PUBLICLY AVAILABLE SPECIFICATION

# ISO/PAS 21448

First edition
2019-01

# Road vehicles — Safety of the intended functionality

*Véhicules routiers - Sécurité de la fonction attendue*

Reference number
ISO/PAS 21448:2019(E)

© ISO 2019

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27

## COPYRIGHT PROTECTED DOCUMENT

© ISO 2019

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

# Contents

Page



© ISO 2019 – All rights reserved



Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27


© ISO 2019 – All rights reserved

# Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee SC 32, *Electrical and electronic components and general system aspects*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT8IF3EW.2-2022-01-12 18:46:27

© ISO 2019 – All rights reserved

# Introduction

The safety of road vehicles during their operation phase is of paramount concern for the road vehicles industry. Recent years have seen a large increase in the number of advanced functionalities included in vehicles. These rely on sensing, processing of complex algorithms and actuation implemented by electrical and/or electronic (E/E) systems.

An acceptable level of safety for road vehicles requires the avoidance of unreasonable risk caused by every hazard associated with the intended functionality and its implementation, especially those not due to failures, e.g. due to performance limitations. ISO 26262-1 defines the vehicle safety as the absence of unreasonable risks that arise from malfunctions of the E/E system. ISO 26262-3 specifies a Hazard Analysis and Risk Assessment to determine vehicle level hazards. This evaluates the potential risks due to malfunctioning behaviour of the item and enables the definition of top-level safety requirements, i.e. the safety goals, necessary to mitigate the risks. The other parts of the ISO 26262 series provide requirements and recommendations to avoid and control random hardware failures and systematic failures that could violate safety goals.

For some systems, which rely on sensing the external or internal environment, there can be potentially hazardous behaviour caused by the intended functionality or performance limitation of a system that is free from the faults addressed in the ISO 26262 series. Examples of such limitations include:

— The inability of the function to correctly comprehend the situation and operate safely; this also includes functions that use machine learning algorithms;

— Insufficient robustness of the function with respect to sensor input variations or diverse environmental conditions.

The absence of unreasonable risk due to these potentially hazardous behaviours related to such limitations is defined as the safety of the intended functionality (SOTIF). Functional safety (addressed by the ISO 26262 series) and SOTIF are distinct and complementary aspects of safety.

To address the SOTIF, activities are implemented during the following phases:

— Measures in the design phase;

EXAMPLE Requirement on sensor performance.

— Measures in the verification phase;

EXAMPLE Technical Reviews, test cases with a high coverage of relevant scenarios, injection of potential triggering events, in the loop testing (e.g. SIL/HIL/MIL) of selected SOTIF are relevant use cases.

— Measures in the Validation phase.

EXAMPLE Long term vehicle test, simulations.

A proper understanding of the function by the user, its behaviour and its limitations (including the human/machine interface) is the key to ensuring safety.

In many instances, a triggering event is necessary to cause a potentially hazardous behaviour; hence the importance of analysing hazards in the context of particular use cases.

In this document the hazards caused by a potentially hazardous system behaviour, due to a triggering event, are considered both for use cases when the vehicle is correctly used and for use cases when it is incorrectly used in a reasonably foreseeable way (this excludes intentional alterations made to the system's operation).

EXAMPLE Lack of driver attention while using a level 2 driving automation.

In addition, reasonably foreseeable misuse, which could lead directly to potentially hazardous system behaviour, is also considered as a possible triggering event.

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT8IF3EW.2-2022-01-12 18:46:27

 © ISO 2019 – All rights reserved

A successful attack exploiting vehicle security vulnerabilities can also have very serious consequences (i.e. data or identity theft, privacy violation, etc.). Although security risks can also lead to potentially hazardous behaviour that needs to be addressed, security is not addressed by this document.

It is assumed that the E/E random hardware faults and systematic faults of the E/E system are addressed using the ISO 26262 series. The activities mentioned in this document are complementary to those given in the ISO 26262 series.

Table 1 illustrates how the possible causes of hazardous event map to existing standards.

**Table 1 — Overview of safety relevant topics addressed by different ISO standards**

| Source | Cause of hazardous event | Within scope of |
|---|---|---|
| System | E/E System failures | ISO 26262 series |
| | Performance limitations or insufficient situational awareness, with or without reasonably foreseeable misuse | ISO/PAS 21448 |
| | Reasonably foreseeable misuse, incorrect HMI (e.g. user confusion, user overload) | ISO/PAS 21448<br>ISO 26262 series<br>European statement of principal on the design of human-machine-interface |
| | Hazards caused by the system technology | Specific standards |
| External factor | successful attack exploiting vehicle security vulnerabilities | ISO 21434[a] or SAE J3061 |
| | Impact from active Infrastructure and/or vehicle to vehicle communication, external devices and cloud services. | ISO 20077 series; ISO 26262 series |
| | Impact from car surroundings (other users, “passive” infrastructure, environmental conditions: weather, Electro-Magnetic Interference…) | ISO/PAS 21448<br>ISO 26262 series |
| [a] Under preparation. Stage at the time of publication: ISO/SAE CD 21434. | | |

NOTE Options for automated driving level definitions (from NHTSA, SAE and OICA, etc.) are discussed in the ITS-Informal Group ECE/TRANS/WP29.

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT8IF3EW.2-2022-01-12 18:46:27

© ISO 2019 – All rights reserved

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.Y0HZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27

# Road vehicles — Safety of the intended functionality

## 1 Scope

The absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or by reasonably foreseeable misuse by persons is referred to as the Safety Of The Intended Functionality (SOTIF). This document provides guidance on the applicable design, verification and validation measures needed to achieve the SOTIF. This document does not apply to faults covered by the ISO 26262 series or to hazards directly caused by the system technology (e.g. eye damage from a laser sensor).

This document is intended to be applied to intended functionality where proper situational awareness is critical to safety, and where that situational awareness is derived from complex sensors and processing algorithms; especially emergency intervention systems (e.g. emergency braking systems) and Advanced Driver Assistance Systems (ADAS) with levels 1 and 2 on the OICA/SAE standard J3016 automation scales. This edition of the document can be considered for higher levels of automation, however additional measures might be necessary. This document is not intended for functions of existing systems for which well-established and well-trusted design, verification and validation (V&V) measures exist at the time of publication (e.g. Dynamic Stability Control (DSC) systems, airbag, etc.). Some measures described in this document are applicable to innovative functions of such systems, if situational awareness derived from complex sensors and processing algorithms is part of the innovation.

Intended use and reasonably foreseeable misuse are considered in combination with potentially hazardous system behaviour when identifying hazardous events.

Reasonably foreseeable misuse, which could lead directly to potentially hazardous system behaviour, is also considered as a possible event that could directly trigger a SOTIF-related hazardous event.

Intentional alteration to the system operation is considered feature abuse. Feature abuse is not in scope of this document.

## 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 26262-1:2018, *Road vehicles — Functional Safety Part 1: Vocabulary*

## 3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 26262-1:2018 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27

© ISO 2019 – All rights reserved

**3.1**
**action**
atomic behaviour that is executed by any actor in a scene

Note 1 to entry: The temporal sequence of actions/events and scenes specify a scenario.

EXAMPLE Ego vehicle activates the hazard warning lights.

**3.2**
**erroneous pattern**
input that can trigger unintended behaviour

**3.3**
**event**
occurrence at a certain place and at a particular point in time

Note 1 to entry: The temporal sequence of actions/events and scenes specify a scenario.

Note 2 to entry: In particular this document addresses *triggering events* (3.15) and hazardous events. A hazardous event is the combination of a hazard (caused by malfunctioning behaviour) and a specific operational situation. Refer to Figure 12 for details.

EXAMPLE 1 Tree falling on a street 50 m ahead of a vehicle XY.

EXAMPLE 2 Traffic light turning green at time XX:XX.

**3.4**
**functional improvement**
modification to a function, system or element specification to reduce risk

**3.5**
**intended behaviour**
specified behaviour of the intended functionality including interaction with items

Note 1 to entry: See Clause 5 for additional information about the specification of intended behaviour.

Note 2 to entry: The specified behaviour is the behaviour that the developer of the item considers to be the nominal (i.e. fault-free) functionality, with its capability limitations due to inherent characteristics of the components and technology used.

**3.6**
**intended functionality**
behaviour specified for a system

**3.7**
**misuse**
usage of the system by a human in a way not intended by the manufacturer of the system

Note 1 to entry: Misuse can result from overconfidence in the performance of the system.

Note 2 to entry: Misuse includes human behaviour that is not specified but does not include deliberate system alterations.

**3.8**
**misuse scenario**
scenario in which misuse occurs

**3.9**
**performance limitation**
insufficiencies in the implementation of the intended functionality

EXAMPLE Incomplete perception of the scene, insufficiency of the decision algorithm, insufficient performance of actuation.

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27


© ISO 2019 – All rights reserved

**3.10**
**Safety Of The Intended Functionality**
**SOTIF**
absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or from reasonably foreseeable misuse by persons

Note 1 to entry: Nominal performance includes intended functionality and the implementation of intended functionality that can be affected by performance limitations or by foreseeable misuse by persons.

**3.11**
**scenario**
description of the temporal development between several scenes in a sequence of scenes

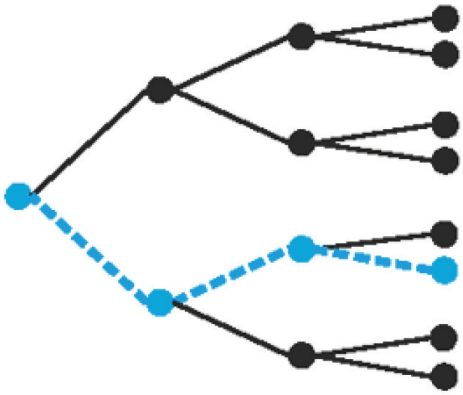


**Figure 1 — Scenario (dashed) as a temporal sequence of actions/events (edges) and scenes (nodes)**

Note 1 to entry: Every scenario starts with an initial scene. Actions and events, as well as goals and values, may be specified to characterise this temporal development within a scenario. In contrast to a scene, a scenario spans a certain amount of time.

Note 2 to entry: See Figures 1, 2 and 3[1].

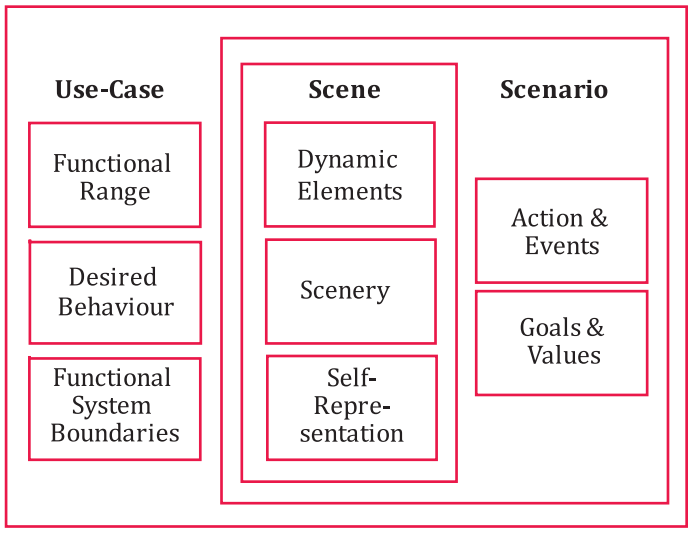



**Figure 2 — Taxonomy of use case, scene and scenario**

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT8IF3EW.2-2022-01-12 18:46:27

© ISO 2019 – All rights reserved

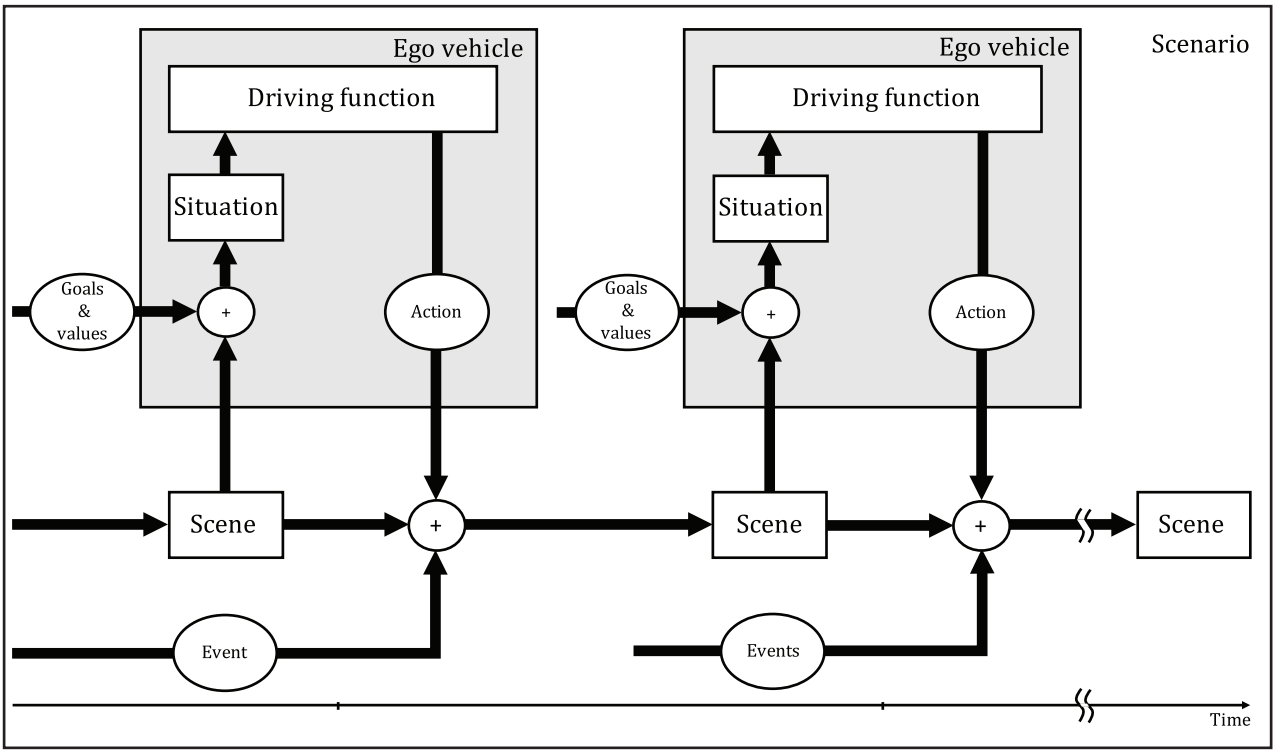



**Figure 3 — Temporal view of scenes, events, actions and situations in a scenario**

**3.12**
**scene**
snapshot of the environment including the scenery, dynamic elements, and all actor and observer self-representations, and the relationships between those entities

Note 1 to entry: See Figure 4.

Note 2 to entry: Only a scene representation in a simulated world can be all-encompassing (i.e. an objective scene, or ground truth). In the real world the scene is incomplete, incorrect, uncertain, and from one or several observers' points of view (i.e. a subjective scene).

Note 3 to entry: Refer to Reference [1].

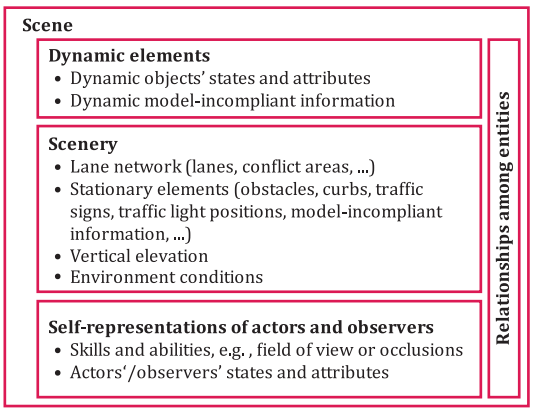



**Figure 4 — Characteristics of a scene**

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27


© ISO 2019 – All rights reserved

**3.13**
**situation**
selection of an appropriate behaviour pattern at a particular point of time

Note 1 to entry: A situation entails all relevant conditions, options and determinants for the behaviour. A situation is derived from the scene, by an information selection and augmentation process that is based on transient (e.g. mission-specific) as well as permanent goals and values. Hence, a situation is always subjective as it represents an element's point of view.

Note 2 to entry: See Figure 5 and Reference [1].

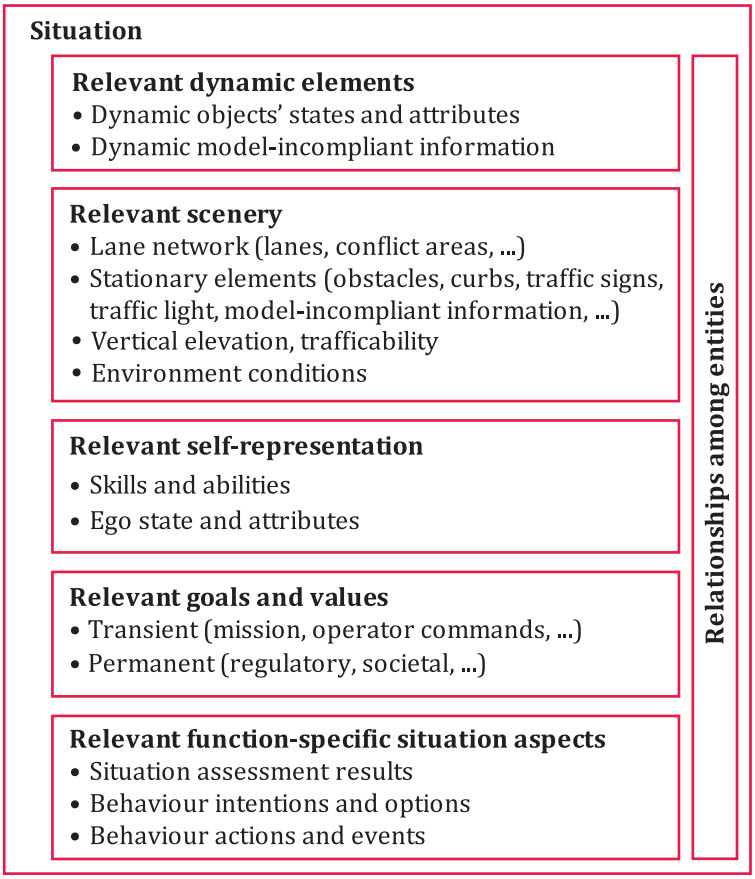



**Figure 5 — Characteristics of a situation**

**3.14**
**test case**
set of conditions to determine if a system is working according to its intended functionality

Note 1 to entry: A test case entails a (logical) scenario with a specific set of parametric values for each aspect of the scenario, together with the pass-fail criteria on which to evaluate it.

