BS ISO 21448:2022

BSI Standards Publication

Road vehicles — Safety of the intended functionality

Documents
Document Sharing Hub

Full document details: BS ISO 21448:2022

National foreword

This British Standard is the UK implementation of ISO 21448:2022. It supersedes PD ISO/PAS 21448:2019, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee AUE/32, Electrical and electronic components and general system aspects (Road vehicles).

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2022
Published by BSI Standards Limited 2022

ISBN 978 0 539 04082 1

ICS 43.040.10

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 July 2022.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO 21448:2022

INTERNATIONAL STANDARD

ISO 21448

First edition
2022-06

Road vehicles — Safety of the intended functionality

Véhicules routiers — Sécurité de la fonction attendue

Reference number
ISO 21448:2022(E)

Documents
Document Sharing Hub

© ISO 2022

Full document details: BS ISO 21448:2022

COPYRIGHT PROTECTED DOCUMENT

© ISO 2022

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
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

© ISO 2022 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO 21448:2022

Contents

Page

Foreword ... **v**

Introduction ... **vi**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **2**

4 Overview and organization of SOTIF activities ... **11**
4.1 General ... 11
4.2 SOTIF principles ... 11
4.2.1 SOTIF-related hazardous event model ... 11
4.2.2 The four scenario areas ... 12
4.2.3 Sense-Plan-Act model ... 15
4.3 Use of this document ... 16
4.3.1 Flow chart and structure of this document ... 16
4.3.2 Normative clauses ... 19
4.3.3 Interpretation of tables ... 19
4.4 Management of SOTIF activities and supporting processes ... 19
4.4.1 Quality management, systems engineering and functional safety ... 19
4.4.2 Distributed SOTIF development activities ... 20
4.4.3 SOTIF-related element out of context ... 20

5 Specification and design ... **21**
5.1 Objectives ... 21
5.2 Specification of the functionality and considerations for the design ... 21
5.3 System design and architecture considerations ... 22
5.4 Performance insufficiencies and countermeasures considerations ... 23
5.5 Work products ... 25

6 Identification and evaluation of hazards ... **25**
6.1 Objectives ... 25
6.2 General ... 26
6.3 Hazard identification ... 26
6.4 Risk evaluation ... 29
6.5 Specification of acceptance criteria for the residual risk ... 30
6.6 Work products ... 31

7 Identification and evaluation of potential functional insufficiencies and potential triggering conditions ... **31**
7.1 Objectives ... 31
7.2 General ... 31
7.3 Analysis of potential functional insufficiencies and triggering conditions ... 32
7.3.1 General ... 32
7.3.2 Potential functional insufficiencies and triggering conditions related to planning algorithms ... 35
7.3.3 Potential functional insufficiencies and triggering conditions related to sensors and actuators ... 35
7.3.4 Analysis of reasonably foreseeable direct or indirect misuse ... 36
7.4 Estimation of the acceptability of the system's response to the triggering conditions ... 37
7.5 Work products ... 38

8 Functional modifications addressing SOTIF-related risks ... **38**
8.1 Objectives ... 38
8.2 General ... 38
8.3 Measures to improve the SOTIF ... 38
8.3.1 Introduction ... 38

AVA Documents
Document Sharing Hub

© ISO 2022 – All rights reserved

Full document details: BS ISO 21448:2022

8.3.2 System modification 39
8.3.3 Functional restrictions 40
8.3.4 Handing over authority 41
8.3.5 Addressing reasonably foreseeable misuse 41
8.3.6 Considerations to support the implementation of SOTIF measures 42
8.4 Updating the input information for "Specification and design" 42
8.5 Work products 42

9 Definition of the verification and validation strategy 42
9.1 Objectives 42
9.2 General 42
9.3 Specification of integration and testing 43
9.4 Work products 45

10 Evaluation of known scenarios 46
10.1 Objectives 46
10.2 General 46
10.3 Sensing verification 46
10.4 Planning algorithm verification 47
10.5 Actuation verification 48
10.6 Integrated system verification 48
10.7 Evaluation of the residual risk due to known hazardous scenarios 49
10.8 Work products 50

11 Evaluation of unknown scenarios 50
11.1 Objectives 50
11.2 General 50
11.3 Evaluation of residual risk due to unknown hazardous scenarios 50
11.4 Work products 52
11.4.1 Validation results for unknown hazardous scenarios fulfilling objective 11.1 52
11.4.2 Evaluation of the residual risk fulfilling objective 11.1 52

12 Evaluation of the achievement of the SOTIF 52
12.1 Objectives 52
12.2 General 53
12.3 Methods and criteria for evaluating the SOTIF 53
12.4 Recommendation for SOTIF release 54
12.5 Work products 54

13 Operation phase activities 55
13.1 Objectives 55
13.2 General 55
13.3 Topics for observation 56
13.4 SOTIF issue evaluation and resolution process 57
13.5 Work products 57

Annex A (informative) **General guidance on SOTIF 58**

Annex B (informative) **Guidance on scenario and system analyses 95**

Annex C (informative) **Guidance on SOTIF verification and validation 125**

Annex D (informative) **Guidance on specific aspects of SOTIF 159**

Bibliography 179

© ISO 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

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*.

This first edition cancels and replaces the first edition of ISO/PAS 21448:2019, which has been technically revised.

The main changes are as follows:

— the scope has been extended to include all levels of driving automation;

— the clauses and annexes have been reworked and expanded for clarification and additional guidance;

— the definitions (Clause 3) have been reworked, in particular to clarify the hazard model; and

— Clause 13 has been added to address the operation phase after the function has been activated for end users.

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.

© ISO 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

Introduction

The safety of road vehicles is a concern of paramount importance for the road vehicle industry. The number of automated driving functionalities included in vehicles is increasing. 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 absence of unreasonable risk caused by every hazard associated with the intended functionality and its implementation, including both hazards due to failures and due to insufficiencies of specification or performance insufficiencies.

For the achievement of functional safety, ISO 26262-1 defines functional safety as the absence of unreasonable risk due to hazards caused by malfunctioning behaviour of the E/E system. ISO 26262-3 describes how to conduct a hazard analysis and risk assessment (HARA) to determine vehicle-level hazards and associated safety goals. 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 E/E systems, e.g. systems which rely on sensing the external or internal vehicle environment to build situational awareness, the intended functionality and its implementation can cause hazardous behaviour, despite these systems being free from the faults addressed in the ISO 26262 series. Example causes of such potentially hazardous behaviour include:

— the inability of the function to correctly perceive the environment;

— the lack of robustness of the function, system, or algorithm with respect to sensor input variations, heuristics used for fusion, or diverse environmental conditions;

— the unexpected behaviour due to decision making algorithm and/or divergent human expectations.

In particular, these factors are relevant to functions, systems or algorithms that use machine learning.

The absence of unreasonable risk resulting from hazardous behaviours related to functional insufficiencies is defined as the safety of the intended functionality (SOTIF). Functional safety (addressed by the ISO 26262 series) and the SOTIF are complementary aspects of safety (see A.2 for a better understanding of the respective scopes of the ISO 26262 series and this document).

To address the SOTIF, measures to eliminate hazards or reduce risks are implemented during the following phases:

— the specification and design phase;

EXAMPLE 1 Modification of vehicle functionality or of sensor performance requirements, driven by identified system insufficiencies or by hazardous scenarios identified during the SOTIF activities.

