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 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

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.

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.

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 ISO 26262 series 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 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.

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/

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.

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

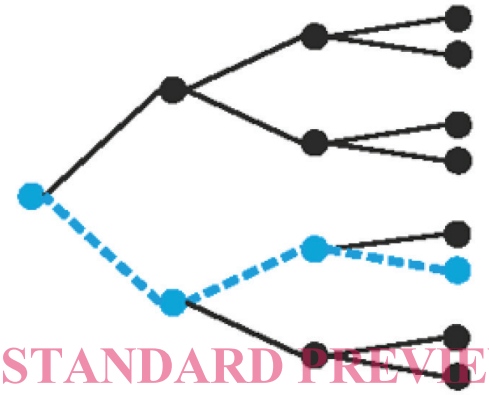


Figure 1 — Scenario (dashed) as a temporal sequence of actions/events (edges) and scenes (nodes)

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].

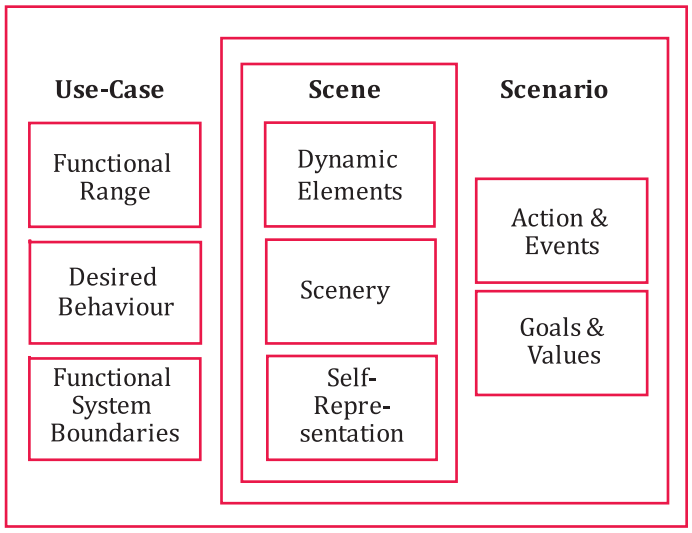


Figure 2 — Taxonomy of use case, scene and scenario

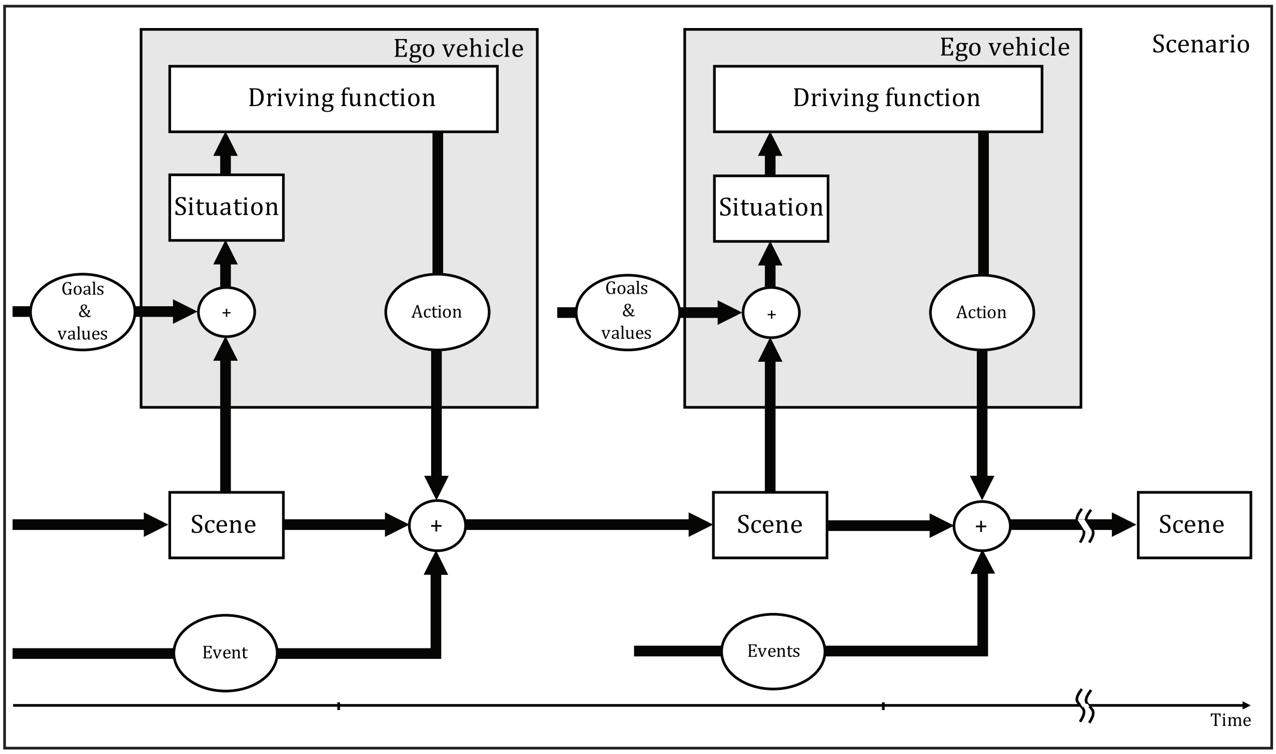


Figure 3 — Temporal view of scenes, events, actions and situations in a scenario

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].

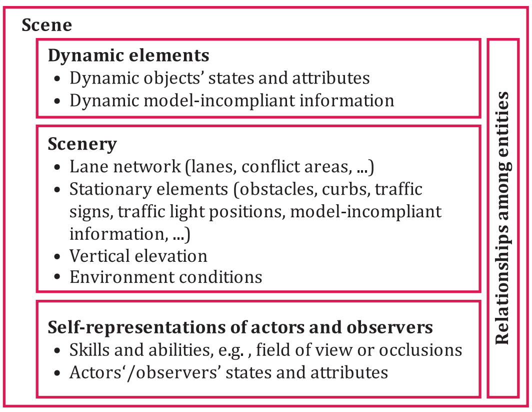


Figure 4 — Characteristics of a scene

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].

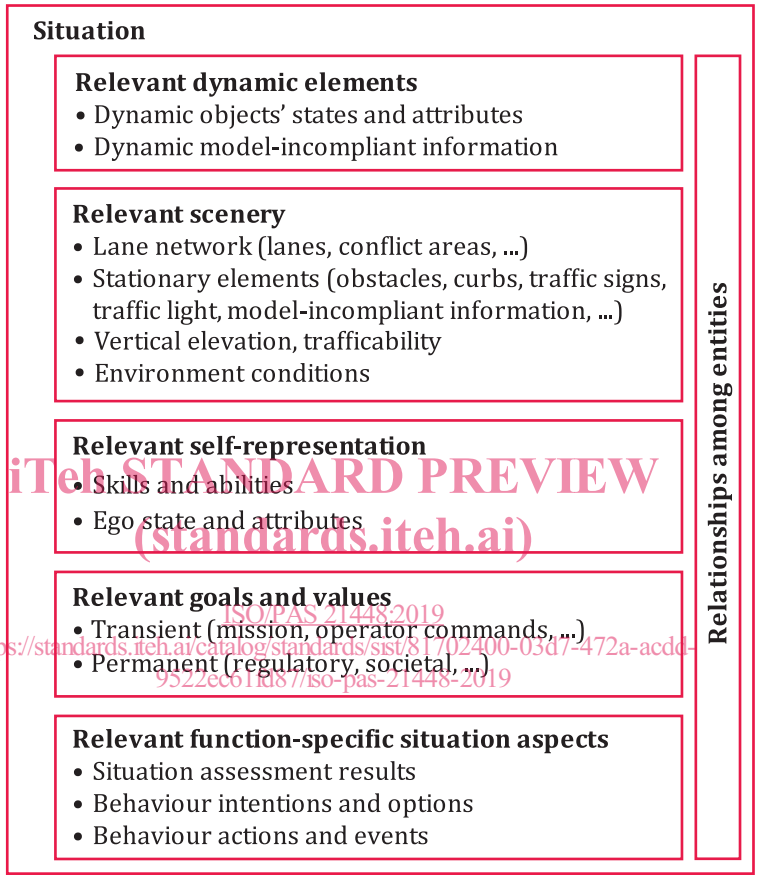


Figure 5 — Characteristics of a situation

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.

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.