Note 2 to entry: Refer to Reference [2].

**3.15**
**triggering event**
specific conditions of a driving scenario that serve as an initiator for a subsequent system reaction possibly leading to a hazardous event

EXAMPLE While operating on a highway, a vehicle's automated emergency braking (AEB) system misidentifies a road sign as a lead vehicle resulting in braking at X g for Y seconds.

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27

© ISO 2019 – All rights reserved

**3.16**
**use case**
specification of a generalized field of application, possibly entailing the following information about the system:

— one or several scenarios;

— the functional range;

— the desired behaviour; and

— the system boundaries

Note 1 to entry: The use case description typically does not include a detailed list of all relevant scenarios for this use case. Instead a more abstract description of these scenarios is used.

**3.17**
**unexpected item behaviour**
unintended behaviour not specified

Note 1 to entry: The unintended behaviour might be discovered during validation.

**3.18**
**validation**
set of activities gaining confidence that an item is able to accomplish its expected functionalities and missions

Note 1 to entry: Verification activities address mainly Area 2 of Figures 7, 8 and 9 including the verification of known use cases, whereas Validation activities address mainly Area 3 of Figures 7, 8 and 9, including the validation of SOTIF in unknown use cases.

## 4 Overview of this document's activities in the development process

The objective sub-clauses of this document (5.1, 6.1, 7.1, 8.1, 9.1, 10.1, 11.1 and 12.1) are normative. All other content is informative. Compliance to this document can be claimed by listing the objectives and providing an argument that the objectives have been achieved.

A development interface agreement can be defined between all development parties when applicable for a distributed product development. The goal of an agreement is to confirm in the early stages of a project all responsibilities of the SOTIF activities.

Achieving SOTIF requires some activities which are complementary to the ISO 26262:2018 series. One of the main objectives of this document is to outline the process and rationale used to ensure that the likelihood of a hazardous event is sufficiently low. Furthermore, this document also seeks to assess that the remaining residual risk from:

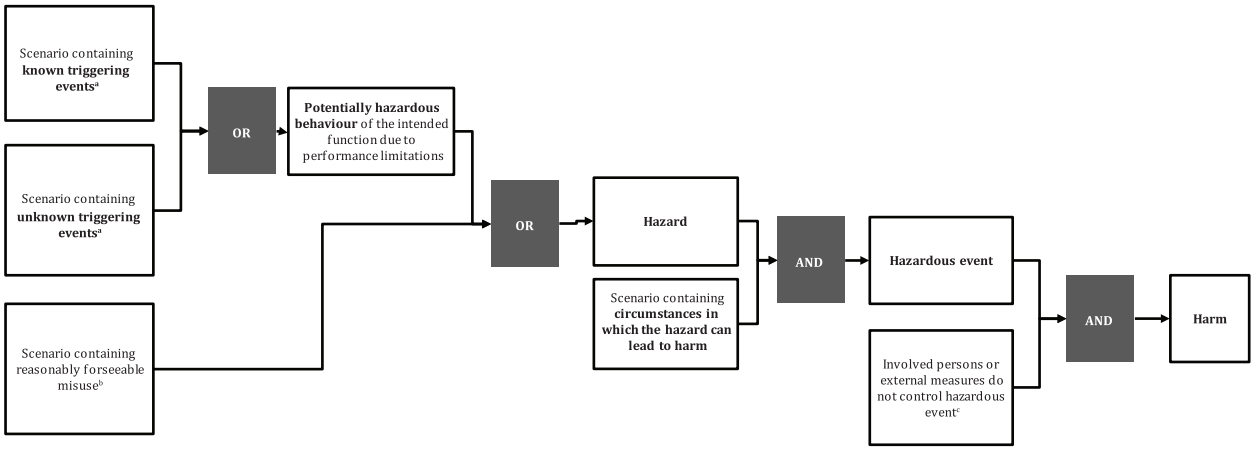
i) a system not able to process a given scenario in a safe manner, and

ii) the involved persons (driver, other vehicle occupants, or bystanders) are not capable of mitigating the hazardous event, is acceptable (see Figure 6).

The functional and system specification includes relevant use cases and those use cases are comprised of several relevant scenarios. These scenarios could contain triggering events (see Clause 3 definitions) that lead to harm (see Figure 6).

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27


© ISO 2019 – All rights reserved



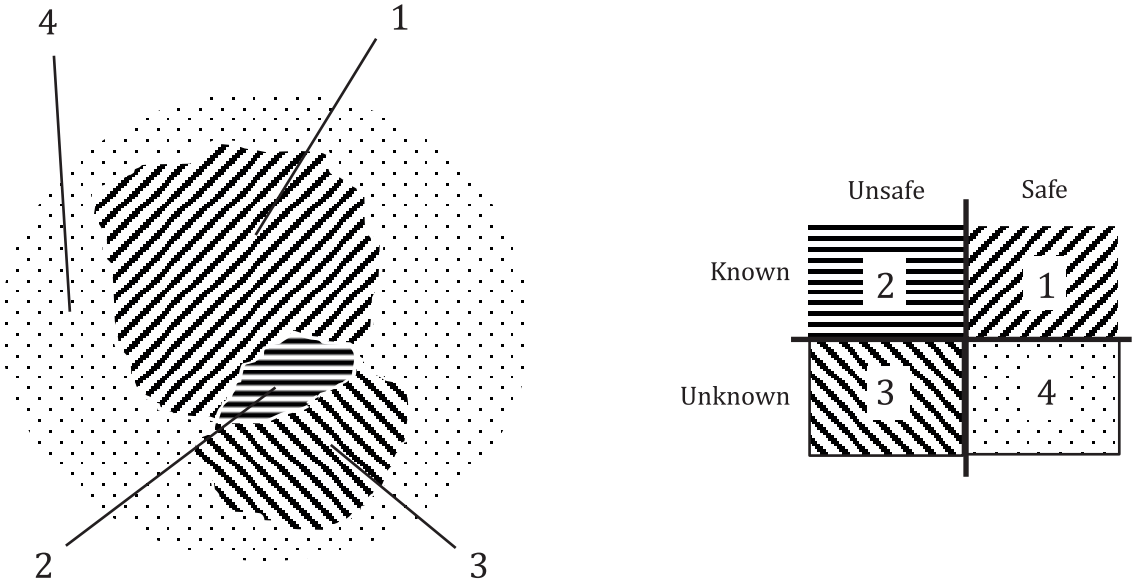

a These scenarios can also be caused by reasonably foreseeable misuse, e.g. activating a functionality intended for the highway in an urban setting causes the vehicle to be in a scenario in which it does not detect a red traffic light.

b Reasonably foreseeable misuse can lead directly to a hazard, e.g. in case of mode confusion where the driver assumes that the system is active even though it is deactivated.

c The inability to control the hazardous event can also be the result of a reasonably foreseeable misuse, e.g. the driver does not supervise the system as he is supposed to do.

**Figure 6 — Visualisation of a Potential SOTIF-related Hazardous Event Model**

Within this document, the scenarios which are part of the relevant use cases are therefore classified into four areas (see Figure 7).




**Key**

1 known safe scenarios (Area 1)

2 known unsafe scenarios (Area 2)

3 unknown unsafe scenarios (Area 3)

4 unknown safe scenarios (Area 4)

**Figure 7 — Visualisation of the Known/Unknown and Safe/Unsafe Scenario categories**

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT8IF3EW.2-2022-01-12 18:46:27

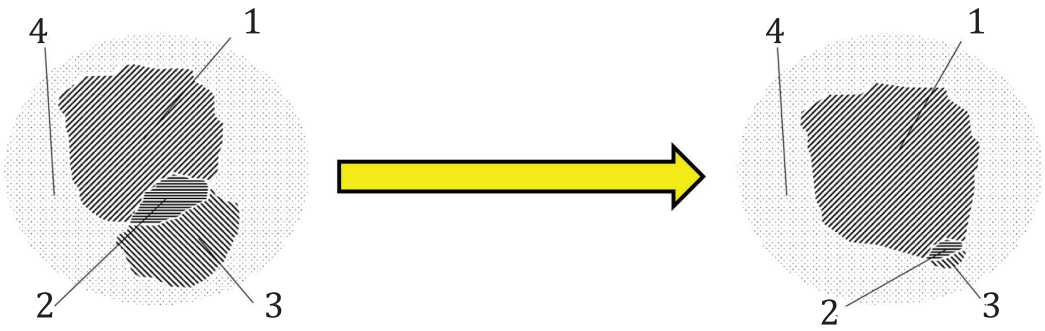
© ISO 2019 – All rights reserved

Areas 1, 2 and 3 are used as a mental model to structure this document. Area 4 is referenced for completeness but is not needed for the purposes of this document and therefore not used further. When considering the areas in the model, it can be useful to imagine their size as representing the proportion of each type of scenario that falls within each respective area.

A given use case can include known as well as unknown scenarios.

At the beginning of the development Areas 2 and Area 3 might be too large, resulting in unacceptable residual risk. The ultimate goal of the SOTIF activities to evaluate the SOTIF in Area 2 and Area 3 and to provide an argument that these areas are sufficiently small and therefore that the resulting residual risk is acceptable. While the known scenarios and the corresponding use cases of Area 2 can be explicitly evaluated, the scenarios and corresponding use cases of Area 3 are evaluated by industry best practice or by other approaches such as design measures, systematic analyses, or dedicated experiments. The results of these evaluations provide an argument that Area 3 is sufficiently small and Area 2 is managed through SOTIF improvements and therefore the probability of encountering these kinds of scenarios is sufficiently low.

It is expected that Areas 2 and Area 3 will be reduced and Area 1 will grow during development (see Figure 8).




**Key**

1 known safe scenarios (Area 1)

2 known unsafe scenarios (Area 2)

3 unknown unsafe scenarios (Area 3)

4 unknown safe scenarios (Area 4)

**Figure 8 — Evolution of the scenario categories resulting from the ISO/PAS 21448 activities**

The goals of the SOTIF process with respect to Area 1, Area 2, and Area 3 and relevant scenarios are:

— Area 1: Maximize or maintain area, while minimizing Areas 2 & 3. This retains or improves safe functionality.

— Area 2: Minimize area with technical measures to an acceptably small level, with statistical significance of that level appropriate to the relative impact of the technical measure; evaluate the potential risk and, if necessary, move hazardous scenarios into Area 1 by improving the function or by restricting the use/performance of the function.

— Area 3: Minimize area (the risk of the unknown) as much as possible with an acceptable level of effort (every detected hazardous scenario is moved into Area 2).


© ISO 2019 – All rights reserved

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27

Figure 9 describes a flowchart for the improvement of the intended functionality to ensure its safety. The circled numbers denote the corresponding clauses within this document.

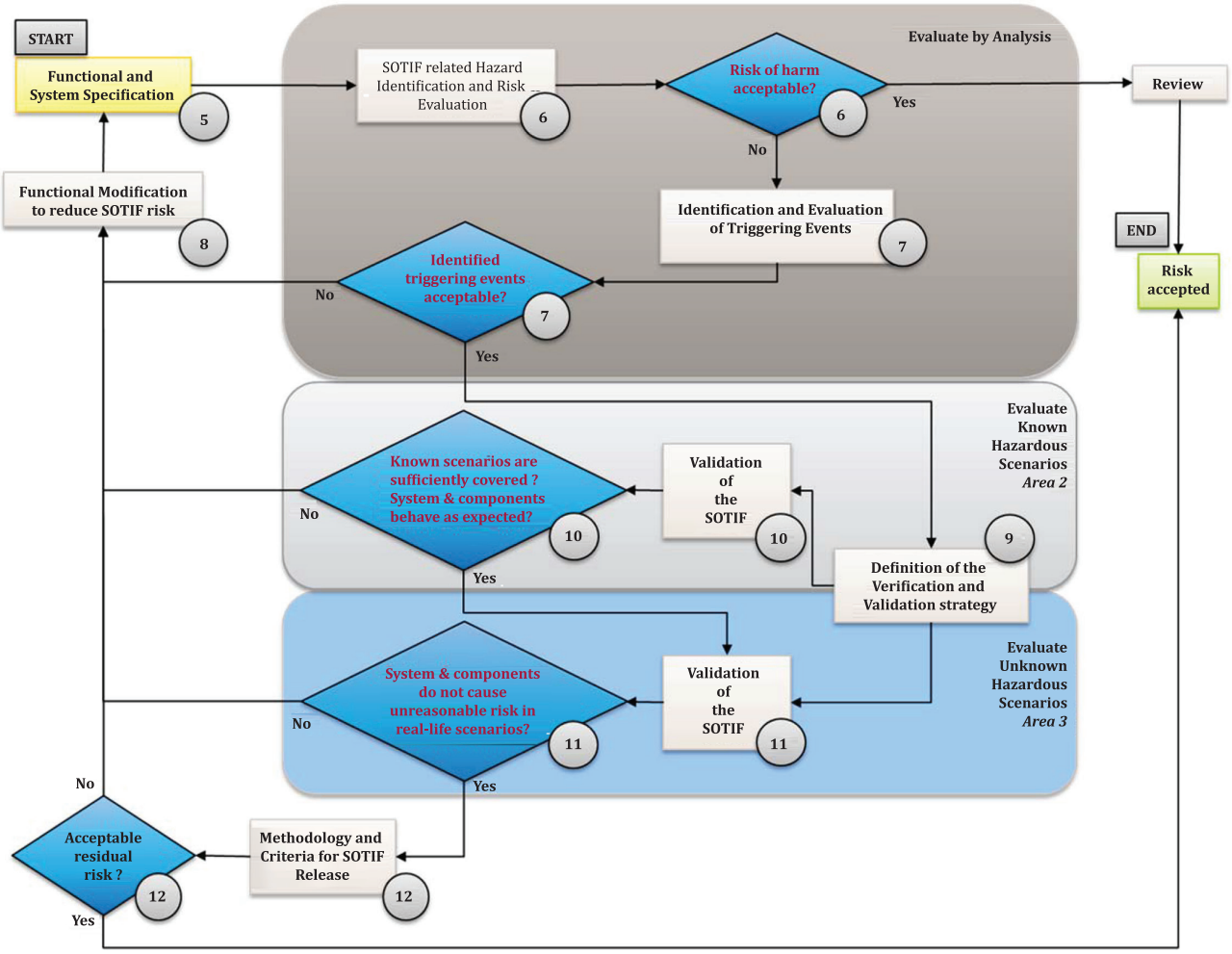



**Figure 9 — Flowchart of this document's activities**

In Figure 9, the process starts with a definition of the functional and system specification (see Clause 5). The possible hazardous behaviours of the intended function are subjected to a Hazard Identification and Risk Evaluation (see Clause 6) that identifies potential hazardous events. If it is shown that these potentially hazardous events do not lead to harm, then no improvement is necessary and the intended functionality can be considered free from unreasonable risk.

If it is shown that harm is possible, then an analysis of the possible hazardous triggering events (e.g. misdetection of certain objects under certain environmental conditions or driver misuse) is conducted (see Clause 7).

Clause 6 and Clause 7 address different aspects of the SOTIF. Clause 6 does not consider the causes of possible hazardous intended behaviour of the function, but only their consequences for safety. Clause 6 is, therefore, focused on evaluating hazardous events that could result from hazardous intended behaviour, and on defining the verification and validation targets to be met. Clause 7 addresses the analysis of the causes of potentially hazardous behaviour. These are mitigated in Clause 8 and verified and validated in Clause 9, Clause 10 and Clause 11.

Functional improvement or restrictions of the use cases are applied to avoid these hazards or to further reduce the resulting risk (see Clause 8).

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT8IF3EW.2-2022-01-12 18:46:27

© ISO 2019 – All rights reserved

A verification and validation strategy is developed to provide an argument that the residual risk is below an acceptable level (see Clause 9). This includes enforcement of the resulting strategy. Corresponding verification and validation test cases can be derived from this analysis (see Clauses 10 & 11).

Finally, the residual risk is evaluated (Clause 12) considering the results from verification and validation. If the risk is determined to be unacceptable, further functional improvement or restrictions of the use cases can be necessary (Clause 8). This verification and validation strategy can include model-in-the-loop (MIL), software-in-the-loop (SIL), hardware-in-the-loop (HIL), test track experiments, dedicated analyses, long-term endurance tests, or other approaches.

Possible causes of unintended behaviour considered in this document are closely related to the performance of sensing, processing of algorithms, actuation, and their implementation for the functionality under development. Therefore, this document's activities are applicable to the vehicle, system, and component levels.

Similarly, the selection of a capable, overall system architecture becomes a primary concern to ensure the SOTIF, and, to ensure that overall capability, corresponding activities take place both at early stages and throughout the overall functional development lifecycle.

It can be necessary to include specific mechanisms to ensure the SOTIF. For instance, a dedicated Human-Machine Interface (HMI) can be defined to prevent/mitigate some reasonably foreseeable misuses by the driver (see Annex E). During the product development, both this document's activities and activities specified in the ISO 26262:2018 series activities are carried out and the measures for SOTIF are evaluated.