— the verification and validation phase; and

EXAMPLE 2 Technical reviews, test cases with a high coverage of relevant scenarios, injection of potential triggering conditions, in the loop testing (e.g. SIL: software in the loop / HIL: hardware in the loop / MIL: model in the loop) of selected SOTIF-relevant scenarios.

EXAMPLE 3 Long-term vehicle testing, test-track vehicle testing, simulation testing.

— the operation phase.

EXAMPLE 4 Field monitoring of SOTIF incidents.

These hazards can be triggered by specific conditions of a scenario, defined as triggering conditions, which can include reasonably foreseeable misuse of the intended functionality. Additionally, the interaction with other functions at the vehicle level can lead to hazards (e.g. activation of the parking brake while the automated driving function is active).

© ISO 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

Therefore, a proper understanding by the user of the functionality, its behaviour and its limitations (including the human/machine interface) is essential to ensure safety.

EXAMPLE 5 Lack of driver attention while using a Level 2 automated driving system.

EXAMPLE 6 Mode confusion (e.g. the driver thinks the function is activated when it is deactivated) can directly lead to a hazard.

NOTE 1 Reasonably foreseeable misuse excludes intentional alterations made to the system's operation.

Information provided by the infrastructure (e.g. V2X – Vehicle2Everything communication, maps) is also part of the evaluation of functional insufficiencies if it can have an impact on the SOTIF. See D.4 for guidance on V2X features.

EXAMPLE 7 For automated valet parking systems, the functionalities of route planning and object detection could be achieved jointly by the infrastructure and the vehicle.

NOTE 2 Depending on the application, elements of other technologies can be relevant when evaluating the SOTIF.

EXAMPLE 8 The location and mounting of a sensor on the vehicle can be relevant to avoid noisy sensor output resulting from vibration.

EXAMPLE 9 The windshield optical properties can be relevant when evaluating the SOTIF of a camera sensor.

It is assumed that the random hardware faults and systematic faults (including hardware and software faults) of the E/E system are addressed using the ISO 26262 series.

One could interpret the functional insufficiencies addressed in this document as systematic faults. However, the measures to address these functional insufficiencies are specific to this document and complementary to the ones described in the ISO 26262 series. Specifically, the ISO 26262 series assumes that the intended functionality is safe, and addresses E/E system faults that can cause hazards due to a deviation from the intended functionality. The requirement-elicitation process for the system and its elements can include aspects of both standards.

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

© ISO 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

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

Source of hazard	Cause of hazardous events	Within scope of
System	E/E system faults	ISO 26262 series
	Functional insufficiencies	This document
	Incorrect and inadequate Human-Machine Interface (HMI) design (inappropriate user situational awareness, e.g. user confusion, user overload, user inattentiveness)	This document European Statement of Principles on human-machine interface[1]
	Functional insufficiencies of artificial intelligence-based algorithms	This document
	System technologies EXAMPLE Eye damage from the beam of a lidar.	Specific standards EXAMPLE IEC 60825
External factor	Reasonably foreseeable misuse by the user or by other road participants	This document The ISO 26262 series
	Attack exploiting vehicle security vulnerabilities	ISO/SAE 21434
	Impact from active infrastructure and/or vehicle to vehicle communication, and external systems	This document ISO 20077; ISO 26262 series, IEC 61508 series
	Impact from vehicle surroundings (e.g. other users, passive infrastructure, weather, electromagnetic interference)	This document The ISO 26262 series ISO 7637-2, ISO 7537-3 ISO 11452-2, ISO 11452-4, ISO 10605 and other relevant standards

© ISO 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

Road vehicles — Safety of the intended functionality

1 Scope

This document provides a general argument framework and guidance on measures to ensure the safety of the intended functionality (SOTIF), which is the absence of unreasonable risk due to a hazard caused by functional insufficiencies, i.e.:

a) the insufficiencies of specification of the intended functionality at the vehicle level; or

b) the insufficiencies of specification or performance insufficiencies in the implementation of electric and/or electronic (E/E) elements in the system.

This document provides guidance on the applicable design, verification and validation measures, as well as activities during the operation phase, that are needed to achieve and maintain the SOTIF.

This document is applicable to intended functionalities where proper situational awareness is essential to safety and where such situational awareness is derived from complex sensors and processing algorithms, especially functionalities of emergency intervention systems and systems having levels of driving automation from 1 to 5[2].

This document is applicable to intended functionalities that include one or more E/E systems installed in series production road vehicles, excluding mopeds.

Reasonably foreseeable misuse is in the scope of this document. In addition, operation or assistance of a vehicle by a remote user or communication with a back office that can affect vehicle decision making is in scope of this document when it can lead to safety hazards.

This document does not apply to:

— faults covered by the ISO 26262 series;

— cybersecurity threats;

— hazards directly caused by the system technology (e.g. eye damage from the beam of a lidar);

— hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, release of energy and similar hazards, unless directly caused by the intended functionality of E/E systems; and

— deliberate actions that clearly violate the system's intended use, (which are considered feature abuse).

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 (e.g. dynamic stability control systems, airbags).

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, *Road vehicles — Functional safety — Part 1: Vocabulary*

© ISO 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

3 Terms and definitions

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

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

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

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

3.1
acceptance criterion
criterion representing the absence of an unreasonable level of *risk* (3.23)

Note 1 to entry: The acceptance criterion can be of qualitative as well as quantitative nature, e.g. physical parameters that define when a specific behaviour is considered as hazardous behaviour, maximum number of incidents per hour, as low as reasonably practicable (ALARP).

EXAMPLE 1 From traffic statistics, a reasonable level of risk of one accident per X km is derived.

EXAMPLE 2 The comparison with an equivalent vehicle-level effect that is proven in use to be controllable by the driver can support the definition of an acceptance criterion. For instance, the trajectory perturbation due to an unwanted lane keeping assist function intervention might be compared to a lateral wind gust to define an acceptable level of authority for the function.

3.2
action
single act or behaviour that is executed by any actor in a *scene* (3.27)

Note 1 to entry: The temporal sequence of actions/*events* (3.7) and scenes are parts of the definition of a *scenario* (3.26).

EXAMPLE *Ego vehicle* (3.6) activates the hazard warning lights.

Note 2 to entry: In the context of this definition, an actor can be a person, another object, another system or any element in interaction with the considered function.

3.3
driving policy
strategy and rules defining acceptable *actions* (3.2) at the vehicle level

3.4
dynamic driving task
DDT
real-time operational and tactical functions required to operate a vehicle in traffic

Note 1 to entry: The following functions are part of the DDT:

— lateral vehicle motion control (operational);

— longitudinal vehicle motion control (operational);

— monitoring the driving environment (operational and tactical) and object and *event* (3.7) response execution (operational and tactical), see *object and event detection and response (OEDR)* (3.20);

— manoeuvre planning (tactical); and

— enhancing conspicuity via lighting, signalling or gesturing, etc. (tactical).

Note 2 to entry: The concept was originally defined in SAE J3016[2].

© ISO 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

3.5
DDT fallback
response by the driver or automation system to either perform the *dynamic driving task (DDT)* (3.4) or transition to a *minimal risk condition (MRC)* (3.16) after the occurrence of a failure(s) or detection of a *functional insufficiency* (3.8) or upon detection of a potentially hazardous behaviour

EXAMPLE An *operational design domain (ODD)* (3.21) exit or a sensor blocked by ice can lead to hazardous behaviour which requires a response by the driver.

Note 1 to entry: The concept was originally defined in SAE J3016[2].