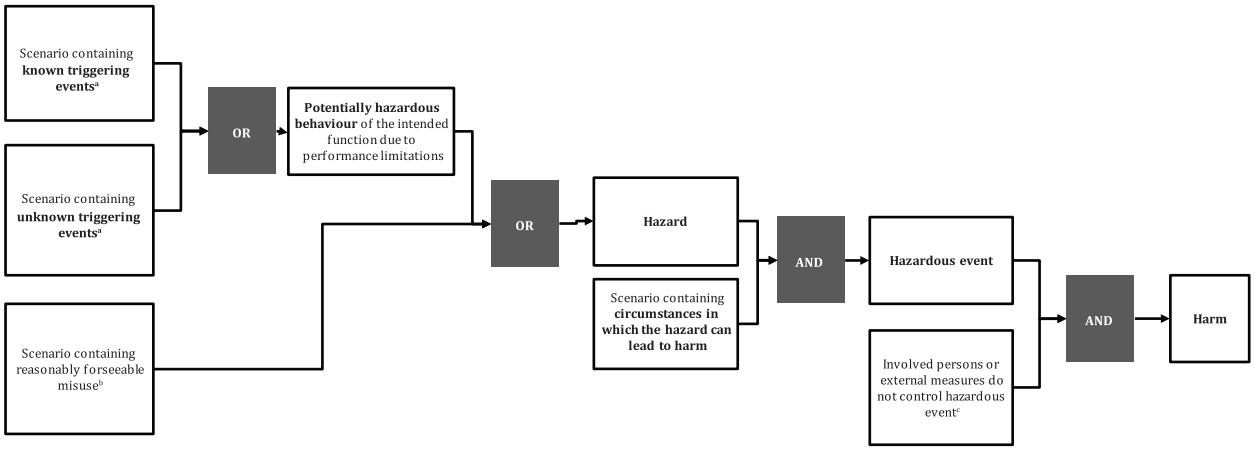
A development interface agreement can be defined between all development parties when applicable for a distributed product development. The goal of an agreement is to confirm in the early stages of a project all responsibilities of the SOTIF activities.

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).



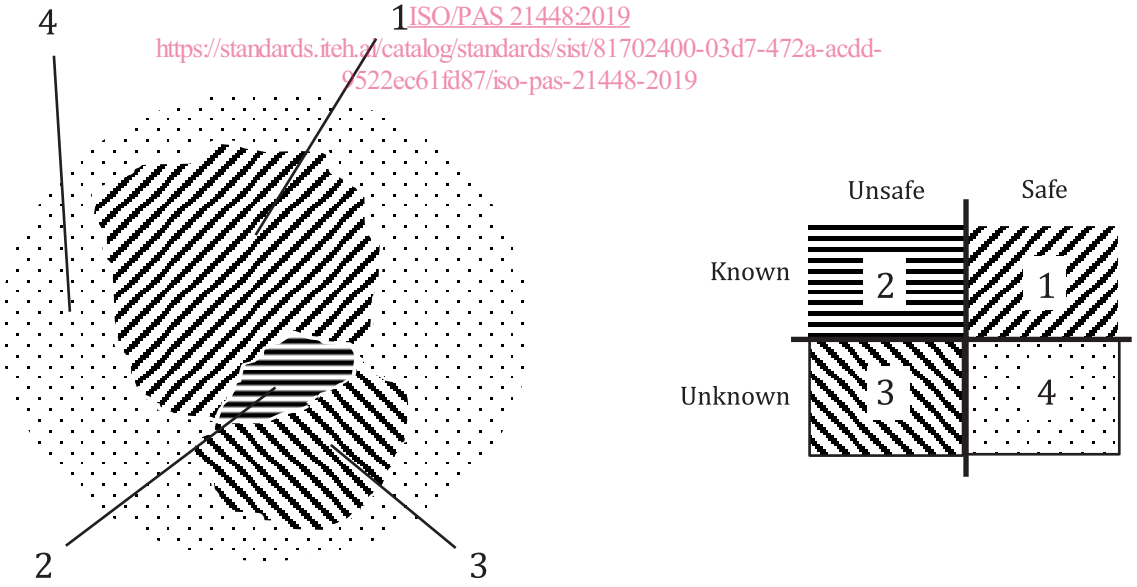
a These scenarios can also be caused by reasonably foreseeable misuse, e.g. activating a functionality intended for the highway in an urban setting causes the vehicle to be in a scenario in which it does not detect a red traffic light.

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