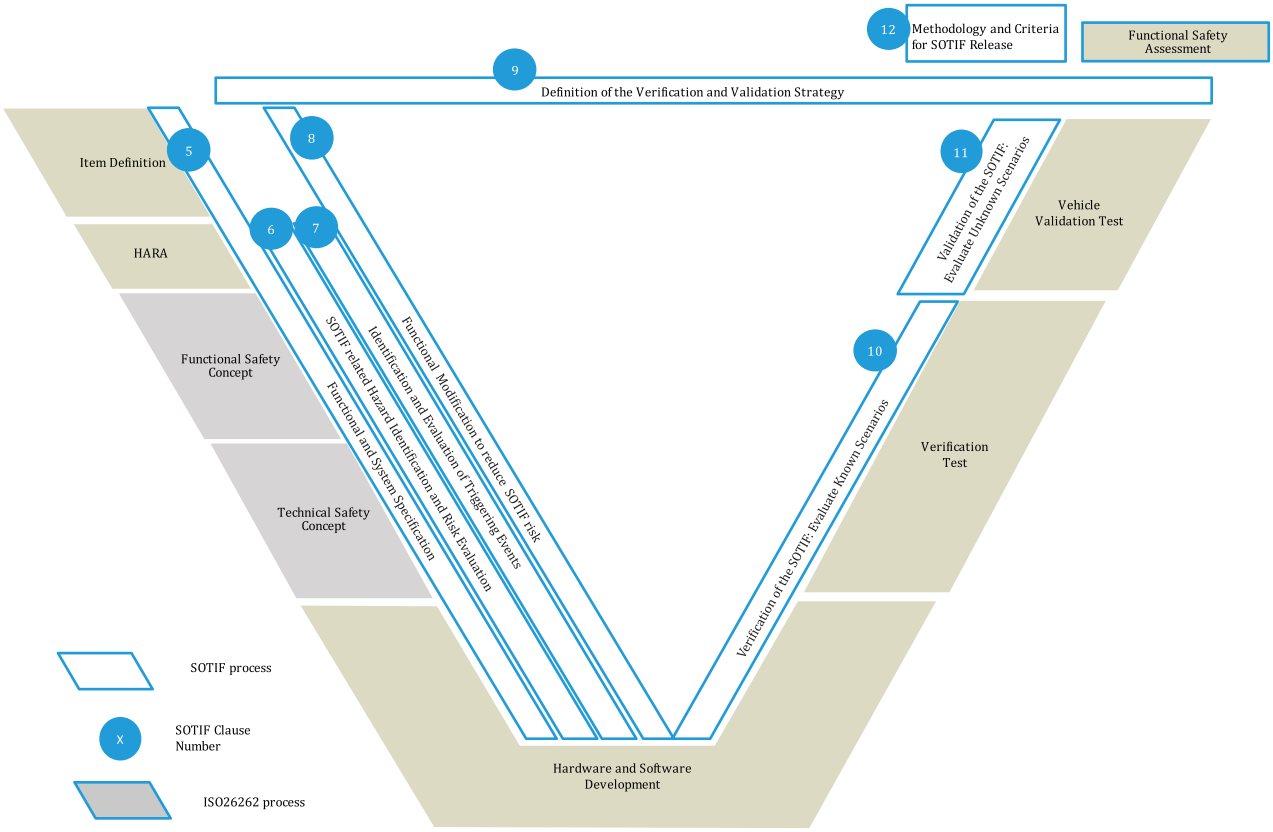



**Figure 10 — Possible interactions of product development activities between this document and the ISO 26262 series processes**

Figure 10 describes possible interactions between this document and the ISO 26262:2018 series activities. The product development phases will typically require several iterations to produce a final functional and system specification. These iterations are not represented in the figure.


© ISO 2019 – All rights reserved

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT8IF3EW.2-2022-01-12 18:46:27

A set of methods and measures are selected in order to:

— Identify and evaluate the SOTIF related hazards associated with the intended functionality (Clause 6);

— Identify and evaluate hazardous triggering events (Clause 7);

— Improve the system design as necessary through functional modifications or use case restriction to reduce SOTIF risk (Clause 8); and

— Verify and validate the appropriateness of the design with respect to the SOTIF (Clause 9–11).

NOTE The hazard identification process is similar to the process described in ISO 26262-3:2018, because the vehicle-level effects of SOTIF related potentially hazardous behaviour and the system failures covered by the ISO 26262 series can be identical.

Annex A presents an example of application of the SOTIF activities.

This document provides a non-exhaustive collection of methods and measures, from which the development team can select the appropriate combination. Other equivalent methods can also be applied.

# 5 Functional and system specification (intended functionality content)

## 5.1 Objectives

The functional and system specification activity shall:

— Compile and create evidence containing the information sufficient to initiate the SOTIF related activities;

— Update the evidence as necessary after each iteration of the SOTIF related activities (see Figure 9).

## 5.2 Functional description

The functional and system specification includes (where applicable):

Function related:

— The goals of the intended functionality;

— The use cases in which the intended functionality is activated, deactivated and active;

— The description of the intended functionality;

— The level of automation/authority over the vehicle dynamics; and

— The dependencies on, and interaction with:

  — the car driver, passengers, pedestrians and other road users;

  — relevant environmental conditions; and

  — the interfaces with the road infrastructure.

System related:

— The description of the system and elements implementing the intended functionality.

— The description and behaviour of the installed sensors, controllers and actuators used by the intended functionality.

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27

© ISO 2019 – All rights reserved

— The assumptions about how the intended functionality makes use of inputs from other elements.

— The assumptions about how other elements make use of outputs from the intended functionality.

— The concepts and technologies for the system and sub systems.

— The limitations and their countermeasures.

— The system architecture supporting the countermeasures.

— The degradation concept.

— The warning strategies.

— The dependencies on, and interaction with other functions and systems of the vehicle.

NOTE This document and the ISO 26262-3:2018 item definition can contain common information.

## 5.3 Consideration on system design and architecture

The functional and system specification provides an adequate understanding of the system and its functionality so that the activities in subsequent phases can be performed. This includes a list of all performance limitations and their countermeasures. Some limitations and countermeasures are known and documented before the SOTIF related process begins while others are revealed as a result of the SOTIF activities.

Each iteration of the SOTIF related activity (Figure 9) can result in engineering activity and an update to this specification. Each iteration relies on this specification being up to date, such that it reflects all information discovered in previous iterations. Cooperation between all development parties (OEM, Tier1, TierN) is used to discover limitations and develop countermeasures during all development phases.

The functional and system specification lists performance limitations of every individual mechanisms, algorithms, or elements related to the safety of the intended functionality. The system is thus designed considering such limitations and ensuring that countermeasures are taken to mitigate their effect on the overall system if needed.

As the SOTIF activities identify new limitations and consequences (Clause 7), and define new mitigation measures (Clause 8), the functional and system specification is updated. This will ensure that all the required work is done both for closure of previous iterations, and at the beginning of the next iteration.

Specifically, the design includes considerations of system limitations that can result in erroneous subsystem output values being reported with high confidence (low confidence values might be ignored by design) and which can lead to potentially hazardous behaviour. Examples of limitations include incorrect classification, incorrect measurements, incorrect tracking, misdetection, ghosts, incorrect target selection, incorrect kinematic estimation, etc.

The final system architecture achieves robustness by considering every component, technology and system limitation. The system development is based on the assumption made about the limitations in design. Implementing measures to ensure SOTIF and integrating them into the functional and system specification, decreases the sizes of Area 2 and Area 3, and increases overall robustness by increasing the size of Area 1. Area 3 testing is used to uncover new issues only when the countermeasures, with respect to the original system design, are incomplete or not applicable to newly introduced use cases.

NOTE 1 Methods such as qualitative fault tree, HAZOP, FMEA, STPA and event tree analysis can be used to increase the confidence for the SOTIF.

NOTE 2 Performance limitations can be addressed by redundancy, diversity, functional restrictions or other measures.

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27


© ISO 2019 – All rights reserved

EXAMPLE 1 A highway lane boundary detection algorithm, for functions such as lane keeping, might incorrectly determine the lane due to debris on the roadway. However, lane excursions that result in a collision can be mitigated by other autonomous driving functionality such as: using a high definition map and localization to confirm the lane, rationalizing the vehicle trajectory with the trajectory of preceding vehicles, collision avoidance algorithms maintaining separation with other vehicles even if this implies leaving the perceived lane, etc.

EXAMPLE 2 An object detection algorithm detects a person on a skateboard as a pedestrian but rejects the object as due to its speed being implausible. A collision with the skateboarder is mitigated by a collision mitigation braking system which uses sensing and processing that is independent from that of the object detection algorithm.

EXAMPLE 3 An optical illusion drawing of a child running into the road is used to alert drivers in some areas. The image is drawn specifically to fool the human perception and can also fool a vision system into detecting a non-existent object. In this case, an optical flow-based analysis mechanism can prevent false braking. Optical flow analyses as well as radar-based environment recognition are alternative countermeasures for such cases, as well as other common detection cases such as ghosts that result from classification errors.

**Figure 11 — Example of optical illusion drawing that could fool a vision system**

EXAMPLE 4 Using an automated parking system with a big item protruding from the open trunk can lead to a hazardous event. A countermeasure in the system design can be to only permit automatic parking when the trunk is closed.

# 6 Identification and Evaluation of hazards caused by the intended functionality

## 6.1 Objectives

The potential hazards related to the SOTIF shall be systematically identified and evaluated such that:

— The possible hazardous events, caused by functionality that results in potentially hazardous behaviour and their potential consequences, are identified and evaluated.

— The acceptance criteria (e.g. a validation target) to evaluate the design in the validation phase are specified.

NOTE Such acceptance criteria could be the minimum length of the required endurance run combined with a maximum number of observed failures for each type (e.g. false positives, false negatives).

— The possible hazardous events caused by reasonably foreseeable misuse of the function, by the user, are identified and evaluated.

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27

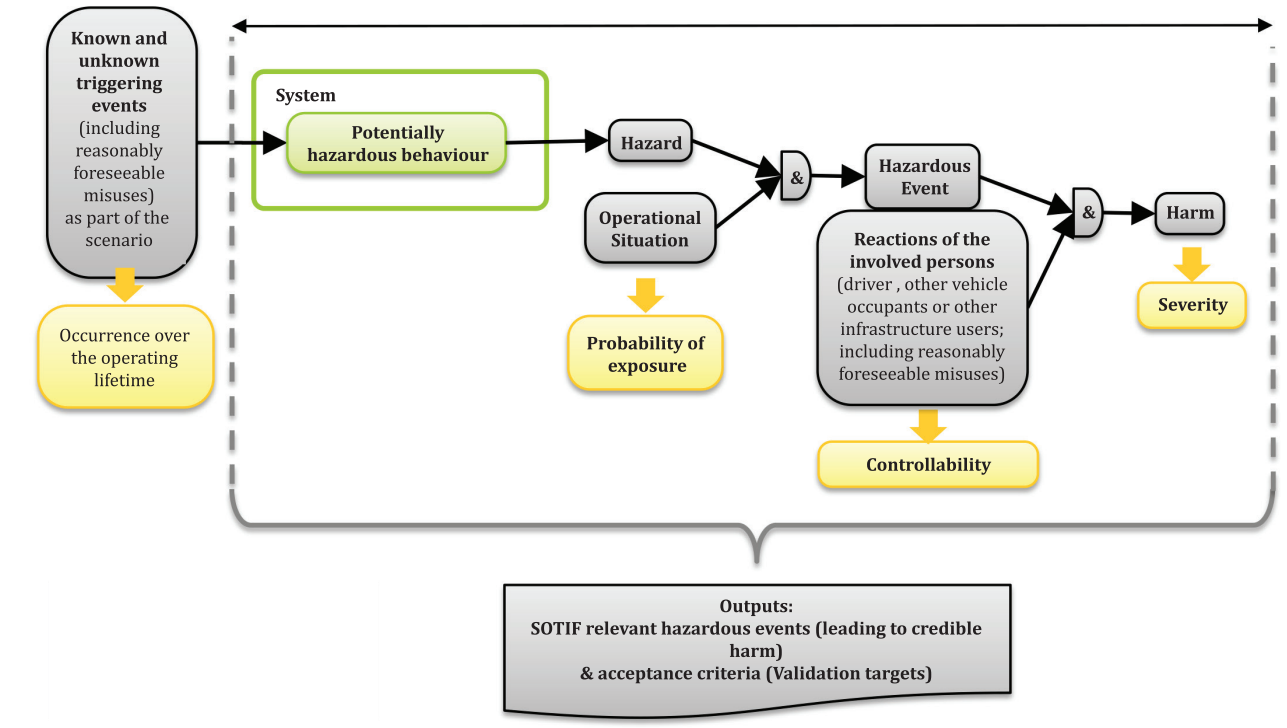
© ISO 2019 – All rights reserved

## 6.2 Hazard identification

The hazards, caused by the unintended behaviour of the function, are determined systematically. This systematic identification is primarily based on knowledge about the function and its possible deviations. This can be achieved by applying the methods proposed in ISO 26262-3:2018 while considering performance limitations of the intended functionality. An illustration of the common elements of the hazard analyse process required by both the ISO 26262 series and by this sub-clause can be found in Figure 12. Figure 13 uses an automated emergency braking (AEB) system as an example to show how the terms from Figure 12 are used.

EXAMPLE 1 For an AEB system, an incorrect detection can cause unintended full braking. However, the system can be designed to limit the allowable braking commanded by AEB. An incorrect detection of a lead vehicle can therefore only trigger braking up to this intended limit. Nevertheless, unwanted braking (due to incorrect detection) limited to the specified authority can have safety consequences. Such unwanted braking events are considered in the SOTIF related risk evaluation.

EXAMPLE 2 A system specified to implement an adaptive cruise control (ACC) function might exhibit undesirable behaviour if several vehicles are using ACC to drive one after another in a line. In such cases, high control loop latencies can lead to an "accordion effect" building-up, until the system is unable to brake hard enough and the driver has to intervene. Although this operational situation might be considered controllable by the driver, the need to avoid such build-up effects might still be analysed as part of the SOTIF.




**Key**

causality

evaluated characteristics

**Figure 12 — An illustration of common elements of hazard analysis in the ISO 26262 series and in this document**

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27



© ISO 2019 – All rights reserved

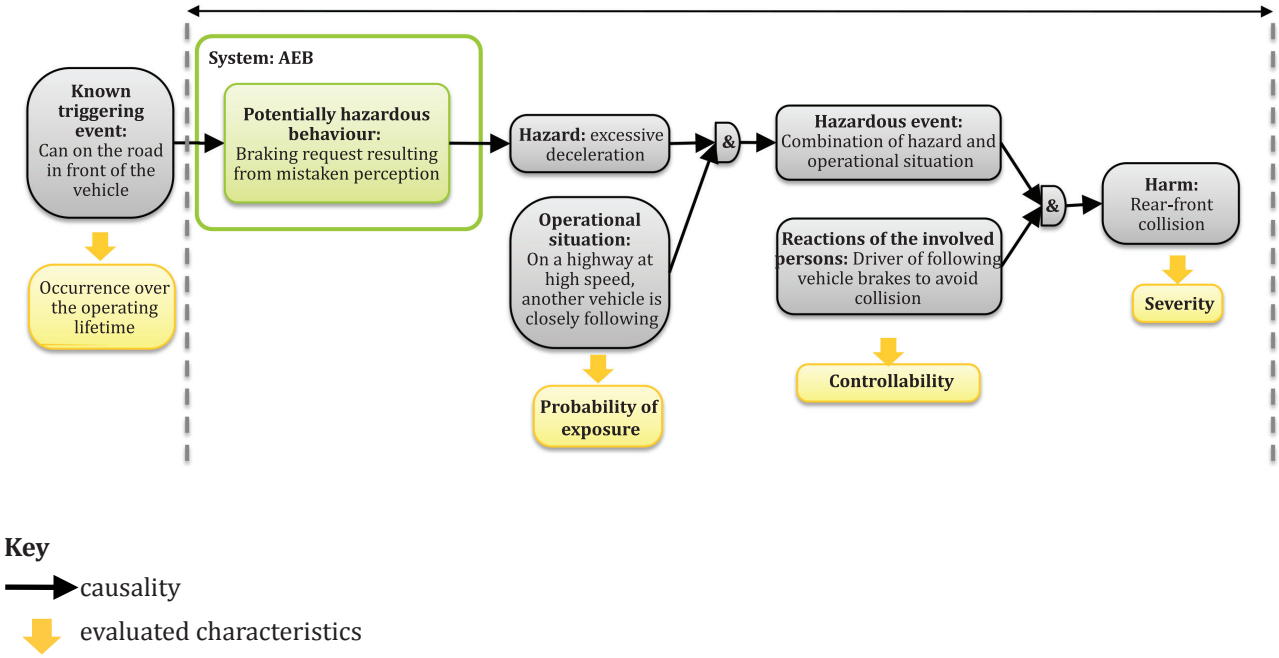



**Figure 13 — An AEB example using terms from Figure 12**

NOTE Unlike in ISO 26262-3:2018, when analysing a SOTIF related hazard, no ASIL is determined for a hazardous event. However, the S, E and C parameters can be used to adjust the validation effort.

## 6.3 Hazard analysis

The harm and controllability of hazardous events can be estimated using the method described in ISO 26262-3:2018, Clause 6 but their evaluation for an individual hazardous event can be specific to a given SOTIF related hazard.

EXAMPLE 1 The severity of a rear collision, caused by emergency braking, can be reduced by limiting the brake intervention magnitude. The magnitude limit can be seen as a safety mechanism to increase controllability, or as a modification to the intended behaviour. When analysing the hazard, the limit is considered part of the intended behaviour; whereas functional failures relating to the implementation of the limit would be the subject of other safety standards, such as the ISO 26262 series.