3.6
ego vehicle
vehicle fitted with functionality that is being analysed for the *SOTIF* (3.25)

3.7
event
occurrence at a point in time

Note 1 to entry: The temporal sequence of *actions* (3.2)/events and *scenes* (3.27) are parts of the definition of a *scenario* (3.26).

Note 2 to entry: While every action is also an event, not every event is an action, i.e. the set of all actions is a subset of all events.

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

EXAMPLE 2 Traffic light turning green at a given time.

3.8
functional insufficiency
insufficiency of specification (3.12) or *performance insufficiency* (3.22)

Note 1 to entry: Functional insufficiencies include the insufficiencies of specification or performance insufficiencies at the vehicle level or the E/E elements of the system.

Note 2 to entry: The *SOTIF* (3.25) activities include the identification of functional insufficiencies and the evaluation of their effects. Functional insufficiencies lead to hazardous behaviour or inability to prevent or detect and mitigate a reasonably foreseeable *misuse* (3.17) by definition (see 3.12 and 3.22). The term "potential functional insufficiency" can be used when the ability to contribute to hazardous behaviour or inability to prevent or detect and mitigate a reasonably foreseeable misuse is not yet established.

Note 3 to entry: Figures 1 to 3 describe the SOTIF cause and effect model, in which the relation of *triggering conditions* (3.30), functional insufficiencies, output insufficiencies, hazardous behaviour, inability to prevent or detect and mitigate a reasonably foreseeable indirect misuse, *hazard* (3.11), hazardous *event* (3.7) and harm is described.

Note 4 to entry: In the case of indirect misuse contributing to the occurrence of harm, two functional insufficiencies are typically involved. One is the functional insufficiency leading to the hazardous behaviour of the system in combination with triggering conditions, the other is the functional insufficiency leading to the inability to prevent or detect and mitigate the reasonably foreseeable indirect misuse. See Figures 1, 2 and 3.

EXAMPLE A vehicle is equipped with a Level 2 highway driving assist functionality. A driver monitoring camera to detect the inattentiveness of the driver is part of the system. For sake of simplicity let us assume that the following statements are true:

— the sense element has a functional insufficiency that, if activated by the triggering condition 1, leads to the hazardous behaviour – execution of an incorrect vehicle trajectory; and

— the driving monitoring camera has a functional insufficiency that, if activated by the triggering condition 2, leads to the inability of the system to detect and mitigate a reasonably foreseeable indirect misuse.

For the harm to occur the *scenario* (3.26) needs to contain the following:

© ISO 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

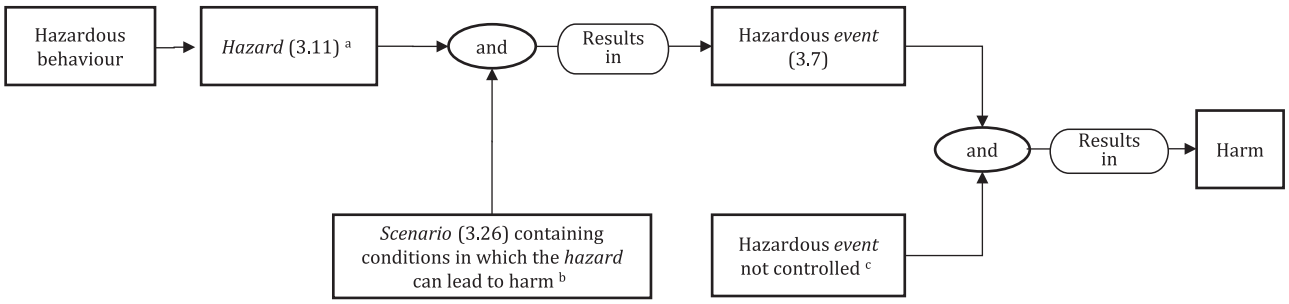
— presence of an indirect misuse by the driver: driver is inattentive and does not detect the hazardous behaviour of the system in time to be able to control it;

— presence of triggering condition 2 leading to the inability of the system to detect and mitigate the present reasonably foreseeable indirect misuse in time; and

— presence of triggering condition 1 leading to the hazardous behaviour of the system.

Note 5 to entry: If a functional insufficiency at the vehicle level is activated by a triggering condition, it results in either a hazardous behaviour or an inability to prevent or detect and mitigate a reasonably foreseeable indirect misuse. See Figure 3 (A).

Note 6 to entry: If a functional insufficiency on element level is activated by a triggering condition, it results in what is referred to as an output insufficiency. See Figure 3 (B). An output insufficiency, either by itself or in combination with one or more output insufficiencies of other elements, contributes to either a hazardous behaviour at the vehicle level or an inability to prevent or detect and mitigate a reasonably foreseeable indirect misuse. See Figure 3 (B).



Key

a The hazard is the potential source of the harm, caused by a hazardous behaviour at the vehicle level.

b The scenario containing conditions in which the hazard can lead to harm is a contributing factor to the occurrence of harm, but not its source.

c The inability to gain sufficient control of the hazardous event is a contributing factor to the occurrence of harm, but not its source.

Figure 1 — Correlation between hazard and occurrence of harm

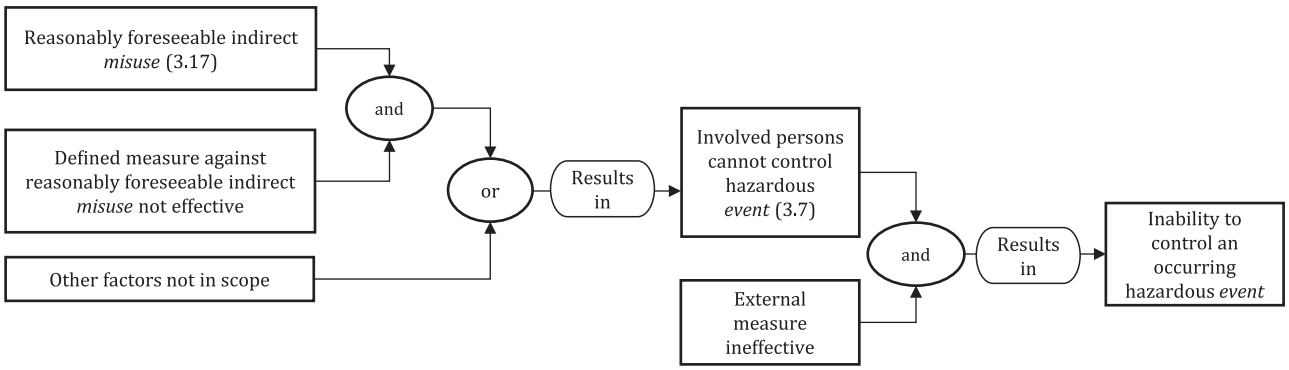
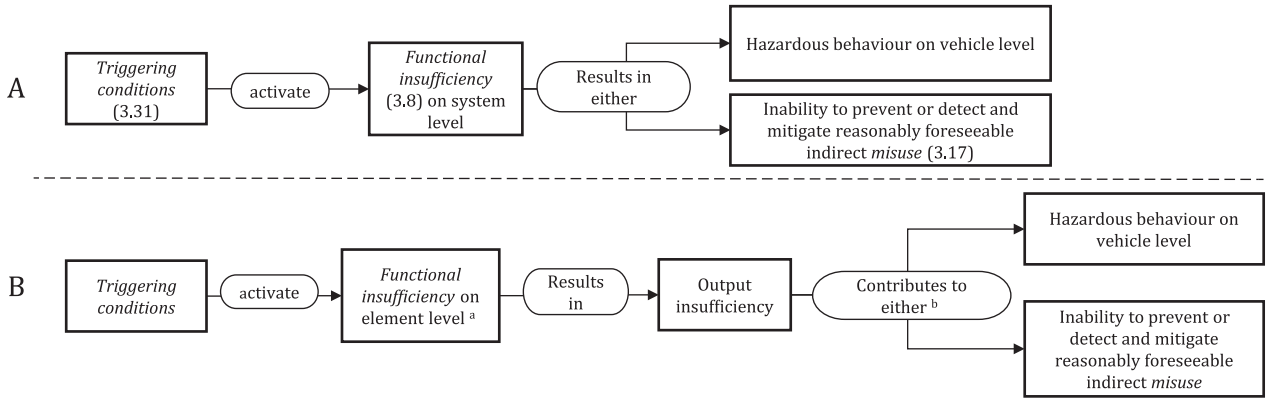


