication or a time constraint on the interaction between the driver/user and the system/vehicle interfaces (see Figure B.2).

   For example, the following interface subjects can be derived:

   — system operation by the driver (usage): interface from driver to system/vehicle;

     EXAMPLE 1 The system, which is expected to be activated by the voice instruction of the driver, might also be activated unexpectedly due to the key words being spoken in the conversation between occupants.

   — warning notification from the system: interface from system/vehicle to driver; and

   — system/vehicle behaviour: interface from system/vehicle to driver.

This is a preview. Click here to purchase the full publication.
- All rights reserved