The severity and controllability of the potentially hazardous behaviour, in a given scenario, are considered to determine whether a credible harm can result. For hazardous event classification a delayed or no reaction to control the hazard, from the involved persons, can be considered.

EXAMPLE 2 An environmental condition that is not supported by an ADAS that requires the driver to resume control.

Delays due to the reaction time of the driver can impact the controllability evaluation and can be a topic of the SOTIF related analysis.

EXAMPLE 3 Table 2 gives an example of the evaluation of a potential consequence for an AEB system and a SOTIF related hazardous event.

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT8IF3EW.2-2022-01-12 18:46:27

© ISO 2019 – All rights reserved

**Table 2 — Example of a hazardous event**

| Hazardous event | Potential consequence | Severity | | Controllability | |
|---|---|---|---|---|---|
| | | Rating | Note | Rating | Note |
| Unintended AEB activation at x m/s² for y s while operating on a highway | Rear collision with following vehicle | S > 0 | Effective impact speed:<br>v ≥ x km/h | C > 0 | The trailing vehicle might not be able to brake to avoid collision. |

## 6.4 Risk evaluation of the intended function

The risk evaluation considers the performance limitations of the intended functionality to judge whether controllability or severity is acceptable; that is controllability is “controllable in general” or severity is “no resulting harm”. The severity and controllability evaluation can take into account the expected system limitations and the measures that have been implemented to mitigate their effects (according to the functional and system specification described in Clause 5).

## 6.5 Specification of a validation target

Validation targets take into account any applicable governmental and industry regulations as well as the current level of functional performance needed to ensure safety. The specified validation targets will depend on the methods chosen in the validation strategy.

EXAMPLE 1 Deductive analysis requires a list of all known and relevant triggering events to be considered. For such analysis, a relevant validation target would ensure the coverage of all events on this list. In contrast, an inductive analysis of SOTIF related hazards would involve a search for previously unknown triggering events that are relevant to the application. In this case, validation targets would be defined with a statistical confidence that the empirical data supports the hypothesis that triggering events do not impose unreasonable risk.

Approaches that can be considered when specifying these targets include:

— the available traffic data for the target market (e.g. accident statistics, traffic analyses) (see D.3); and

— pre-existing targets from similar functions operating in the field.

EXAMPLE 2 The pass/fail criteria for simulation testing, in a given situation, could be defined as: The allowable false positive and false negative rates for a function executing when not required, and, the allowable false positive and false negative rates for a function not executing when required.

If only a subset of scenarios is relevant to a specific hazard, then the exposure to the relevant scenarios (similar to the exposure in ISO 26262-3:2018, Clause 6) can be considered when determining the target value for this hazard and the associated validation duration.

When evaluating the likelihood that, in a given scenario, a triggering event will violate the quantitative target, the exposure, controllability and severity of the resulting behaviour are factors that can be taken into account. This can result in a reduction in the effort required to demonstrate the occurrence rate of the triggering event in Area 3, see Annex B of this document.

EXAMPLE 3 Consider the example from 6.3 where unintended braking only results in a rear crash if a trailing vehicle is present. The exposure rate to a trailing vehicle can be considered when specifying a validation target.

If applicable traffic statistics or field data are unavailable, then an appropriate target can be chosen provided a valid rationale is given.

NOTE 1 A rationale could be based on a risk tolerability principle, such as the French GAMAB or GAME; both have the meaning "globally at least as good". Following this principle, the residual risk (with respect to safety) of any new system is not significantly higher than those of existing systems having comparable functionality and hazards. The application of such a risk tolerability principle to the overall residual risk, that considers all hazards of the new system, allows relevant risk trade-offs to be made. For example, a system can be released even though the residual risk for a given hazard has increased, provided that this is compensated by counter balancing reductions in one or more other residual risks.

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27


© ISO 2019 – All rights reserved

NOTE 2 A rationale could also be based on the ALARP (as low as reasonably practicable) principle. The ALARP Risk Management framework can provide a useful risk reduction principle, particularly with regard to the development and introduction of novel technologies where "good practice" does not currently exist. By acknowledging that a state of zero/no risk is not possible, the ALARP principle aims to reduce risk to a level considered "reasonably practicable" by weighing the risk against the sacrifice needed to further reduce it.

# 7 Identification and Evaluation of triggering events

## 7.1 Objectives

The triggering events:

— that can trigger potentially hazardous behaviour shall be identified;

— shall be evaluated for their acceptability with respect to the SOTIF.

NOTE Triggering event identification can be supported by a detailed environmental model.

## 7.2 Analysis of triggering events

A systematic method can be established to perform the analysis of triggering events. This method can consider knowledge gained from similar projects and field experience. The analysis aims to identify the system weaknesses (including those of its sensors, algorithms, actuators) and the related scenarios that could lead to an identified hazard.

This analysis can be conducted in parallel, starting from both:

— the known limitations of the system components to determine scenarios that could result in hazardous behaviour due to these limitations; and from

— the identified environment conditions and foreseeable misuses to determine the system limitations that could trigger potentially hazardous behaviour of the system. Further detail is given in Annex E and Annex F.

These analyses will increase the understanding of the limitations of the systems and will improve the identification of unknown triggering events.

NOTE The analysis can be supported by inductive and/or deductive methods.

### 7.2.1 Triggering events related to algorithms

An analysis of triggering events related to algorithms is used to determine:

— SOTIF risk mitigation methods and measures according to 8.3;

— decision algorithm verification according to 10.3; and

— validation of functionality according to Clause 11.

The analysis considers categories such as:

— environment and location;

— road infrastructure;

— urban infrastructure;

— highway infrastructure;

— driver behaviour (including reasonably foreseeable driver misuse);

— expected behaviour of other drivers/road users;

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27

© ISO 2019 – All rights reserved

— driving scenario (e.g. a construction site, an accident, a traffic jam with emergency corridor, driving the wrong-way); and

— algorithm limitation, (e.g. capability to handle possible scenarios, or non-deterministic behaviour.).

NOTE The identified functional limitations are included in the list mentioned in Clause 5.

### 7.2.2 Triggering events related to sensors and actuators

An analysis of triggering events related to sensor disturbances and actuator limitations is used to determine:

— SOTIF risk improvement methods and measures according to 8.3;

— sensor verification strategy according to 10.2;

— actuator verification strategy according to 10.4; and

— validation of functionality according to Clause 11.

The analysis considers categories that can cause triggering events such as:

— weather conditions;

— mechanical disturbance (including installation, design location, transmission of signals);

— EMI interference;

— interference from other vehicles or other sources (e.g. radar or lidar);

— acoustic disturbance;

— glare

— poor-quality reflection;

— accuracy;

— range;

— response time;

— durability; and

— authority capability (applicable to actuators).

EXAMPLE 1 Rain and snow can affect radar performance.

EXAMPLE 2 Rising sun in the front of the vehicle can affect the performance of a video camera.

EXAMPLE 3 A heavy woollen coat can affect the performance of ultrasonic sensors.

EXAMPLE 4 An improper alignment can affect many sensor types.

NOTE 1 The considered sensors can include inertial sensors, cameras, radar, etc.

NOTE 2 A potential scenario can be a scenario resulting from a theoretical combination of already observed scenarios.

NOTE 3 For specific analysis categories see Annexes D, E and F. For each category, a list of detailed disturbances is determined based on knowledge and experience (including knowledge gained on similar projects and in field experience).

In addition, a systematic analysis of each environmental input, in the range of possible values (including potential and observed scenarios), can be conducted.


© ISO 2019 – All rights reserved

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27

### 7.3 Acceptability of the triggering events

The identified triggering events are evaluated considering the acceptance criteria that are specified during the SOTIF risk identification and evaluation (as described in Clause 6).

The response of the system to these triggering events can be considered as acceptable with respect to the SOTIF without need of further functional improvement (as described in Clause 8) if:

— The probability of the system causing a hazardous event is lower than the validation target value specified in 6.5; and

— There is no systematically unacceptable scenario in relation to a specific vehicle that has the potential to lead to a hazardous event.

NOTE Even if a fleet has a very low probability of a triggering event, it can be unacceptable if for a specific systematic vehicle behaviour, the probability is high.

EXAMPLE A particular structure that always causes the AEB system to brake excessively.

## 8 Functional modifications to reduce SOTIF related risks

### 8.1 Objectives

The development activities of the functional modifications to reduce the SOTIF related risks shall achieve the following objectives:

— identification and allocation of measures to avoid, reduce, or mitigate the SOTIF related risks;

— estimation of the effect of the SOTIF related measures on the intended function; and

— improvement of the information required by Clause 5 (Functional and system specification).

### 8.2 General

This sub-clause deals with identification of measures to avoid, reduce, or mitigate the SOTIF related risks. The function and system descriptions are developed through several iterations and each time the Functional and System specification (required by Clause 5) is updated with information about the identified measures.

A functional modification to reduce SOTIF related risks may be needed when the identified triggering events:

a) have the possibility to trigger a potentially hazardous behaviour leading to a hazardous event with credible harm (according to Clause 6); and

b) cannot be evaluated as acceptable with respect to the safety of the intended functionality (according to Clause 7).

To support achieving the objectives of this clause, the following information can be considered:

a) information on the system architectural design;

b) the functionality which is defined and described in accordance with Clause 5;

c) the evaluation of the potential outcome of possible hazardous events in accordance with Clause 6;

d) the possible scenarios that can trigger an unintended system behaviour leading to a hazardous event in accordance with Clause 7;

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT8IF3EW.2-2022-01-12 18:46:27

© ISO 2019 – All rights reserved

e) knowledge derived from previous verification results, where the system and components did not behave as expected for specific use cases during verification in accordance with Clause 10 (if any); and

f) knowledge derived from previous validation results including real-life use cases, where the function did not behave as expected and the system and component limitations cause an unreasonable level of risk in accordance with Clause 11 (if any).

## 8.3 Measures to improve the SOTIF

Measures to improve the SOTIF address the identified system limitations (in accordance with 7.2) that lead to a safety violation. Depending on the evaluated SOTIF related risks, the measures to improve the SOTIF can be aimed at avoidance, reduction, or mitigation.

The improvement measures can include:

a) System improvement to avoid or reduce the SOTIF related risks, including but not limited to:

1) Increased sensor performance and/or accuracy by:

— sensor algorithm improvement;

— adequate sensor technology;

— sensor location modification;

— sensor disturbance detection that triggers an appropriate warning and degradation strategy;

— recognition of exiting the operational design domain[3], i.e. recognition of a known unsupported environmental condition that requires a transition to an appropriate sensor usage strategy;

— diverse sensor technology;

2) Increased actuator performance and/or accuracy by:

— adequate actuator technology (e.g. increase accuracy, extend range of output, shorter response times, improve durability, arbitrate authority capability);

3) Increased performance of the recognition and decision algorithms by:

— algorithmic improvements;

— recognition of exiting the operational design domain[3], i.e. recognition of a known unsupported environmental condition that requires a transition to an appropriate warning and degradation strategy;

— design strategy that incorporates the triggering of an appropriate warning and degradation strategy for a known unsupported SOTIF use case;

EXAMPLE Lane keeping.

— strategy for mitigation and resolution of functional interference/conflict (avoidance of unintended behaviour due to inter-system dead lock/live lock);

EXAMPLE Conflict between lane keeping and automatic lane change.

4) Improved testability by:

— allowing verification of system and component behaviour.

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27


© ISO 2019 – All rights reserved

b) Functional restriction made to the intended function to reduce, or mitigate the SOTIF related risks, including but not limited to:

   1) Restriction of the intended function for specific SOTIF use cases;

      EXAMPLE Lane keeping assist functionality is reduced to avoid an undesired steering intervention when lane detection devices cannot clearly detect the lane.

   2) Restriction of authority for the intended function for specific use cases;

      EXAMPLE Camera blinded by a reflection of surrounding light caused by the afternoon sun, operation continues with restricted authority using radar and other sensors.

   3) Restriction of overall authority for the intended function for specific use cases.

      EXAMPLE All perception sensors blinded by a snow storm, driver requested to take over control.

c) Handing over the authority from a system to the driver to improve the controllability (the transition itself being controllable and not representing additional risk to the driver) of the critical operational situation's effect, including but not limited to:

   1) Improving the Human-Machine Interface;

   2) Improving the warning and degradation strategy;

   3) Taking guidance from other sources.

      EXAMPLE RESPONSE3[4].

d) Reduction or mitigation of reasonably foreseeable misuse effects, including but not limited to:

   1) Improving the information provided to the driver about the intended functionality

      EXAMPLE User manual.

   2) Improving the Human-Machine Interface;

   3) Implementation of a monitoring and warning system.

      EXAMPLE Driver warning when the steering wheel is released.

EXAMPLE Table 3 gives an example derivation of SOTIF related measures.

**Table 3 — Example of derived SOTIF related measures**

| | Causal factor of hazard with example | Example of derived SOTIF measure |
|---|---|---|
| E/E System Factor | Exceeding E/E System performance limitation | — Reduce the performance of the system and inform the driver of the reduced or disabled functionality and hand over the authority to the driver.<br>— Gently terminate the function<br>— Degrade and keep the function |
| Driver Factor | Reasonably foreseeable misuse | — Provide measures against inadvertent or careless operation by the driver.<br>— Inform driver about correct operation.<br>— Monitor and warn the driver when an incorrect operation is detected. |

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27

© ISO 2019 – All rights reserved

### 8.4 Updating the system specification

The following information is identified in order to update the functional and system specification:

— measures of system improvements to avoid, reduce, or mitigate the SOTIF related risks;

— measures of functional restrictions to reduce or mitigate critical operational situation effects;

— measures of improvement of the Human-Machine Interface and warning and degradation strategy; and

— measures resulting from the handling of reasonably foreseeable misuses.

## 9 Definition of the verification and validation strategy

### 9.1 Objectives

A verification and validation strategy shall be defined such that:

— It supports the rationale for the SOTIF;

— The necessary evidence (e.g. analysis results, test reports, dedicated investigations) is generated; and

— The procedures to generate the evidence are developed.

The system verification and validation activities with regard to the risk of potentially hazardous behaviour (excluding the faults addressed by the ISO 26262 series) include integration testing activities to address the following scope:

— The ability of sensors and the sensor processing algorithms to model the environment;

— The ability of the decision algorithms to handle both known and unknown situations and to make the appropriate decisions according to the environment model and the system architecture;

— The robustness of the system or function;

— The ability of the HMI to prevent reasonably foreseeable misuse; and

— The manageability of the handover scenario by the driver.

To support the achievement of the objectives of this sub-clause, the following information can be considered:

— Functional concept, including sensors, actuators and algorithm specifications;

— System design specification;

— Verification and validation targets;

— Vehicle architecture;

— Analysis of triggering events results as described in 7.2;

— System design;

— System integration & testing plan;

— Lessons learned.

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT8IF3EW.2-2022-01-12 18:46:27


© ISO 2019 – All rights reserved

## 9.2 Planning and specification of integration and testing

A verification and validation strategy is defined to provide evidence that the objectives are achieved and to state how the targets are to be met. The verification and validation strategy can cover both E/E elements and elements of other technologies considered relevant to the achievement of the SOTIF.

Verification and validation activities consider calibration and configuration data to achieve the SOTIF.

NOTE 1 Variability of the triggering event parameters is considered by evaluating the verification and validation strategy. See Annex D for further practices for the verification and validation of automotive perception systems.

NOTE 2 As functional improvements are made, the system is analysed to determine if additional functions are retested during verification and validation. These dependent functions are verified with regression tests. This ensures that known or new triggering events do not cause potentially hazardous behaviour in unchanged functions. Triggering events found during verification and validation activities, where potentially hazardous behaviour is present, are retested on every release. With a proper rationale, the testing scope can be reduced. To ensure that correct functional behaviour is maintained, complete testing is documented for any release intended for production. This includes documentation of parts that have not been affected and retesting of parts that have been affected by changes.

Methods to specify the verification and validation activities (e.g. integration test cases, analysis) can be derived using an appropriate combination of methods, and by considering the integration level, as illustrated by Table 4.

**Table 4 — Methods for deriving verification and validation activities**

| | Methods |
|---|---|
| A | Analysis of requirements |
| B | Analysis of external and internal interfaces |
| C | Generation and analysis of equivalence classes |
| D | Analysis of boundary values |
| E | Error guessing based on knowledge or experience |
| F | Analysis of functional dependencies |
| G | Analysis of common limit conditions, sequences, and sources of dependent failures |
| H | Analysis of environmental conditions and operational use cases[a] |
| I | Analysis of field experience and lessons learned[b] |
| J | Analysis of system architecture (including redundancies) |
| K | Analysis of sensors design and their known potential limitations |
| L | Analysis of algorithms and their decision paths |
| M | Analysis of system ageing |
| N | Analysis of triggering events |

[a] Including known sources of potentially hazardous behaviour of the element or system.

[b] This considers various driving conditions, driving styles, driving environment and end customer claims

NOTE Annex G discusses verification and validation activities for off-line training such as used for machine learning.

# 10 Verification of the SOTIF (Area 2)

## 10.1 Objectives

The system and components (sensors, algorithms and actuators) shall be verified to show that they behave as expected for known hazardous scenarios and reasonably foreseeable misuse (derived from previous analyses and knowledge). It shall be verified that system and components are covered sufficiently by the tests (see Area 2 of Figure 9).

© ISO 2019 – All rights reserved


Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27

To support the achievement of the objectives of this clause, the following information can be considered:

— Verification strategy, as defined in Clause 9;

— Functional concept, including sensors, actuators and algorithm specification;

— System design specification;

— Verification targets;

— Vehicle design (e.g. mounting position); and

— Analysis of triggering events results as described in 7.2.

The structure of 10.2 to 10.5 is following the input (10.2) — process (10.3) — output (10.4) (IPO) pattern and adds an additional 10.5 that specifically addresses integration aspects of the verification.