Figure 2 — Reasons for the hazardous event not being controlled

© ISO 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022



Key

a Depending on the architecture of the system this functional insufficiency on an element level can be recognized either as a *single-point functional insufficiency* (3.28) or *a multiple point functional insufficiency* (3.19).

b An output insufficiency, either by itself or in combination with one or more output insufficiencies of other elements, contributes to either a hazardous behaviour at the vehicle level or an inability to prevent or detect and mitigate a reasonably foreseeable indirect misuse.

Figure 3 — The SOTIF cause and effect model

3.9
functional modification
alteration of a functional specification

Note 1 to entry: Functional modification is not the same as the term “modification” defined in ISO 26262-1:2018. The "functional modification" of this document would be referred to as "change" in ISO 26262 terms.

3.10
fallback-ready user
user who is able to operate the vehicle and is capable of intervening to perform the *DDT fallback* (3.5) as required and within a time span appropriate for the defined non-driving occupation

Note 1 to entry: The concept was originally defined in SAE J3016[2].

3.11
hazard
potential source of harm caused by the hazardous behaviour at the vehicle level

[SOURCE: ISO 26262-1:2018, 3.75, modified — The word "malfunctioning" has been replaced by "hazardous", the phrase "of the item" has been replaced by "at the vehicle level" and the Note 1 to entry has been removed.]

3.12
insufficiency of specification
specification, possibly incomplete, contributing to either a hazardous behaviour or an inability to prevent or detect and mitigate a reasonably foreseeable indirect *misuse* (3.17) when activated by one or more *triggering conditions* (3.30)

EXAMPLE 1 An incomplete specification of the adaptive cruise control headway distance results in the *ego vehicle* (3.6) not keeping a safe distance to the vehicle in front.

EXAMPLE 2 System inability to handle uncommon road signs due to specification gaps, i.e. the uncommon road sign is not part of the specification and thus the system cannot process it appropriately.

Note 1 to entry: Insufficiency of specification can be either known or unknown at a given point in the system lifecycle.

© ISO 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

Note 2 to entry: The *SOTIF* (3.25) activities include the identification of insufficiencies of specification and the evaluation of their effects. The term "potential insufficiency of specification" can be used when the ability to contribute to hazardous behaviour or inability to prevent or detect and mitigate a reasonably foreseeable misuse is not yet established.

Note 3 to entry: Requirements derived from the specification, from the assumptions of other systems or elements, or from systematic analyses (such as those included in Clause 6 or other analyses that elicit design and implementation requirements for the SOTIF) can be included in formal databases to support assurance of verification. These requirements might not be designated as the "specification" in many organizations but are necessary to ensure the SOTIF. The usage of the term "insufficiency (insufficiencies) of specification" in this document includes insufficiencies in such derived requirements.

3.13
intended behaviour
behaviour of the *intended functionality* (3.14)

Note 1 to entry: The intended behaviour is that which the developer considers to be the nominal functionality considering capability limitations due to inherent characteristics of the components and technology used.

Note 2 to entry: The intended behaviour specified by the developer, while not representing *unreasonable risk* (3.31), might not match the driver's expectation of the system behaviour.

3.14
intended functionality
specified functionality

Note 1 to entry: Intended functionality is defined at the vehicle level.

3.15
levels of driving automation
mutually exclusive set of driving automation levels, ranging from Level 0 (no automation) to Level 5 (full automation), defining the roles of the driver or user and automation system in relation to each other

Note 1 to entry: See Table 2.

Note 2 to entry: The concept was originally defined in SAE J3016[2].

Table 2 — Levels of driving automation

		DDT (3.4)			
Level	Name	Lateral and longitudinal vehicle motion control	*OEDR* (3.20)	*DDT fallback* (3.5)	*ODD* (3.21)
0	No driving automation	Driver	Driver	Driver	Not applicable
1	Driver assistance	Driver and system	Driver	Driver	Limited
2	Partial driving automation	System	Driver	Driver	Limited
3	Conditional driving automation	System	System	*Fallback-ready user* (3.10)	Limited
4	High driving automation	System	System	System	Limited
5	Full driving automation	System	System	System	Unlimited

3.16
minimal risk condition
MRC
vehicle state in order to reduce the *risk* (3.23), when a given trip cannot be completed

Note 1 to entry: This is one expected outcome of a *DDT fallback* (3.5).

Note 2 to entry: The functional safety analogue of the ISO 26262 series would be the safe state.

© ISO 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

Note 3 to entry: The concept was originally defined in SAE J3016[2].

3.17
misuse
usage in a way not intended by the manufacturer or the service provider

Note 1 to entry: Misuse includes human behaviour that is not intended but does not include deliberate system alterations or use of the system with the intention to cause harm.

Note 2 to entry: Misuse can result from overconfidence in the performance of the system.

Note 3 to entry: Depending on the causal relationship to the hazardous behaviour, there are two kinds of misuse, direct and indirect.

Note 4 to entry: Direct misuse, which could be a cause for the occurrence of a hazardous behaviour of the system, is considered to be a potential *triggering condition* (3.30). If its ability to contribute to the occurrence of a hazardous behaviour is established, then it is considered to be a triggering condition. It is also possible that the direct misuse is part of a triggering condition, i.e. next to the direct misuse additional specific conditions of a scenario need to be present for the hazardous behaviour of the system to occur.

EXAMPLE 1 Direct misuse: activating a functionality intended for the highway in an urban setting results a *scenario* (3.26) in which the vehicle does not detect and react to a STOP sign.

EXAMPLE 2 Direct misuse: driver activates automated system when outside the *operational design domain (ODD)* (3.21) specified in the user manual. This is considered direct misuse independent of whether the system includes an *ego vehicle* (3.6) localization component that prevents activation outside the specified ODD.

Note 5 to entry: Indirect misuse leads to a reduced controllability of the hazardous behaviour, to a potentially increased severity of an occurring accident, or a combination of both. It is not considered to be a potential triggering condition since it cannot contribute to the hazardous behaviour of the system itself.

EXAMPLE 3 Indirect misuse: a hands-free Level 2 highway assistant with known perception issues, requires the driver to continuously monitor the correct execution of the *dynamic driving task (DDT)* (3.4) by the system and intervene if necessary. Indirect misuse is the driver falling asleep and not monitoring. This is considered indirect misuse independent of whether or not the situation is detected and mitigated by a driver monitoring system.

EXAMPLE 4 Indirect misuse: passenger unbuckling the seat belt while ego vehicle is in motion and driving autonomously. This is indirect misuse due to the potential to increase the severity of an accident while not being a triggering condition.