## 10.2 Sensor verification

Methods to demonstrate the correct functional performance, timing, accuracy, and robustness of the sensors for their intended use can be applied as illustrated by Table 5.

**Table 5 — Sensor verification**

| | Methods |
|---|---|
| A | Verification of standalone sensor characteristics (e.g. range, precision, resolution, timing constraints, bandwidth, signal-to-noise ratio) |
| B | Requirements based test |
| C | Injection of system inputs that trigger the potentially hazardous behaviour[a] |
| D | In the loop testing (e.g. SIL/HIL/MIL) on selected SOTIF relevant use cases and scenarios |
| E | Vehicle level testing on selected SOTIF relevant use cases and scenarios |
| F | Sensor test under different environmental conditions (e.g. cold, damp, light, visibility conditions) |
| G | Verification of sensor ageing effects (e.g. accelerated life testing, etc.) |
| H | Verification of vehicle mounted sensing system characteristics[b] |

[a] In some cases, it is possible to emulate a potentially hazardous behaviour of the sensor by means of error injection at the simulation level. A rationale as to why the error models are able to represent the tested phenomena is provided. Outcomes of those simulations can be combined with results of the analysis of triggering events.

[b] This includes the operation of the different sensors under different operating conditions (e.g. where one sensor technology is failing, such as fog affecting a camera)

NOTE For test case derivation the method of combinatorial testing can be used[5].

Annex D provides examples for the verification of perception sensors.

## 10.3 Decision algorithm verification

Decision-algorithms are included in all parts of the functional chain (e.g. classification, sensor data fusion, situation analysis, function). Methods to verify the ability of the decision-algorithm to react when required and its ability to avoid unwanted action can be applied as illustrated by Table 6.

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27



© ISO 2019 – All rights reserved

**Table 6 — Decision Algorithm verification**

| Methods | |
|---|---|
| A | Verification of robustness to interference from other sources, e.g. white noise, audio frequencies, Signal-to-Noise Ratio degradation (e.g. by noise injection testing) |
| B | Requirement-based test (e.g. classification, sensor data fusion, situation analysis, function) |
| C | Verification of the architectural properties including independence, if applicable |
| D | In the loop testing (e.g. SIL/HIL/MIL) on selected SOTIF relevant use cases and scenarios |
| E | Vehicle level testing on selected SOTIF relevant use cases and scenarios |
| F | Inject inputs into the system that trigger potentially hazardous behaviour |
| NOTE For test case derivation the method of combinatorial testing can be used[5]. | |

## 10.4 Actuation verification

Methods to verify the actuators for their intended use and for their reasonably foreseeable misuse in the decision algorithm can be applied as illustrated by Table 7.

**Table 7 — Actuation verification**

| Methods | |
|---|---|
| A | Requirements-based test (e.g. precision, resolution, timing constraints, bandwidth) |
| B | Verification of actuator characteristics, when integrated within the vehicle environment |
| C | Actuator test under different environmental conditions (e.g. cold conditions, damp conditions) |
| D | Actuator test between different preload conditions (e.g. change from medium to maximum load) |
| E | Verification of actuator ageing effects (e.g. accelerated life testing) |
| F | In the loop testing (e.g. SIL/HIL/MIL) on selected SOTIF relevant use cases and scenarios |
| G | Vehicle level testing on selected SOTIF relevant use cases and scenarios |

## 10.5 Integrated system verification

Methods to verify the robustness and the controllability of the system integrated into the vehicle can be applied as illustrated by Table 8.

**Table 8 — Integrated system verification**

| Methods | |
|---|---|
| A | Verification of robustness to Signal-to-Noise Ratio degradation (e.g. by noise injection testing) |
| B | Requirement-based Test when integrated within the vehicle environment (e.g. range, precision, resolution, timing constraints, bandwidth) |
| C | In the loop testing (e.g. SIL/HIL/MIL) on selected SOTIF relevant use cases and scenarios |
| D | System test under different environmental conditions (e.g. cold, damp, light, visibility conditions) |
| E | Verification of system ageing affects. (e.g. accelerated life testing) |
| F | Randomized input tests [a)] |
| G | Vehicle level testing on selected SOTIF relevant use cases and scenarios |
| H | Controllability tests (including reasonably foreseeable misuse) |
| [a] Randomized input tests can include erroneous patterns e.g. in the case of image sensors adding flipped images or altered image patches; or in the case of radar sensors adding ghost targets to simulate multi-path returns. | |

Annex D provides examples for the verification of perception systems.

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27

© ISO 2019 – All rights reserved

# 11 Validation of the SOTIF (Area 3)

## 11.1 Objectives

The functions of the system and the components (sensors, decision-algorithms and actuators) shall be validated to show that they do not cause an unreasonable level of risk in real-life use cases (see Area 3 of Figure 9). This requires evidence that the validation targets are met.

To support the achievement of this objective the following information can be considered:

— Validation strategy, as defined in Clause 9;

— Verification results in defined use cases, as defined in Clause 10;

— Functional concept, including sensors, actuators and decision-algorithm specification;

— System design specification;

— Validation targets, as defined in Clause 6;

— Vehicle design (e.g. sensor mounting position); and

— Analysis of triggering events results as described in 7.2.

## 11.2 Evaluation of residual risk

Methods to evaluate the residual risk arising from real-life situations, that could trigger a hazardous behaviour of the system when integrated in the vehicle, can be applied as illustrated by Table 9.

**Table 9 — Evaluation of residual risk**

| | Methods |
|---|---|
| A | Validation of robustness to Signal-to-Noise Ratio degradation (e.g. by noise injection testing) |
| B | Verification of the architectural properties including independence, if applicable |
| C | In the loop testing on randomized test cases (derived from a technical analysis and by error guessing) |
| D | Randomized input tests[a] |
| E | Vehicle level testing on selected test cases (derived from a technical analysis and by error guessing) |
| F | Long term vehicle test |
| G | Fleet tests |
| H | Test derived from field experience |
| I | Tests of corner cases[b] and reasonably foreseeable misuse |
| J | Comparison with existing systems |
| K | Simulation of selected scenarios |
| L | Analysis of worst case scenarios |

[a] Randomised input tests can include erroneous patterns e.g. in the case of image sensors adding flipped images, altered image patches; or in the case of radar sensors adding ghost targets to simulate multi-path returns.

[b] A corner case is a rare or unusual condition.

## 11.3 Validation test parameters

For each of the applied methods described in Table 9, an appropriate cumulated test length is selected. A rationale for the test length selected is provided and correlated with the number and distribution of scenarios. Generally, for all selected test methods a rationale is provided establishing that the resulting distribution of system inputs is representative of either the general operational environment or the specific use case, scene or scenario. Vehicle test length determination (long term tests, fleet tests) can take into account knowledge from prior vehicle programmes, driver controllability, or the criticality


© ISO 2019 – All rights reserved

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27

of selected test routes. In the case of the use of randomised input tests, the number of scenarios being simulated in which erroneous patterns are injected can be correlated with the test length and test content that is representative of the target market.

Annexes B, C and D provide examples for the validation of SOTIF relevant systems.

EXAMPLE When evaluating an image recognition algorithm using simulation, a cumulated test length of X hours is selected, with Y different scenarios. The distribution of scenarios is adjusted according to the challenging scenarios and the distribution of driving use cases from traffic data. The susceptibility of the algorithm to real-life triggers is identified by analysis of the algorithm and its decision paths. Scenarios with the most sensitive algorithm characteristics are included with a distribution emphasizing the challenging scenarios and representing their statistical relevance. The probabilities of occurrence of the influencing parameters in real-life use cases can also be considered to determine the appropriate test length.

# 12 Methodology and criteria for SOTIF release

## 12.1 Objectives

A SOTIF release shall be performed to:

— review the SOTIF activities, and

— evaluate the acceptability of the residual risk considering the findings of the SOTIF activities.

To support the achievement of the objectives of this clause, the following information is considered:

— functional and system specification as defined in Clause 5;

— verification and validation targets as defined in Clause 6;

— analysis of triggering events as defined in Clause 7;

— functional improvements as the result of Clause 8 activities;

— verification and validation strategy, as defined in Clause 9;

— results of verification as defined in Clause 10; and

— results of the validation of the SOTIF as defined in Clause 11

## 12.2 Methodology for evaluating SOTIF for release

The prerequisite information is reviewed taking the following into account:

1) Did the validation strategy take into account all the specified use cases within the scope of the intended functions?

   a) Did the testing cover identified triggering events?

      EXAMPLE Narrow metallic structures for the radars falsely triggering braking.

   b) Was it tailored for differences from previous validations?

2) Does the intended functionality achieve a minimum fall-back risk condition[3], when necessary, providing a state without unreasonable risk to the occupants or other road users:

   a) Using only the specified driver intervention;

   b) Taking into account reasonably foreseeable misuse; and

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27

© ISO 2019 – All rights reserved

c) Warning to the vehicle occupants and/ or the other road users of the malfunctioning vehicle.

3) Was sufficient verification and validation completed and acceptance criteria met, to have confidence that the risk is not unreasonable?

   a) Has the intended function been exercised sufficiently to evaluate both nominal behaviour and potential unwanted behaviour?

   b) Was no unintended behaviour observed with the possibility to lead to a hazardous event?

4) In case of an unintended behaviour with the possibility to lead to a hazardous event, was evidence provided to argue the absence of unreasonable risk?

EXAMPLE See Annexes B, C and D.

NOTE The examination of the results of the SOTIF activities can be considered in ISO 26262-2:2018 functional safety assessment.

## 12.3 Criteria for SOTIF release

Based on evidence of the methodology from 12.2, 3) above, a recommendation of "acceptance", "conditional acceptance", or "rejection" for release may be determined using the following criteria:

a) For "acceptance", points 1, 2, and 3 of 12.2 are satisfied.

b) For "conditional acceptance", points 1, 2, and 4 of 12.2 are satisfied. The condition is satisfied when the risk is shown not to be unreasonable by the specified date.

c) Neither 12.3 a) nor 12.3 b) are satisfied, the SOTIF release status is "rejection".

See Figure 14 for a flowchart of the SOTIF release decision logic.

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT8IF3EW.2-2022-01-12 18:46:27


© ISO 2019 – All rights reserved

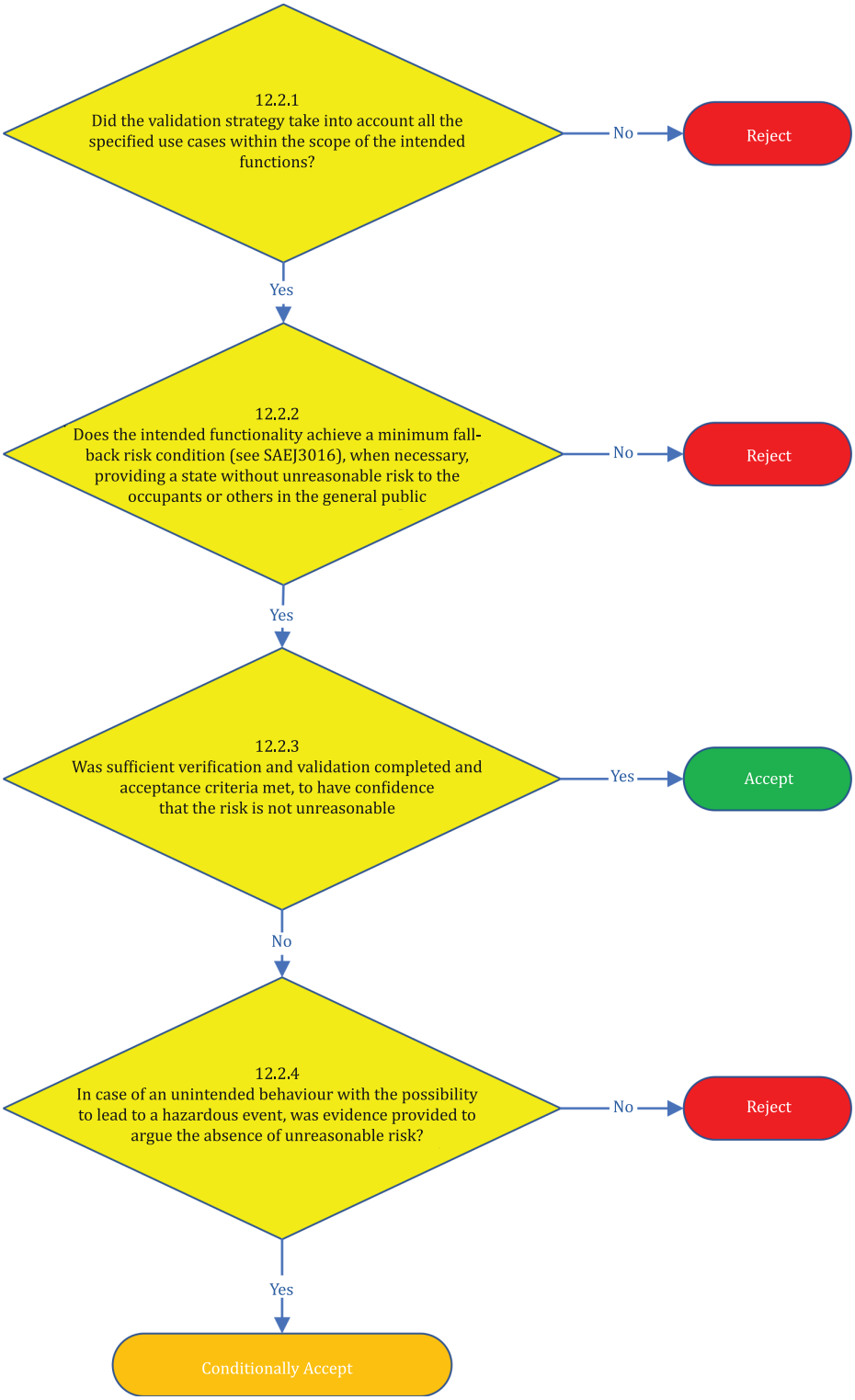



**Figure 14 — Evaluation of criteria for SOTIF release**

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27

© ISO 2019 – All rights reserved

# Annex A
(informative)

# Examples of the application of SOTIF activities

| Elements of flow diagram | Example 1: Lane Keeping Support (LKS) | Example 2: Automatic Emergency Braking (AEB) | Area of SOTIF diagram (see Figure 7) |
|---|---|---|---|
| Start - functional system specification | This function uses a video camera to detect the lane markings ahead of the vehicle. If it detects that the vehicle is getting too close to the side of its lane, Lane Keeping Support (LKS) will take action by applying a corresponding steering torque. | This function uses a radar sensor to scan the distance to the obstacle (e.g. vehicle) in front. If it detects an imminent collision, Automatic Emergency Braking (AEB) will be triggered. | NA |
| SOTIF-related hazard identification and risk evaluation | Traffic situation: driving on the highway with LKS active. The driver might rely on the function and drive hands-off.<br>Potential hazard: Unwanted steering activation could lead to a collision with oncoming traffic or with other obstacles. | Traffic situation: driving on roads with heavy traffic (e.g. suburban road).<br>Potential hazard: Unwanted emergency braking could lead to a rear end collision with the following vehicle. | Area 2<br>Area 3 |
| Risk of harm acceptable? (NO) | No control of the hazard because the driver might rely on the function and be driving hands-off and be unable to take over in time. | No control of the hazard by the driver. Control of hazard by the following driver depends on the distance between the two vehicles. | Area 2<br>Area 3 |
| Identification and evaluation of triggering events | Crossing lane marking (e.g. before construction zone)[6]<br>  | Special road conditions (e.g. manhole cover, tunnels, beverage can) can give a radar echo, which could be interpreted as a potential obstacle. | Area 2<br>Area 3 |
| Identified triggering events acceptable? (NO) | "No": The SOTIF related risk is not accepted. The controllability of the function by the driver must be ensured. | The severity of the rear end collision caused by unwanted emergency braking must be reduced. | Area 2 |
| Functional modification to reduce SOTIF risk | Functional improvement: Implemented detection of driver not holding steering wheel. | Limit the duration and/or strength of the braking intervention. | Area 1<br>Area 2 |

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27


© ISO 2019 – All rights reserved

| Elements of flow diagram | Example 1: Lane Keeping Support (LKS) | Example 2: Automatic Emergency Braking (AEB) | Area of SOTIF diagram (see Figure 7) |
|---|---|---|---|
| Functional and system specification | This function uses a video camera to detect the lane markings ahead of the vehicle. If it detects that the vehicle is getting too close to the side of its lane, LKS will take action.<br>*Additional specification: Driver warning in case of hands-off, detected based on capacitive sensing, to ensure hands-on driving maintained.* | This function uses a radar sensor in order to scan the distance to the vehicle in the front. If it detects an imminent collision, Automatic Emergency Braking (AEB) will be triggered.<br>*Additional specification: Limitation of the braking intervention to minimise or prevent damage in case of unwanted emergency braking.* | Area 1<br>Area 2 |
| Identified triggering events acceptable? (Yes) | "Yes": The SOTIF related risk is accepted. No further improvements. | No further improvements. | Area 2 |
| Definition of the verification and validation strategy | Definition of test cases for evaluating the LKS function in known and unknown unsafe scenarios based on Clause 9, Table 4. | Definition of test cases for evaluating the AEB function in known and unknown unsafe scenarios based on Clause 9, Table 4. | Area 2<br>Area 3 |
| Verification of the SOTIF | Verification of hands-off detection at system integration level, based on Clause 10, Table 8 (e.g. capacitive-measurement on HIL, robustness tests)<br>Additionally, studies with test persons e.g. using a driving simulator | Known scenarios which could lead to unwanted emergency braking (e.g. manhole, beverage can) are considered in each new project and verified on a test track and/or in simulation and/or during an endurance run.<br>Result: All known scenarios are removed except the detection and reaction to a moving beverage can. | Area 2 |
| Known scenarios are sufficiently covered?<br>System and components behave as expected? (Yes) | "Yes". Increasing driver awareness due to the warnings resulting from hands-off detection. Evidence of sufficient controllability by studies with test persons. | Assumption that the probability of the occurrence of a moving beverage can in front of the vehicle is very low and so acceptable. | Area 2 |

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT8IF3EW.2-2022-01-12 18:46:27

© ISO 2019 – All rights reserved

| Elements of flow diagram | Example 1: Lane Keeping Support (LKS) | Example 2: Automatic Emergency Braking (AEB) | Area of SOTIF diagram (see Figure 7) |
|---|---|---|---|
| Validation of the SOTIF | Long-term endurance run based on a knowledge-based driving catalogue to prove controllability in further (unknown) scenarios.<br>Result from endurance run: false hands-on detection only possible with intentional steering wheel alterations. This is considered as abuse. | Vehicle level testing on selected test cases (derived from technical analysis and error guessing).<br>Endurance run for the function that is representative of the target market and that obtains statistical evidence about remaining unknown scenarios | Area 3 |
| System and components do not cause unreasonable risk in real-life scenarios? (Yes) | "Yes". Target level for endurance run complies with the state of the art and GAMAB principle (description of GAMAB see 6.5) | Target level for endurance run complies with the state of the art and GAMAB principle (description of GAMAB see 6.5).<br>Reduction in the amount of endurance runs possible by using experience and results from preceding projects. Justification of the reusability of test evidence is necessary. | Area 3 |
| Methodology and criteria for SOTIF release/ Acceptable residual risk?<br>(YES) | "Yes". Verification of hands-off detection done by testing. No further unknown unsafe scenarios identified during endurance run.<br>Residual risk acceptable. | Achievement of the verification and validation target values is demonstrated.<br>Residual risk acceptable. | Area 2<br>Area 3 |

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.Y0HZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27


© ISO 2019 – All rights reserved

# Annex B
(informative)

# Example for definition and validation of an acceptable false alarm rate in AEB systems

## B.1 Objective and structure of this annex

The objective of this Annex is to show an example of evaluating SOTIF for release (see 12.2 and 12.3). This example demonstrates a method for the validation of an Automatic Emergency Braking system (AEB) based on published traffic accident statistics. Test driving was chosen as the validation method. The target mileage was calculated using statistical methods and a 4-step analysis. The steps are described in the individual sub-clauses of this Annex (see also Figure B.1). The list of steps is given below and for each step its partial objective is formulated.

1) Partition of system failures

   — For the target system, identify parameters that can lead to a hazardous event caused by suboptimal model boundary definitions

   — Clarify the relationship between the SOTIF hazardous event and the combination of these parameters

2) Modelling of hazardous events

   — Consider representative parameters that cause system performance limitations

   — Model the scenarios of hazardous events

   — Use the derived scenarios to assess the influence of the selected parameters on the probability of harm

3) Analysis of traffic statistics

   — Identify statistical variables relevant to the scenarios derived on the previous step

   — Calculate the probability of occurrence for each hazardous scenario

   — Calculate target validation mileage using statistical simulation based on the models of hazardous scenarios

4) Define test scenarios

   — Select target validation test scenarios according to the mission profile that relate to the false alarm rate

NOTE 1 This annex is related to Area 3 “Unknown unsafe scenarios” (see Figure 7). Actions to reduce the risk in Area 2 “Known unsafe scenarios” (Clause 7) and to complete the verification of the SOTIF (Clause 10) are assumed to be executed prior to production vehicle deployment and are not covered by this annex.

NOTE 2 This annex is based on the presentation[7].

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT8IF3EW.2-2022-01-12 18:46:27

© ISO 2019 – All rights reserved

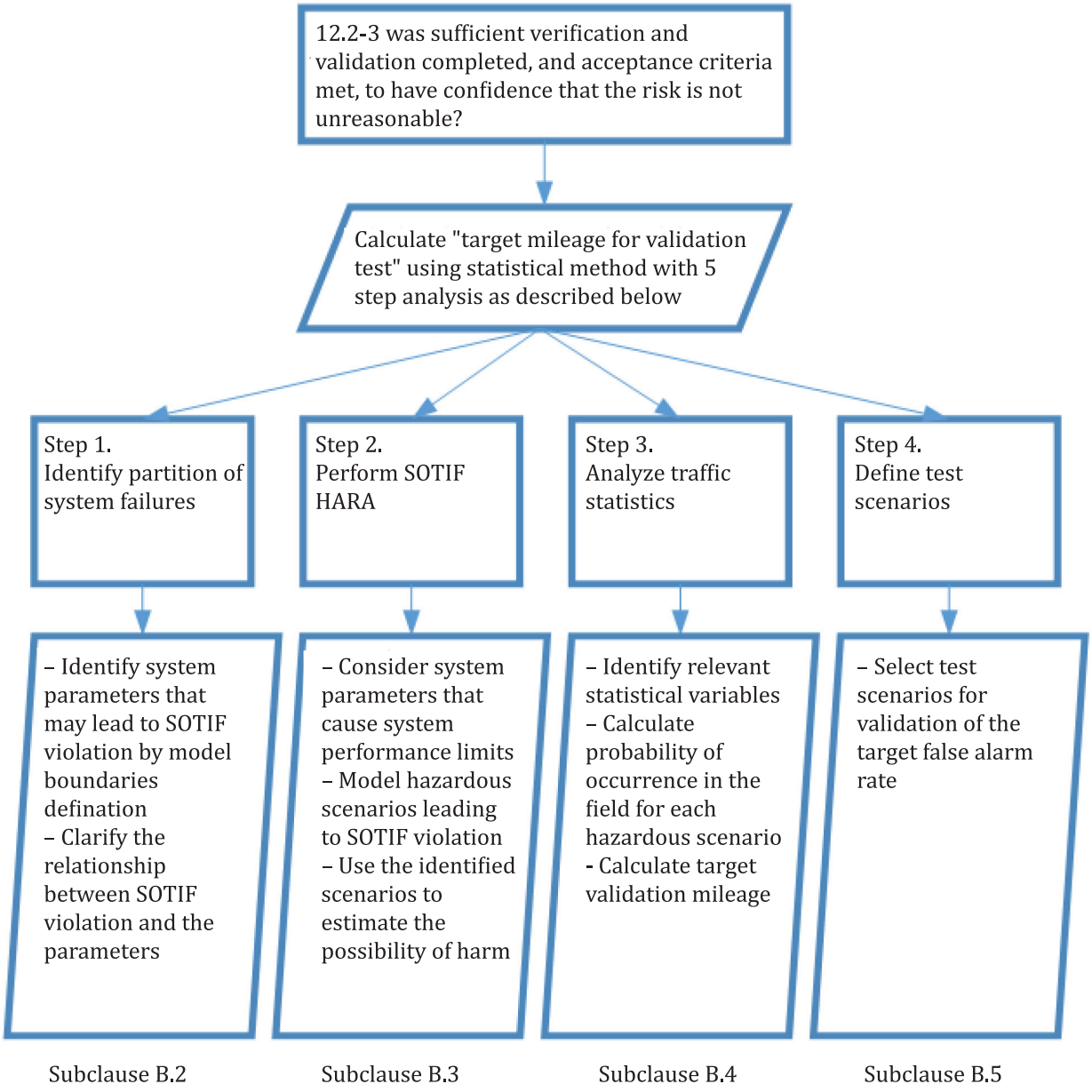



**Figure B.1 — Overview of Annex B**

## B.2 Partition of system failures

Vehicle control systems, which have some authority over the braking system (e.g. AEB), can potentially place the driver or other road users at risk through an erroneous actuation. False identification of the driving scenario might activate emergency braking bringing the vehicle to a complete stop when not needed.

Some ADAS algorithms (e.g. Bayesian estimators, neural networks) for object recognition are affected by failures caused by performance limitations — a group of failures different to those defined within the ISO 26262:2018 series.

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27


© ISO 2019 – All rights reserved

In the case of AEB systems as well as other ADAS functions, the causes of hazardous events can be classified in three categories:

1) Hardware failures (both random and systematic) responsible for safety goal violation can be controlled by the application of ISO 26262-5;

2) Systematic software failures responsible for safety goal violation can be controlled by the application of ISO 26262-6;

3) Unintended behaviour due to performance limitations.

Unintended behaviour due to performance limitations can contribute to safety violations. The scenarios of those violations can be identified in the ISO 26262-3:2018 HARA (e.g. crash due to an as unintended AEB actuation). The safety analyses according to ISO 26262-3, however, tend to focus on design failures (points 1 and 2 from the list above). This document can consider other sources of hazards such as reasonably foreseeable misuse as a triggering event for the potentially hazardous behaviour of the system.

The AEB system behaviour can be modelled at a very high level through three parameters:

— Probability of existence, $P_E$: How confident we are that an object is in front of us?

— Probability of collision, $P_C$: How likely it is that we are going to collide with the object in front?

— Time to collide, *TTC*: Time left before collision.

The system commands AEB activation when the conjunction of the following conditions holds: probability of existence exceeds a given threshold, probability of collision exceeds a given threshold, AND time to collide (TTC) is below a certain threshold ($\overline{TTC}$). Mathematically, this can be written in the following way:

$$\begin{cases} TTC < \overline{TTC} \\ P_C > \overline{P_C} \\ P_E > \overline{P_E} \end{cases} \Rightarrow AEB\ activation$$

The relationship between a safety violation and the combination of these parameters is not linear. Besides the parameters listed in the system above, it can depend on multiple external factors.

## B.3 Modelling of the hazardous event

Considering a system able to perform AEB with the deceleration profile shown in Figure B.2 and within the following performance limitations:

— AEB system commands braking with maximum negative acceleration of 0,9 g in response to a moving object;

— Brake rise time is subject to a brake system pre-fill and limited to 15 m/s$^3$;

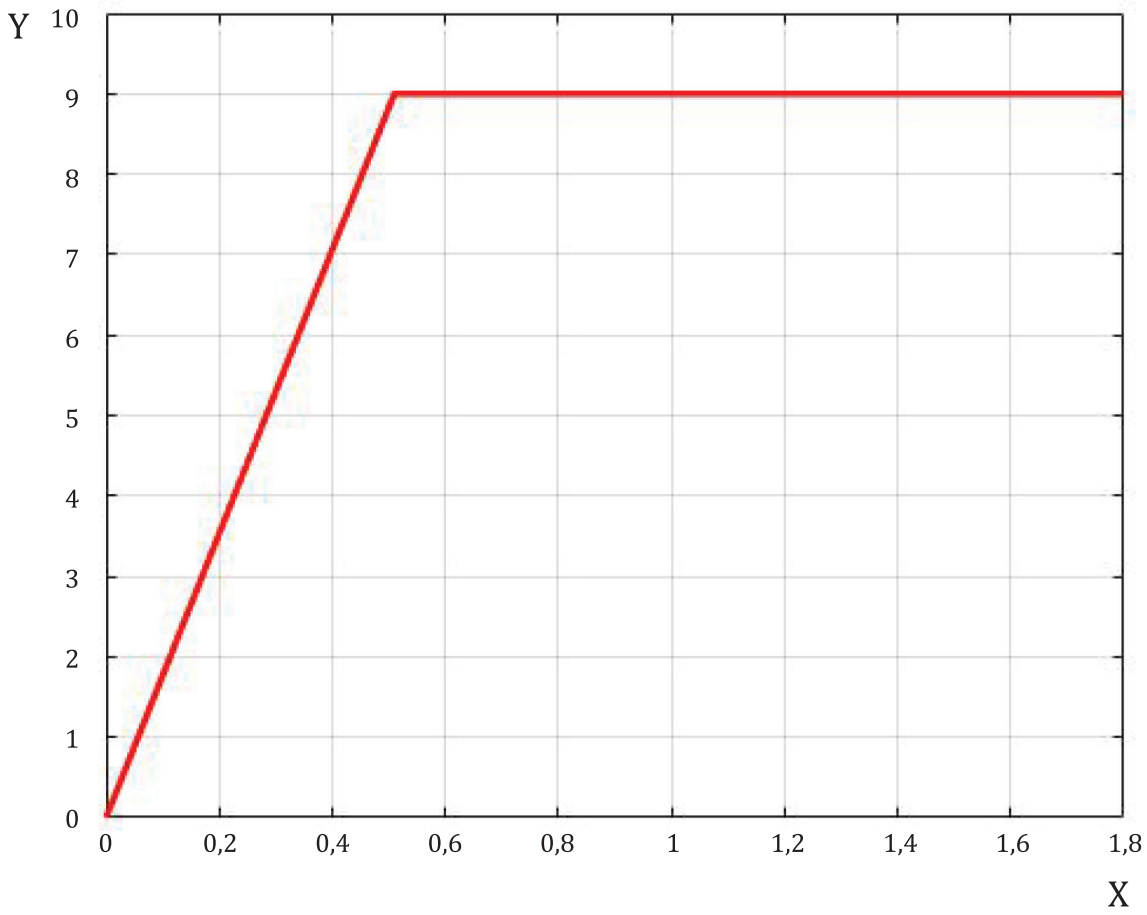
— AEB feature is available between 5 km/h and 80 km/h;

— A maximum speed reduction of 50 km/h is allowed;

— Safety mechanisms in the sensor and the braking systems will prevent AEB commanding deceleration outside the designated speed range.

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT8IF3EW.2-2022-01-12 18:46:27

© ISO 2019 – All rights reserved




**Key**

X Time [s]

Y Deceleration [m/s$^2$]

**Figure B.2 — Deceleration profile for AEB**

The Safety Goal and relevant hazardous scenario were identified in the HARA performed according to ISO 26262-3.

**Safety Goal**: Unintended AEB braking within design intent for longer than 340 ms should be avoided.

**Hazardous scenario**: AEB event lasting longer than 340 ms at a time when an attentive driver would not perceive the need of an AEB actuation.

Possible SOTIF-relevant causes for the realization of the hazardous scenario include a rear-end crash after the AEB is activated by an algorithm error caused by a suboptimal model boundary definition. The Hazard of unintended deceleration can be modelled as a straight road car-following scenario for first order effects (see Figure B.3)[8].

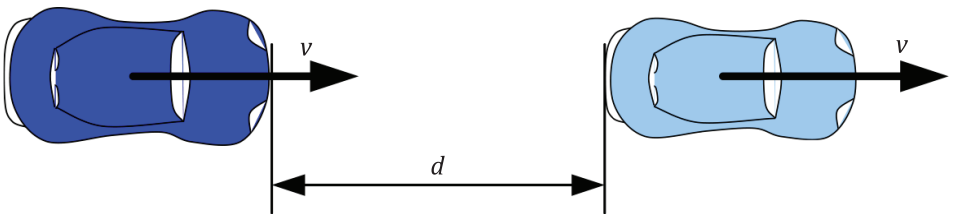



**Figure B.3 — Car-following scenario used in the hazardous event model**

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27



© ISO 2019 – All rights reserved

The scenario is based on the following assumptions:

— Both cars are travelling at the same speed, *v*.

— The headway, *d*, has known probability distribution.

— The first vehicle's AEB activates emergency braking, even though the driving situation does not require that.

— All AEB braking events follow the braking profile pictured on Figure B.2.

— The following driver perceives the hazardous situation and reacts by braking. The reaction time has a known probability distribution.

The Monte Carlo simulation based on the defined distance between cars in traffic and response time distributions was used to identify the outcome of various brake events. Some of them can result in a collision. The outcome largely depends on the speed of the vehicles when the unintended AEB activation occurs.

The simulation model delivers the percentage of unintended AEB activation cases that result in a collision. The simulation takes the start speed $v$ and interval of differential speed at collision $\delta v$ as inputs, while the percentage of the simulations that result in a collision where start speed was of v and speed difference at the time of collision falls into $\delta v$ is considered as the output. The dependency produced by the model is formally described by the Formula (B.1):

$$P_{collision} = P(v, \delta v) \tag{B.1}$$

## B.4 Analysis of traffic statistics

According to ISO 26262-1:2018, a HARA can identify the mishap(s) associated with an ADAS function. It is assumed for AEB that the most common mishap related to AEB functionality is associated with injuries arising as a consequence of rear-end collision between two cars in a car-following scenario (see Figure B.3). An analysis was performed in order to identify the maximum tolerable (accepted) occurrence rate of rear-end collisions. A rate below the existing occurrence rate is considered as accepted by the general public. Traffic statistics provided by national road safety authorities can offer an overview of the existing rate at which the mishap happens in the field, classified by the posted speed in the locality of the accident. The data providers include NHTSA for the US, ONISR for France, ITARDA for Japan, BASt for Germany. Besides statistical overviews of road safety, ONISR also provides a database listing precise characterization of all accidents in France that resulted in injury or death of people (BAAC). Data with similar granularity can be obtained from the GIDAS study (Germany).

Traffic statistics can provide the following data:

— Number of passenger cars in the field ($N$).

— Average distance travelled by each passenger car per year ($K$).

— Number of rear end collision in the field per year within the range of defined posted speed, $v$ ($A_v$).

Based on this information, average distance travelled between collisions in each speed range can be calculated, see Formula (B.2). An assurance coefficient $C_a$ is adopted to avoid under-estimation of the target validation mileage distance (e.g. accidents due to justified braking). The confidence of the model used to determine the probability of collision can be conservative enough not to warrant any further

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27

© ISO 2019 – All rights reserved

consideration of statistical confidence, e.g. much more conservative than a 70 % confidence interval. However, further statistical confidence can be added, if relevant by using the $C_a$ factor.

$$C_{KT\_v} = \frac{NK}{A_v} C_a \tag{B.2}$$

The goal of the analysis is that the end user of the vehicle cannot be exposed to a risk of a rear end collision which is higher than the one normally accepted using a vehicle not equipped with an AEB system. It is assumed that the use of AEB cannot increase the risk of accidents of types other than rear end collision.