Note 6 to entry: Refer to Figures 1 to 3.

3.18
misuse scenario
scenario (3.26) in which *misuse* (3.17) occurs

3.19
multiple-point functional insufficiency
functional insufficiency (3.8) of an element leading to hazardous behaviour or inability to prevent or detect and mitigate a reasonably foreseeable indirect *misuse* (3.17) only in conjunction with functional insufficiencies of other elements when activated by one or more *triggering conditions* (3.30)

3.20
object and event detection and response
OEDR
tasks of the *dynamic driving task (DDT)* (3.4) that include monitoring the driving environment and executing an appropriate response to objects and *events* (3.7) to complete the DDT and/or the *DDT fallback* (3.5)

[SOURCE: SAE J3016:2021, 3.19[2], modified — The phrase "(detecting, recognizing, and classifying objects and events and preparing to respond as needed)" located after "environment" was removed.]

© ISO 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

3.21
operational design domain
ODD
specific conditions under which a given driving automation system is designed to function

Note 1 to entry: Conditions can be spatial, temporal, intrinsic or environmental.

Note 2 to entry: The term "designed" is taken from the definition in SAE J3016[2]. In this document it means "specified".

Note 3 to entry: The conditions of automated driving system itself (e.g. the vehicle speed, computing capabilities, and perception sensing capabilities) are also in the scope of ODD.

Note 4 to entry: The concept was originally defined in SAE J3016[2].

3.22
performance insufficiency
limitation of the technical capability contributing to a hazardous behaviour or inability to prevent or detect and mitigate reasonably foreseeable indirect *misuse* (3.17) when activated by one or more *triggering conditions* (3.30)

Note 1 to entry: Performance insufficiencies can be either known or unknown at a given point in the system lifecycle.

Note 2 to entry: Performance insufficiencies are considered for E/E elements of the system and elements of other technologies considered relevant to the achievement of the *SOTIF* (3.25) (see Note 1 to entry of 3.8).

Note 3 to entry: The SOTIF activities include the identification of performance insufficiencies and the evaluation of their effects. The term "potential performance insufficiency" can be used when the ability to contribute to hazardous behaviour or inability to prevent or detect and mitigate a reasonably foreseeable misuse is not yet established.

EXAMPLE Limitation of technical capabilities are limited calculation performance, limited perception range of a sensor, limited actuation, etc.

3.23
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO 26262-1:2018, 3.128]

3.24
reaction
response to an *action* (3.2) by any actor in a *scene* (3.27)

3.25
safety of the intended functionality
SOTIF
absence of *unreasonable risk* (3.31) due to *hazards* (3.11) resulting from *functional insufficiencies* (3.8) of the *intended functionality* (3.14) or its implementation

Note 1 to entry: A hazardous behaviour of the system that could lead to a *hazard* (see Figure 1) is initiated by a *triggering condition* (3.30) of a *scenario* (3.26). Reasonably foreseeable direct *misuse* (3.17) is considered as a potential triggering condition.

Note 2 to entry: When identifying the hazardous *events* (3.7), intended use and reasonably foreseeable indirect misuse are also considered in combination with hazardous behaviour resulting from *insufficiencies of specification* (3.12) or *performance insufficiencies* (3.22).

© ISO 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

3.26
scenario
description of the temporal relationship between several *scenes* (3.27) in a sequence of scenes, with goals and values within a specified situation, influenced by *actions* (3.2) and *events* (3.7)

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

Note 2 to entry: This definition is adapted from Reference [3].

Note 3 to entry: The referenced "goals and values" are conditional parameters of the *intended functionality* (3.14). A goal could be "staying between the lane markings". A value could be to "prioritize safety of pedestrians over avoiding monetary damage".

3.27
scene
snapshot of the environment including the scenery, dynamic elements, and all actors' and observers' self-representations, and the relationships among those entities

Note 1 to entry: A scene can include environmental elements (state, time, weather, lighting and other surrounding conditions), road infrastructure or internal elements (road or interior geometry, topology, quality, traffic signs, barriers, etc.) and objects/actors (static, dynamic, movable, interactions, manoeuvres if applicable).

Note 2 to entry: An all-encompassing scene (i.e. an objective scene or ground truth) incorporating all entities (e.g. scenery, dynamic elements, actors) can only be modelled in simulation. In the real-world, scenes are perceived by sensors. The scene perceived by the *ego vehicle* (3.6) or human driver is an incomplete, inaccurate, uncertain and potentially erroneous projection of ground truth.

Note 3 to entry: The scene can also include aspects of the ego vehicle and the system implementing the *intended functionality* (3.14), like tyre pressure, user occupation and the presence of failures of parts of the system.

Note 4 to entry: This definition is adapted from Reference [3].

3.28
single-point functional insufficiency
functional insufficiency (3.8) of an element leading directly to hazardous behaviour or the inability to prevent or detect and mitigate a reasonably foreseeable *misuse* (3.17) when activated by one or more *triggering conditions* (3.30)

3.29
situational awareness
understanding of the situation

3.30
triggering condition
specific condition of a *scenario* (3.26) that serves as an initiator for a subsequent system reaction contributing to either a hazardous behaviour or an inability to prevent or detect and mitigate a reasonably foreseeable indirect *misuse* (3.17)

Note 1 to entry: The concept of "triggering" includes the possibility that there can be multiple conditions that can gradually happen, leading to hazardous behaviour or the inability to prevent or detect and mitigate a reasonably foreseeable misuse.

Note 2 to entry: A triggering condition of a *scenario* (3.26) activates a *functional insufficiency* (3.8), resulting in the subsequent system reaction. See Figures 1 to 3.

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. In this example, the triggering condition is the circumstance which leads to the misidentification of the road sign while operating on a highway, whereas AEB has the relevant *performance insufficiency* (3.22) (e.g. low accuracy of perception or misclassification by algorithm).

© ISO 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

Note 3 to entry: The *SOTIF* (3.25) activities include the identification of triggering conditions and the evaluation of the response of the system. The term "potential triggering condition" can be used when the ability to initiate a corresponding reaction is not yet established.

Note 4 to entry: Reasonably foreseeable direct misuse, which could directly initiate a hazardous behaviour of the system, is considered as a potential triggering condition.

Note 5 to entry: Refer to Figures 1 to 3.

3.31
unreasonable risk
risk (3.23) judged to be unacceptable in a certain context according to valid societal moral concepts

[SOURCE: ISO 26262-1:2018, 3.176]

3.32
use case
description of a suite of related *scenarios* (3.26)

Note 1 to entry: A use case can include the following information about the system:

— one or several scenarios;

— the functional range (e.g. maximum allowed speed, maximum allowed deceleration);

— the desired behaviour;

— the system boundaries; and

— assumptions on the environment and human operation.

Note 2 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.

Note 3 to entry: This definition is adapted from Reference [3].

3.33
validation target
value to argue that the *acceptance criterion* (3.1) is met

Note 1 to entry: The definition of a validation target depends on target markets and operational scenarios.

Note 2 to entry: In the context of the *SOTIF* (3.25), validation is the assurance, based on examination and tests, that the acceptance criteria (of the identified hazards) will be achieved with a sufficient level of confidence.

EXAMPLE No hazardous behaviour of the functionality during a Y hour endurance run, or one hazardous behaviour with a certain severity during X times parking

Note 3 to entry: For the complete fulfilment of a given acceptance criterion, the fulfilment of more than one validation target can be necessary.

3.34
vehicle-level SOTIF strategy
VLSS
set of vehicle-level requirements for the *intended functionality* (3.14) used to support design, verification and validation activities to achieve the *SOTIF* (3.25)

Note 1 to entry: A VLSS can be defined for each SOTIF-related system.

© ISO 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

4 Overview and organization of SOTIF activities

4.1 General

Clause 4 provides:

a) an overview of the SOTIF principles;

b) guidance on the workflow of SOTIF activities and use of this document; and

c) guidance on the management of SOTIF activities and supporting processes.

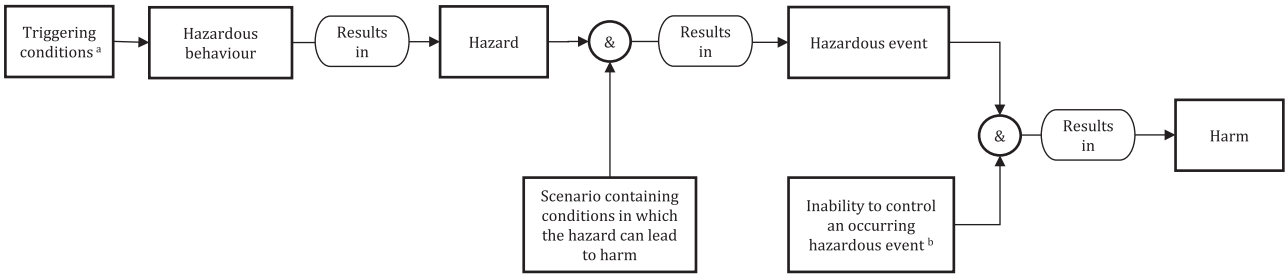
The activities specified in this document are applicable to the vehicle, system and component levels.

4.2 SOTIF principles

4.2.1 SOTIF-related hazardous event model

The main objective of this document is to describe the activities and rationale used to ensure that the risk level associated with all identified SOTIF-related hazardous events is sufficiently low.

The function, system specification and design include relevant use cases which, in turn, comprises several scenarios. These scenarios could contain triggering conditions that lead to harm (for a simplified version see Figure 4, for a more detailed version see Figures 1 to 3). In order to avoid the harm, proper situational awareness is necessary.



Key

a Triggering conditions include reasonably foreseeable direct misuse.

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

Figure 4 — Visualisation of a SOTIF-related hazardous event model

EXAMPLE 1 When activated in an urban setting, a functionality intended for only highway use has limitations in recognizing and interpreting the motion of vulnerable road users.

EXAMPLE 2 Incorrect understanding of the system operating mode by the driver who assumes that the system is active even though it is deactivated. In such a situation, the potential insufficiencies of the system HMI to prevent this confusion or the absence of an appropriate system reaction (if the driver behaviour can be monitored) can also be considered as a hazardous behaviour of the system.

NOTE 1 Proper situational awareness relies on:

— Sufficiently comprehensive and accurate perception of the relevant environmental conditions, a correct understanding of the scene (e.g. detecting a relevant stop sign) and a forecast model regarding the state of each road actor (e.g. heading direction, speed). Situational awareness can be further supported by information such as localization, ego-motion, or communication with other vehicles or the environment;

— appropriate actions or reactions when driving (e.g. obey rules associated with stop signs).

Over the vehicle operational life, the following can vary:

© ISO 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

— the environment (e.g. new type of traffic signs, road markings, vehicles);

— appropriate reactions (e.g. new driving action required by a new traffic sign; changes in driving scenarios, changes in driving laws).

NOTE 2 The monitoring of such changes is addressed in Clause 13 of this document.

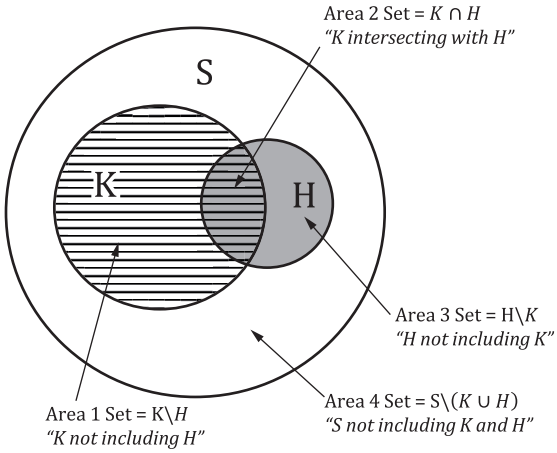
NOTE 3 This concern could be covered by requirements derived for the driving policy. An example of this is in D.1.

Such considerations are taken into account when specifying the operational design domain (ODD) and during system development (risk identification, definition of appropriate measures) to ensure the SOTIF during operation.

4.2.2 The four scenario areas

Within this document, the hazardous scenarios are scenarios causing hazardous behaviour. The scenarios which are part of the relevant use cases are classified into four areas (see Figures 5 and 6).

© ISO 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022



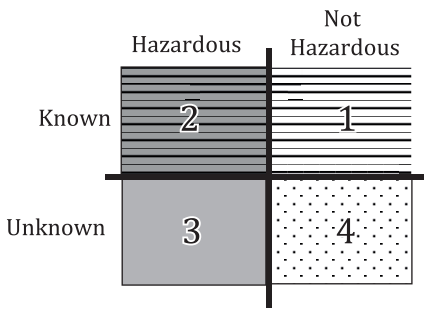
Key

represents the set of known scenarios K

represents the set of all possible scenarios S

represents the set of hazardous scenarios H

Figure 5 — Visualisation of scenario categories



Key

known, not hazardous scenarios (area 1)

known, hazardous scenarios (area 2)

unknown, hazardous scenarios (area 3)

unknown, not hazardous scenarios (area 4)

Figure 6 — Alternative visualisation of scenario categories

Areas 1, 2, 3 and 4 are defined to structure and guide the understanding of this document as follows:

— known not hazardous scenarios (area 1);

— known hazardous scenarios (area 2);

— unknown hazardous scenarios (area 3); and

— unknown not hazardous scenarios (area 4).

EXAMPLE Unknown areas are related to the scenarios when:

© ISO 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

— the potential triggering conditions have been identified (e.g. extreme low temperature, special combination of driving scenarios), however, the behaviour of the system is unknown;

— there are unknown triggering conditions (e.g. “black swan” events); or

— known parameters of scenarios can combine into unknown potential triggering conditions (e.g. combination of weather and traffic conditions).

NOTE 1 Scenarios in area 4 that are unknown but not hazardous do not impose risk of harm. Once a scenario in area 4 is discovered (i.e. becomes known), it is moved to area 1.

This model is a conceptual abstraction representing a goal of the SOTIF activities, which is to:

— perform a risk acceptance evaluation of area 2 based on the analysis of the intended functionality;

— reduce the probability of known hazardous scenarios causing hazardous behaviour, in area 2, to an acceptable level through functional modification (see Clause 8);

— reduce the probability of the unknown scenarios causing potentially hazardous behaviour, in area 3, to an acceptable criterion through an adequate verification and validation strategy (see Clauses 9 and 11).

NOTE 2 This is just a conceptual approach of one aspect of the task since the sizes of the areas are not measurable.