The value $C_{KT\_v}$ represents the target false alarm rate for the system in each posted speed limit interval.

NOTE The target presented above is only a probabilistic theoretical objective to explain risk that can be tolerated in the decision to release the product to the market. Therefore, even if this probability is achieved, when a false alarm occurs in the actual market, the judgment of whether countermeasures are necessary requires another consideration.

Merging the dependencies taken from the traffic statistics analyses (B.2) with the results of the simulation as given by Formula (B.1) and taking all feasible values of $\delta v$ (i.e. $|\delta v| < |v|$) into account, it is possible to identify (in relation to the performance described in B.3) the number of kilometres of data ($D_{\mathrm{km}}$) that need to be collected/analysed at each posted speed limit in order to validate that the system behaviour is robust enough with respect to the SOTIF requirements:

$$D_{km} = P(v) C_{KT\_v} = \frac{K}{A_v C_a} \sum_{\delta v} P(v, \delta v) \tag{B.3}$$

NOTE 1 If a “grey box” approach is used, and the architecture includes independent elements with independent logic such that some statistical independence can be shown, then this architecture can be evaluated taking this independence into account. Reduction in validation requirements for each independent element can result. Any statistical dependency is considered, e.g. as in the Beta Factor in IEC 61508.

NOTE 2 For all calculations and inferences performed based on statistical data, it is required to utilize appropriate methods and confidence levels that are standard for the industry.

## B.5 Definition of the amount of data collection

The vehicle mission profile can be used to address the data collection and validation strategy as well as available data from recognized international standards. As an example, Figure B.4 shows the speed intervals observable on roads of different kinds. Colour coding shows the probability of rear-end collision as a result of an erroneous AEB activation. The information on “risky” speed ranges can be used to address the data collection for the AEB system.

NOTE A potential AEB activation at a speed of more than 80 km/h violates the limitations of the item. This can, for example, be implemented by an external measure as suggested in ISO 26262-3.

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27


© ISO 2019 – All rights reserved

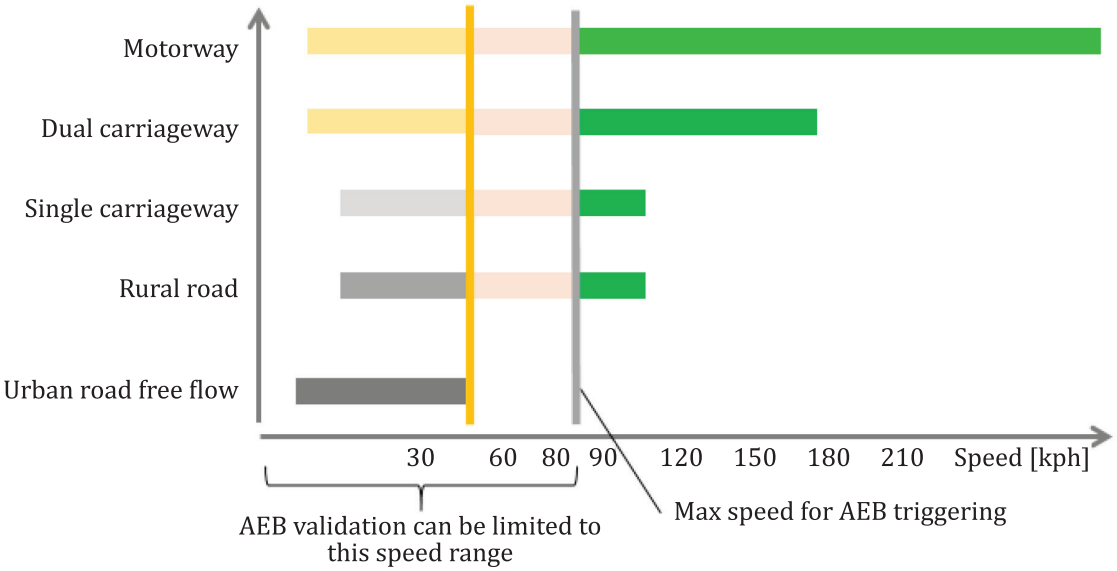



**Figure B.4 — Target validation mileage per posted speed limit**

Depending on the vehicle mission profile and the required performance, the data collection can include a comprehensive variety of driving conditions in terms of weather, time of day, and speed. As an example:

— Speed: the host vehicle speed can be relevant for the feature in scope. For this example, no speeds above 80 km/h are considered.

— Weather condition: the AEB system can be tested according to a representative set of weather conditions. This includes dry, fog, snow, rain, overcast, etc.

— Time of day: depending on the type of sensor, data collection can include different times of day, such as night, dusk, etc.

In addition, the data collection can include relevant driving situations derived from analysis of sensor limitations and feature specific limitations.

An example of data collection specification for the feature that is the subject of this example is given in Table B.1. The specification may be based on real-life profiles for weather, speed and other parameters. An alternative approach suggests choosing the parameters related to the increased probability of a traffic accident of interest (e.g. rear end collision for the considered example). The relationship between external parameters and probability of accidents of specific types may be found via statistical analysis.

**Table B.1 — Example of data collection specification**

| **Time of day** | | |
|---|---|---|
| **Type** | | **Percentage** |
| Day | | 50 % |
| Night | | 35 % |
| Dusk | | 15 % |
| **Vehicle Speed** | | |
| **Speed [mi/h]** | **Speed [km/h]** | **Percentage** |
| 0–25 | 0–40 | 60 % |
| 26–50 | 41–80 | 40 % |
| >50 | >80 | 0 % |
| **Weather condition** | | |

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27

© ISO 2019 – All rights reserved

**Table B.1** *(continued)*

| Type | Percentage |
|---|---|
| Dry/Clear sky | 65 % |
| Rain | 7 % |
| Fog | 5 % |
| Snow | 5 % |
| Overcast | 10 % |
| Heavy rain | 5 % |

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-IDJY0HZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27



© ISO 2019 – All rights reserved

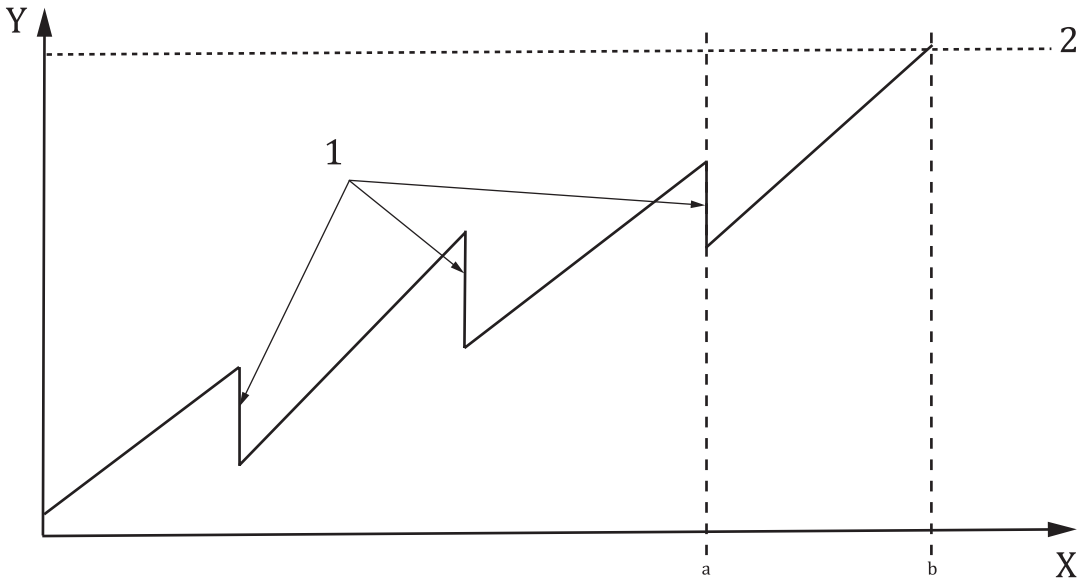
# Annex C
(informative)

# Validation of SOTIF applicable systems

Technical limitations of the system can be a significant source of problems for SOTIF. This annex addresses the validation activities for Figure 9 area 3. Concepts for deriving the validation targets are presented.

For SOTIF, validation can consist of testing the vehicle under a wide range of operating conditions. It can be a mixture of SIL, HIL and real-world operation conditions. It may contain some structured testing, dedicated analysis and simulation but the key aspect, especially for area 3, is to have sufficient testing under sufficiently random operating conditions to expose unknown unsafe scenarios.

Typical vehicle software development for SOTIF applicable systems is expected to have a history trajectory of average hours or kilometres per unintended behaviour as schematically shown in Figure C.1. As the software is tested and unintended behaviours are removed, the average kilometres between unintended behaviours is expected to rise. However, as new features/functions are introduced or enabled, the average hours or kilometres per unintended behaviours could drop and then rise as the bugs introduced with the new feature/functions are addressed. Eventually, the validation target threshold is reached for the specified use case and functionality and the validation activity can be considered to be satisfied.




**Key**

| | | | |
|---|---|---|---|
| 1 | new feature/function implemented | Y | average km per unintended behaviour |
| 2 | validation target | a | Feature/function complete |
| X | development time | b | Validation criteria met |

**Figure C.1 — Expected profile of unintended behaviour rate during development**

For example, prior to testing, the item owner specifies the following:

1) Validation target (stopping rule).

2) Weighting between testing modes, real-world tests, HIL, SIL, etc.

© ISO 2019 – All rights reserved


Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27

3) Definition of validation unintended behaviours, criterion for restarting distance counter.

The process of validating SOTIF applicable systems starts with the selection of a validation target (see 6.5). The target can be calculated based on the system use case (e.g. assisted parking, automatic emergency braking, lane keeping, autonomous parallel parking, low speed autonomous car park shuttle, highway autopilot, autonomous taxi), crash statistics for the use case and a safety margin.

EXAMPLE For a particular use case, human drivers experience an average of x kilometres between incidents. For safety reasons an additional margin y is specified. The validation target for the SOTIF applicable system selected is $x \cdot y$ average kilometres between unintended behaviours or a target incident rate of $\lambda = 1/(x \cdot y)$. The stopping rule assumes that the incidents have a Poisson distribution. The system can be shown to have an incident rate greater than or equal to $\lambda$ with a confidence $\alpha$, if there is $\tau$ quantity of driving with no unintended behaviours, where $\tau$ is given in Formula (C.1)[9]:

$$\tau = -\ln(1-\alpha)/\lambda \tag{C.1}$$

NOTE $\tau$ can be in units of time or distance depending on the units of incident rate.

NOTE 2 For $\alpha = 0{,}63$, $\tau = 1/\lambda$.

In practice, $\tau$, the number of validation kilometres or hours to be driven can be quite large and therefore not practical in some cases. The real-world driving requirement can be lessened by using expert knowledge with similar systems and MIL, SIL and HIL simulated kilometres. An acceptable split between real-world and simulated kilometres can be specified. Real-world and simulated validation test conditions are varied as much as possible (e.g. different weather conditions, time of day, road conditions, traffic conditions, pedestrian conditions, etc.) to try and uncover rare operating situations.

Especially for ADAS functions it is also possible to reduce the validation target $x \cdot y$ by considering the exposure to hazardous situations. Depending on the function it is possible to calculate the exposure quantitatively by using data from on-road data collection.

The criteria that characterise unintended behaviour, are specified. Care is taken if one encounters an issue early in testing. In this case, [9] demonstrates that the additional amount of testing might be greater than $\tau$ (i.e. greater than restarting at zero kilometres with the original metric) for the same confidence level.

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27


© ISO 2019 – All rights reserved

# Annex D
(informative)

# Automotive perception systems verification and validation

The verification and validation of automotive perception systems is difficult. This annex describes example practices for the verification and validation of these systems.

Assumption:

— Test drives might not cover every drivable road.

Drivers normally drive a small number of routes repeatedly but in different environmental conditions.

Example considerations for developing perception systems verification test plans (not comprehensive):

1) Continuous data collection, in different markets, weather and illumination conditions. The data represents the real-world user profile (kilometre distribution over different types of roads, weather, illumination, etc.).

2) Specific data collection, in conditions which are normally rare and less represented in normal driving but that might impact perception:

   a) Vision perception — data at dusk or dawn;

   b) Lidar system — adverse weather;

   c) Radar system — rain and splash conditions on salt spread roads;

   d) All systems — entering, exiting or within a tunnel.

3) Specific data collection, in uncommon scenarios that might increase the likelihood of a safety violation:

   a) Driving on roads with sparse traffic and no lead cars can increase the probability of failure of in-path target selection and detection of ghost targets.

   b) Overtaking a line of trucks with long shadows covering the passing lane(s).

   c) Snow sprayed when passing by a snowplough can lead to a sudden blindness of one or more perception systems.

4) Specific data collection, based on system limitations:

   a) Based on radar braking in metal bridges:

      i) Specific data collection in such bridges will be made, including repetitions in different driving condition (host and target cars);

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27

© ISO 2019 – All rights reserved

ii) Test track set-up will be created to emulate the triggering event, and the robustness of the solutions will be tested in this setup.

b) Based on vision system — high beam control function does not turn on in the absence of oncoming traffic:

i) Driving on dark roads with sparse traffic.

5) Various drivers and driving habits need to be taken into account, including the equivalent of "double blind testing" (for example, tell drivers that they need to test the sound system quality in perception test cars).

6) Dedicated testing in extreme conditions:

a) Weather:

i) Winter testing;

ii) Hot test;

b) Infrastructure quality:

i) Dual-lane motorway;

ii) Roads with poor maintenance and poor road markings;

c) Traffic and driving dynamics:

i) Boston vs San Francisco;

ii) Bangkok;

iii) Seoul rush hour;

iv) Naples;

v) New York;

d) Near road clutter:

i) Las Vegas at night produces a large number of light sources as opposed to a normal road scenario;

e) Urban environment:

i) VRU (Vulnerable Road Users) rich environment.

7) Production tolerances testing — it is expected that there will be ranges within mass production, therefore data is collected with variable performance sensing modules:

a) Camera — testing over expected focus range.

b) Radar — testing with different antenna sensitivity.

8) Active systems — testing the interaction between systems:

a) Need to rule out the effect of one perception system affecting other perception systems (as an example radars jamming each other on different cars or on the same car):

i) On a test track.

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27


© ISO 2019 – All rights reserved

ii) In the real world (staged and unstaged testing).

9) Testing on multiple versions:

   a) Different stages of the code expose system behaviour and possible weaknesses.

   b) Derive better robustness from process repetition.

   c) Prevent problems from re-emerging later on.

10) Feature based testing:

   a) Allows large data set analysis based on discovery of hazardous behaviour.

   b) Use of larger feature scope allows mileage multiplication and rare events identification (e.g. using higher Time To Collision for AEB, ignore driver intent in features).

11) Measurement of standalone perception system performance:

   a) Measure the angular separation capabilities (in azimuth and elevation).

   b) Measure the range separation capabilities.

   c) Measure the object measurement accuracy.

There is much benefit in having an ability to incorporate use cases and lessons learned from system generation into new versions and configurations. Having such an ability (for example, knowing that the code will run data also from past configurations) allows some data re-use between development programmes.

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT8IF3EW.2-2022-01-12 18:46:27

© ISO 2019 – All rights reserved

# Annex E
(informative)

# Method for deriving SOTIF misuse scenarios

## E.1 Overview

For systems that are SOTIF relevant, it is important to consider potential reasonably foreseeable misuse when performing the safety analysis. Misuse scenarios can be derived from various sources, such as: lessons learnt, expert knowledge, brainstorming by designers, etc. This annex gives an example methodology for systematically deriving misuse scenarios to support the SOTIF safety analysis. The concept overview of this example methodology is given in Figure E.1 and an example of a misuse scenario is outlined. The approach to the human factors analysis is described in the HFACS document[10].

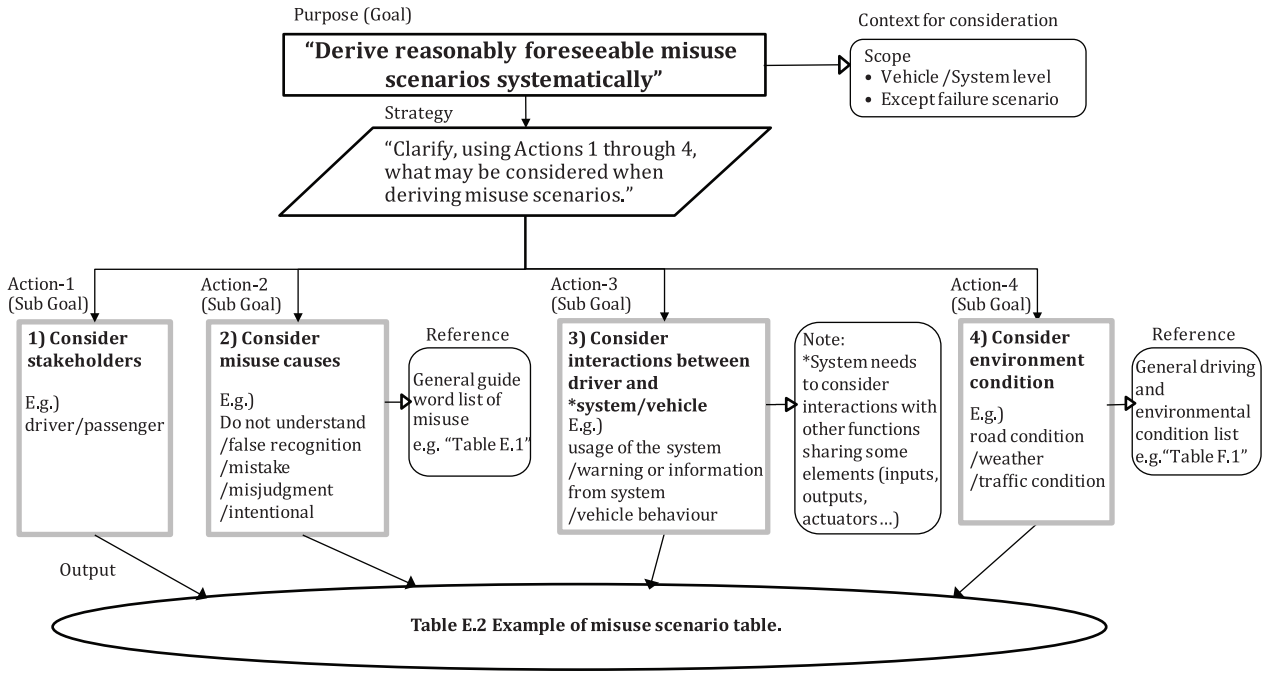



**Figure E.1 — Systematic derivation of SOTIF misuse scenarios.**

Points to consider and an example misuse scenario table are described in E.2.