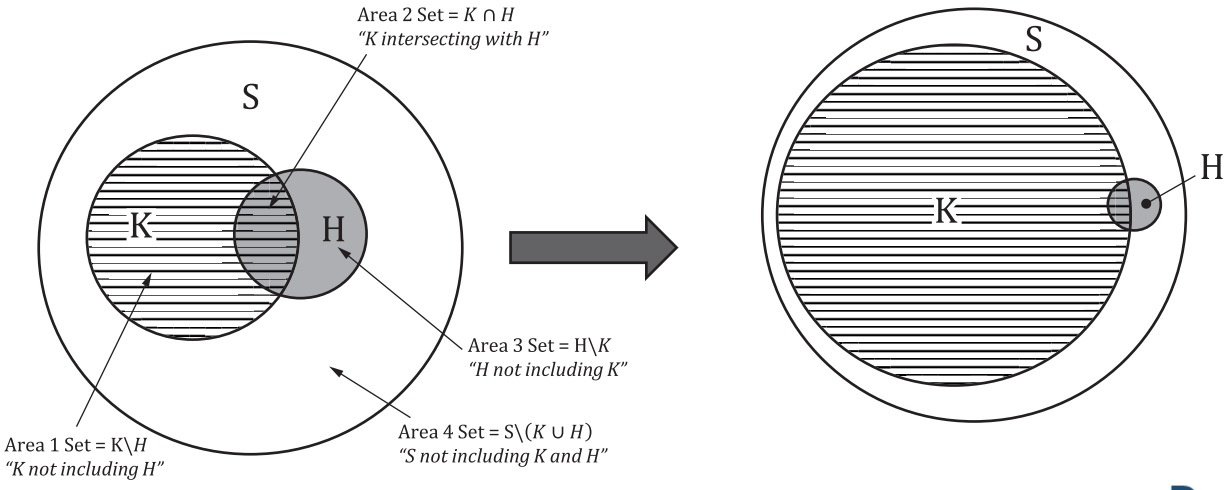
NOTE 3 The size of the areas represents the number of scenarios, not the risk due to these scenarios. However, this is just a conceptual approach of one aspect of the task since the sizes of the areas are not really measurable. The SOTIF task is to provide an argument for a sufficiently low risk of the intended functionality, for which the number of scenarios is one aspect, but not the only one. Severity of the resulting harm and likelihood of occurrence of a hazardous scenario contribute to the risk of the intended functionality but are not represented in the areas.

NOTE 4 If the usage of scenarios for certain SOTIF-related activities is not planned in the applied system development approach, this does not change the goal of SOTIF to avoid unreasonable risk.

A given use case can include known and unknown scenarios. Exploring scenarios of each use case can lead to the identification of previously unknown scenarios.

The ultimate goal of the SOTIF activities is to evaluate the potentially hazardous behaviour present in areas 2 and 3 and to provide an argument that the residual risk caused by these scenarios is sufficiently low, i.e. at or below the acceptance criteria. While the risk resulting from known scenarios in area 2 is explicitly evaluated, the risk resulting from unknown scenarios in area 3 is argued to be sufficiently small by statistics-based testing.

It is expected that the residual risk due to areas 2 and 3 will be reduced. The confidence in the achievement of the SOTIF will be increased by the growing scenario set in area 1 (see Figures 7 and 8).



© ISO 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

Example of an initial starting point of development

Goal for the SOTIF release

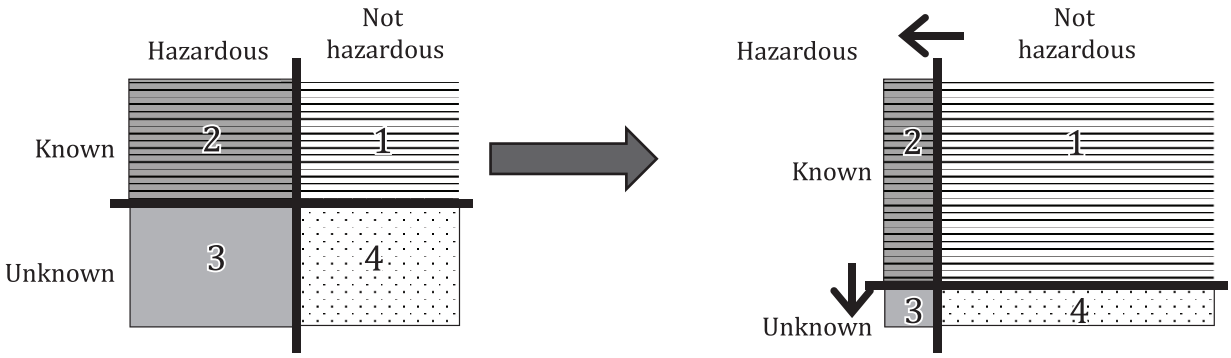
Key

represents the set of know scenarios K

represents the set of all possible scenarios S

represents the set of hazardous scenarios H

Figure 7 — Evolution of the scenario categories resulting from the ISO 21448 activities



Example of an initial starting point of development

Goal for the SOTIF release

Key

known, not hazardous scenarios (area 1)

known, hazardous scenarios (area 2)

unknown, hazardous scenarios (area 3)

unknown, not hazardous scenarios (area 4)

Figure 8 — Alternative evolution of the scenario categories resulting from the ISO 21448 activities

4.2.3 Sense-Plan-Act model

Possible causes of hazardous behaviour considered in this document are closely related to the ability of the system to create a sufficiently accurate environmental model, make the right decisions and derive the correct control actions based on the environmental model and execute the control actions.

The key system elements and their interactions are represented by the "Sense-Plan-Act" model (see Figure 9). The element “Sense” executes the perception part (including localization), i.e. the creation of an environmental model based on the information received from sensing both the vehicle's external and internal environment as well as the vehicle and system states. The element “Plan” applies its goals and policies on the environmental model provided by the Sense element to derive the control actions. Finally, the element “Act” executes the control actions.

NOTE Decision algorithms are included in all elements of the Sense-Plan-Act model (e.g. classification, sensor data, fusion, situation analysis, action decision).

© ISO 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

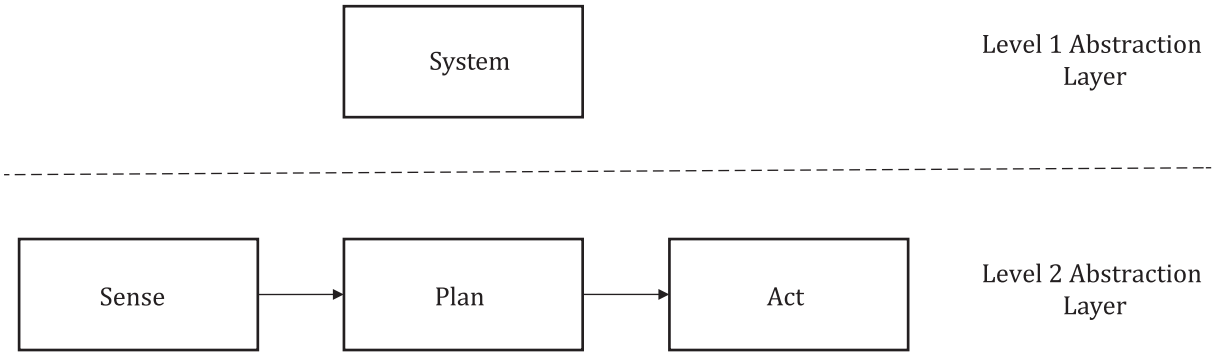


Figure 9 — Visualisation of the Sense-Plan-Act model

Based on the Sense-Plan-Act model, the selection of a capable, comprehensive system architecture can be an important consideration in achieving efficient SOTIF process so that the overall capability and corresponding activities can take place both at early stages and throughout the whole functional development lifecycle. Selecting a capable system architecture is crucial to ensure the SOTIF. Therefore, activities corresponding to the definition of the system architecture can be started at an early stage of the system development. Moreover, the system architecture is reviewed regularly along the system lifecycle and updated if necessary.