## E.2 Flow of safety analysis method for misuse

The points that can be considered when deriving the misuse scenarios are described below:

1) Stakeholders

   Consider who performs the misuse that leads to the hazard (e.g. driver, passenger).

2) Misuse causes

   When considering the misuse causes, general "Guide words," derived from the typical human misuse process (Recognition, Judgment, and Action) can be useful.


© ISO 2019 – All rights reserved

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT8IF3EW.2-2022-01-12 18:46:27

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

**Table E.1 — Guide words for human error**

| Process | Guide word | Example |
|---|---|---|
| Recognition | 1) Do not understand | Cannot operate correctly due to complicated usage. |
| | 2) False recognition | Cannot recognize correctly due to overloaded information. |
| Judgment | 3) Judgment error/misjudgment | Misjudgment due to wrong impression or misunderstanding. |
| Action | 4) Slip/Mistake | Mistake due to loss of concentration (distraction, snooze, etc.). |
| | 5) Intentional | Violation of traffic regulations or social rules. |
| | 6) Unable | Hard to operate |

3) Interactions between the driver and system/vehicle

A possible cause of misuse might be miscommunication between the Driver and the System/Vehicle interfaces. (See Figure E.2).

For example, the following interface subjects can be derived:

— System operation by the driver (Usage): Interface “from Driver to System/Vehicle”;

— Warning notification from the system: Interface “from System/Vehicle to Driver”;

— System/vehicle behaviour: Interface “from System/Vehicle to Driver”.

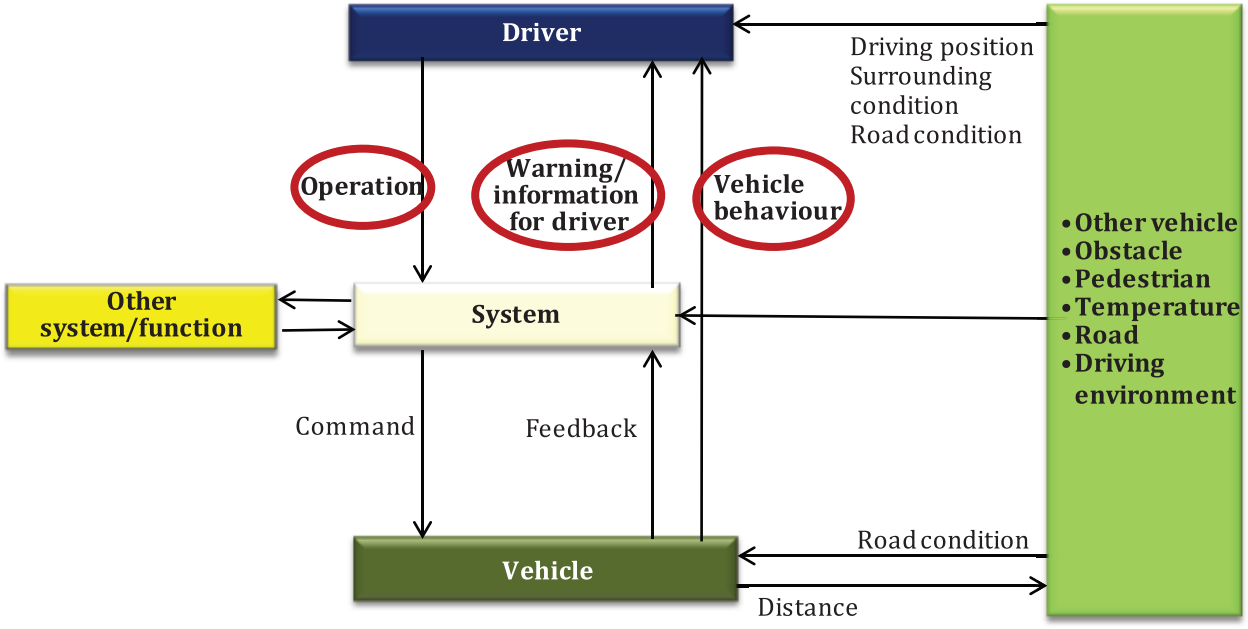



**Figure E.2 — Example of interactions between driver and system/vehicle**

NOTE The boxes and arrows in Figure E.2 have the following meaning:

— Boxes: external factors interacting with the system (possibility);

— Arrow: interaction (possibility).

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27

© ISO 2019 – All rights reserved

4) Consideration of the environment in use case scenarios

The impact of the environment, including road conditions, can be considered when deriving the misuse scenario.

EXAMPLE Some environmental conditions for consideration in use cases scenarios are described in Table F.1.

NOTE Table F.1 can be used both for the performance limit scenario analysis and for misuse scenario analysis.

When the misuse scenario is derived considering points 1) to 4) in Annex E, a scenario table, such as Table E.2, can be used.

**Table E.2 — Example of misuse scenario table based on guide word approach similar to HAZOP**

| Performance limitation scenario | 1) Stakeholders | 2) Misuse causes | | 3) Interactions between driver and system/vehicle | Misuse scenario 4) Consider condition of environment |
|---|---|---|---|---|---|
| | | Process | Guide words | | |
| "While operating autonomously on a highway, the vehicle cannot estimate the location of the lane boundary due to a performance limitation. The vehicle starts to leave the lane and the driver is notified to take control." | Driver … | Recognition | 1) Do not understand | Operation(Usage) | … |
| | | | | Vehicle behaviour | … |
| | | | | Warning/information | "Driver does not take over control of the vehicle and vehicle departs lane because driver does not know meaning of the warning" |
| | | | 2) False recognition | Operation(Usage) | … |
| | | | | Vehicle behaviour | … |
| | | | | Warning/information | … |
| | | Judgment | 3) Judgment error/mis-judgement | … | … |
| | | Action | 4) Slip/ Mistake | … | … |
| | | | 5) Intentional "driver vacated seat" | … | … |
| | | | 6) Unable "Driver not paying attention Driver asleep" | … | … |
| | … | … | | … | … |

NOTE 1 Methods such as HAZOP and STPA analysis can be useful in deriving misuse scenarios. STPA (Systems Theoretic Process Analysis) is a hazard analysis method which considers the hazard factor in interacting function units.

NOTE 2 This Annex E method is not intended to be a comprehensive analysis of all combinations. The methods outlined in Annex E are intended as an example that can be used to initiate the derivation of the analyses required for a specific SOTIF development. Only factors that influence hazardous events are selected for the analysis. Factors that have no influence on hazardous events can be recorded as not applicable.

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27


© ISO 2019 – All rights reserved

# Annex F
(informative)

# Example construction of scenario for SOTIF safety analysis method

This annex gives an example methodology for developing scenario to support the safety analysis of Clause 7.

The following steps are taken to identify and evaluate potential triggering events affecting system performance caused by various conditions, such as: parts characteristics, process, phenomenon, and environment condition.

1) Break down a strategy into three parts: recognition, judgment, and vehicle performance.

2) Construct performance limiting scenarios with influencing factors for each part from triggering condition.

**Table F.1 — Example Scenario of Factors**

| Factor | |
|---|---|
| climate | fine |
| | cloudy |
| | rainy |
| | sleet |
| | snow (accumulation of snow) |
| | hail |
| | fog |
| time of day | early morning |
| | daytime |
| | evening |
| | night time |
| shape of road/lane | straight |
| | curve |
| | downhill |
| | uphill |
| | banked road |
| | step difference |
| | uneven spot(uneven road) |
| | Belgian brick road |
| | narrow road |
| | wide road |
| | existence of median |
| | manhole cover |
| | tollgate |
| | merging |
| | branching |
| | pothole |

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27

© ISO 2019 – All rights reserved

**Table F.1** *(continued)*

| Factor | |
|---|---|
| road condition | dry |
| | wet |
| | low μ path |
| | crossover road |
| | water trough |
| | gravel road |
| ego vehicle operation | vehicle is accelerating |
| | vehicle is decelerating |
| | vehicle is driving at constant speed |
| | vehicle is stopping |
| | drive at high speed |
| | drive at low speed |
| | vehicle is making a turn |
| | vehicle is making a sudden traversing |
| | passing |
| | right or left turn |
| vehicle around<br>— preceding vehicle<br>— to side vehicle<br>— oncoming vehicle<br>including<br>— motorcycle<br>— bicycle | preceding vehicle makes sudden deceleration |
| | preceding vehicle makes deceleration |
| | preceding vehicle makes acceleration |
| | preceding vehicle makes sudden acceleration |
| | interrupting vehicle |
| | trailing vehicle in stop and go traffic |
| | there is vehicle to right of ego vehicle going in same direction |
| | there is vehicle to left of ego vehicle going in same direction |
| | there is an oncoming vehicle |
| | high beam of oncoming vehicle |
| | passing by a motorcycle |
| | bicycle |
| other road participants | pedestrian is walking across |
| | truck |
| | three-wheeled motorcycle |
| | peculiar vehicle |

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.Y0HZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27


© ISO 2019 – All rights reserved

**Table F.1** *(continued)*

| Factor | |
|---|---|
| objects off-roadway (surroundings) | sidewall |
| | sign (upside) |
| | sign (side) |
| | pole |
| | tunnel |
| | multi-story parking space |
| | beneath a viaduct |
| | kerb |
| | guardrail |
| | pylon |
| | pots dots, cats eye |
| | vehicle stopping on the side of the road |
| | animal jumping out |
| | railway crossing |
| | construction site |
| | marked crosswalk |
| | water alongside road |

EXAMPLE Use case construction: climate = rainy, time of day = daytime, shape of road = straight, road conditions = wet, ego vehicle operation = vehicle is stopping, other vehicles = oncoming and on right side, pedestrian = none, objects off-roadway = none.

NOTE Table F.1 is not comprehensive. Other factors can be considered when constructing use cases such as local driving customs and infrastructure.

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27

© ISO 2019 – All rights reserved

# Annex G
(informative)

# Implications for off-line training

Autonomous vehicle technology typically involves some type of machine learning, especially for object detection and classification. Machine learning training has the potential to introduce systematic faults. As this process can be of critical importance to the safe operation of the vehicle, this can lead to the need for the data collection and learning system to be developed according to safety standards, with attention given to reducing hazards such as unintended bias or distortion in the collected data[11].

Off-line training can involve several steps some of which may be considered as tools. ISO 26262-8:2018, Clause 11 deals with the qualification of software tools where an erroneous output of the tool can introduce or fail to detect errors in a safety-related item or element being developed. An argument built around this consideration can be a good basis to justify of tools used to support algorithms which rely on machine learning. However, off-line training can involve several steps and tools and can need additional attention.

An example training process is shown in Figure G.1.

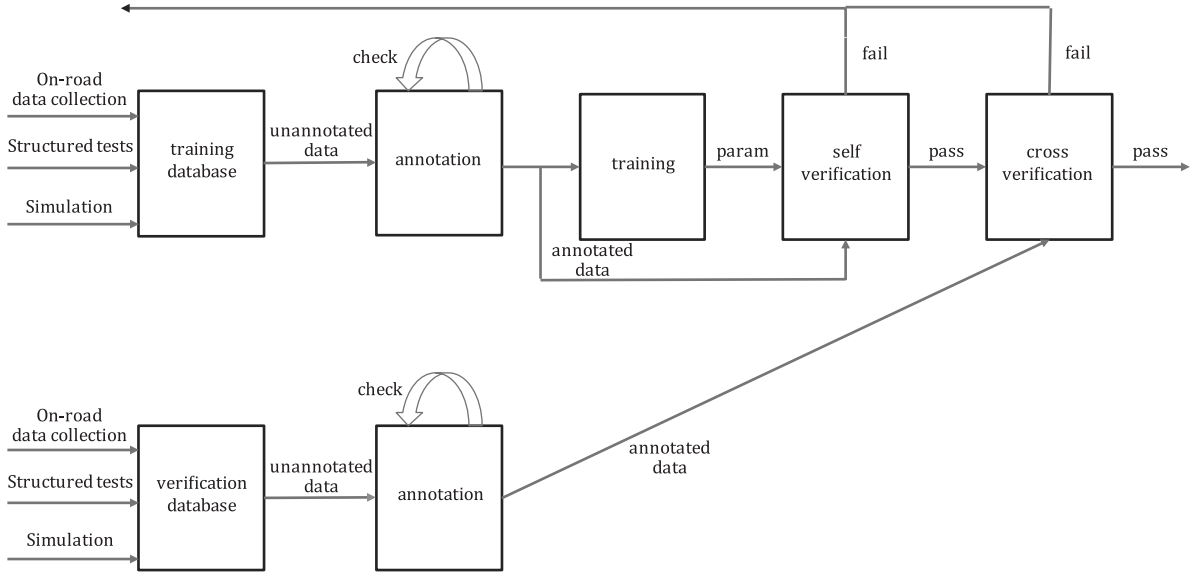



**Figure G.1 — Off-line machine learning process flow**

The top row of Figure G.1, starts with the collection of a training data base that is collected using a mixture of structured testing (e.g. tests designed and implemented on a test track), simulation and on-road random data collection. The data is then annotated for specific features to be learnt (e.g. road boundaries, cars, motorcycles, emergency vehicles). Since annotation is typically a manual process, there can be a check of the annotations; this is represented by the 'circle back' in the figure above.

The annotated data is then used to determine parameters (e.g. neural net weights) via training. The trained system is then verified with the training data using pass/fail criteria, such as acceptable false positive and false negative rates. If the self-verification fails, the process can be restarted after more data is collected and/or training is modified.

Self-verification might be insufficient since it is difficult to ensure that the learning system has trained on the essential characteristics of the training data instead of coincidental correlations[11]. One approach to address this problem is to verify the learning using a separately collected and annotated


© ISO 2019 – All rights reserved

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27

database (bottom row of Figure G.1). The cross-verification step evaluates the performance of the trained system to respond to the data contained in the verification database in a safe manner. Suitable pass-fail criteria are selected before accepting the trained parameters.

Many training limitation issues can be uncovered by verification and validation activities. However, it is recommended that techniques such as a PFMEA (Process Failure Modes and Effects Analysis) can be used to analyse and eliminate possible sources of bias and limitation within the off-line training process. Example issues to be considered include coverage and diversity of:

— Data Collection:
  — Vehicles and drivers;
  — Routes and driving conditions;
  — Structured tests;
— Annotation;
— Annotation Check.

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.Y0HZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27

© ISO 2019 – All rights reserved

# Bibliography


[1] Ulbrich S., Menzel T., Reschka A., Schuldt F., Mauer M. Defining and Substantiating the Terms Scene, Situation, and Scenario for Automated Driving", 2015 IEEE 18th International Conference on Intelligent Transportation Systems (ITSC),

[2] Watzenig D., & Horn M. (editors), "Automated Driving — Safer and More Efficient Future Driving", Springer International, 2017, p. 456. http://rd.springer.com/book/10.1007/978-3-319-31895-0

[3] Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. SAE Recommended Practice J3016:SEPT2016, <http://standards.sae.org/j3016_201609/>

[4] Code of Practice for the design and evaluation of ADAS, EU Project RESPONSE 3"; <http://www.acea.be/uploads/publications/20090831_Code_of_Practice_ADAS.pdf>

[5] Kuhn D.S., Kacker R.N., Lei Y. Combinatorial testing", NIST report, June 25, 2012, https://www.nist.gov/publications/combinatorial-testing

[6] Source: Wikipedia: https://de.wikipedia.org/wiki/Fahrbahnmarkierung#/media/File:Roadworks_Germany_A9_2.jpg

[7] Fabris S., Priddy J., Harris F. "Method for Hazard Severity Assessment for the Case of Unintended Deceleration", presented at 2012 VDA Auto SYS conference in Berlin

[8] Fabris S., Priddy J., Harris F. "Method for hazard severity assessment for the case of undemanded deceleration." Presented at VDA Automotive SYS Conference, Berlin, June 19/20, 2012

[9] Littlewood B., & Wright D. " Some Conservative Stopping Rules for the Operational Testing of Safety-Critical Software", *IEEE Trans. SW Engng.*, **23**(11), 673–683, Nov. 1997

[10] Shappell S.A., & Wiegmann D.A. The Human Factors Analysis and Classification-System — HFACS, February 2000 Final Report. This document is available to the public through the National Technical Information Service, Springfield, Virginia 22161

[11] Koopman P., & Wagner M. Autonomous Vehicle Safety: An Interdisciplinary Challenge," IEEE Intelligent Transportation Systems Magazine, Special Issue on SSIV, 2017, in press Vol. 9 #1, Spring 2017, pp. 90–96

ISO 26262 (all parts), *Road vehicles — Functional safety*


Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27



© ISO 2019 – All rights reserved

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.Y0HZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27

Normen-Download-Beuth-ALTEN GmbH-KdNr.6027897-ID.YOHZNMF15PMNZPPQFT81F3EW.2-2022-01-12 18:46:27

**ICS 43.040.10**

Price based on 54 pages

© ISO 2019 – All rights reserved