4.3 Use of this document

4.3.1 Flow chart and structure of this document

The SOTIF activities (see Figure 10) start with defining the specification and design (see Clause 5). The specification and design already include functional insufficiencies that are already known before the downstream SOTIF activities and cycles. Iterations of SOTIF activities can result in updates to the specification and design, and new previously uncovered functional insufficiencies. Each iteration starting from the specification and design relies on the specification and design being up to date.

The potentially hazardous behaviours of the intended functionality are subjected to a hazard identification and risk evaluation (see Clause 6). The identified hazardous events are evaluated regarding their risk and risk acceptance criteria are defined accordingly. If it is shown that the hazardous events do not lead to unreasonable risk, then no additional design measures are applied. Clause 6 does not consider the causes of hazardous behaviour of the intended functionality, but only their consequences for safety. Therefore, the focus is to evaluate hazardous events that could result from hazardous behaviour, and to define the acceptance criteria that are necessary to meet.

Clause 7 identifies the possible root causes for the hazardous behaviours of the intended functionality (see Figure 3) and evaluates if the risk resulting from the identified potential functional insufficiencies and triggering conditions is reasonable.

The functionality is modified (e.g. improvement of sensor capabilities, further restrictions of the ODD) to improve the SOTIF if deemed necessary as a result of the activities of Clauses 6, 7, 9, 10, 11, 12 and 13 (see Clause 8).

A verification and validation strategy is developed to provide evidence that the SOTIF-related vehicle-level residual risk is below an acceptable level and elements meet their functional requirements (see Clause 9) and the coverage over the operational design domain (ODD) is sufficient. To enable the collection of the required evidence, corresponding verification and validation test cases can be derived from this strategy and the test case coverage over the ODD is sufficiently high (see Clauses 10 and 11).

It is evaluated if the results of the SOTIF activities are sufficient to argue the achievement of the SOTIF (Clause 12).

© ISO 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

A process to evaluate and resolve possible emerging field operation SOTIF issues is defined in the operation phase (see Clause 13).

Figure 10 describes the flow of the activities required in this document to ensure the safety of the intended functionality. The circled numbers denote the corresponding clauses within this document.

© ISO 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

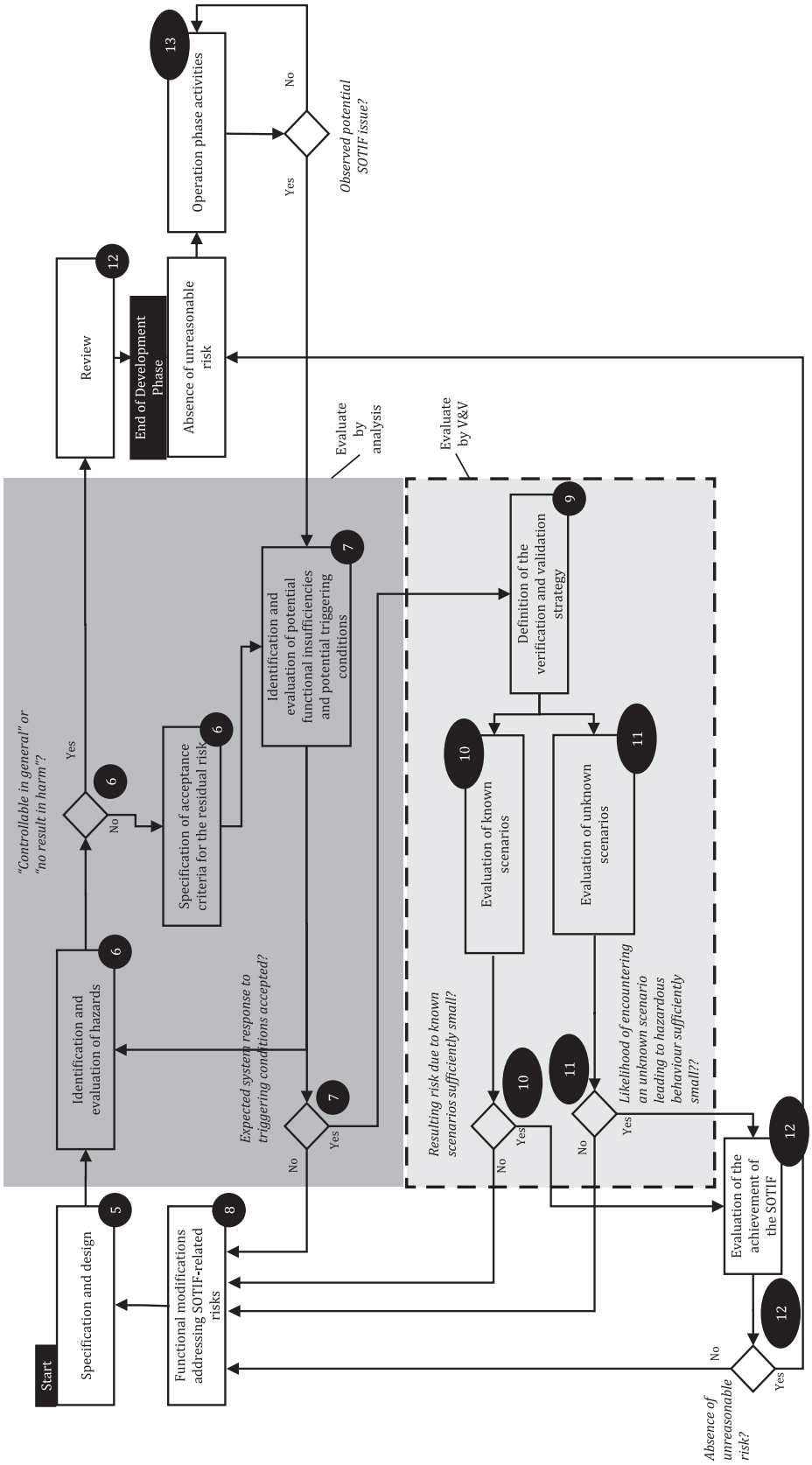


Figure 10 — Dependencies between the ISO 21448 activities

NOTE A.3 presents a simplified SOTIF application across levels of automation.

Annex A provides general guidance on the SOTIF.

© ISO 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

Annex B provides guidance on scenario and system analysis.

Annex C provides guidance on SOTIF verification and validation.

Annex D provides guidance on specific aspects of SOTIF, like the specification of the driving policy, implication for machine learning, and considerations for maps and V2X.

4.3.2 Normative clauses

Compliance to this document is claimed by achieving the objectives listed at the beginning of the clauses and providing evidence of their achievement documented in the corresponding work products. The normative character of the objectives is expressed by the use of the key word "shall", which indicates a requirement.

NOTE A.1 gives examples of such arguments based on the Goal Structuring Notation (GSN).

4.3.3 Interpretation of tables

Some tables within this document list a collection of methods and measures in order to achieve a certain development target. The entries are meant to illustrate possible methods and measures and the table entries are not exhaustive. Other equivalent methods and measures can be applied. The intention of the tables is to support the development team in their selection of one or more appropriate measures and methods.

NOTE The choice of an appropriate set of methods can depend on various factors like complexity or exposure of the hazardous event.

4.4 Management of SOTIF activities and supporting processes

4.4.1 Quality management, systems engineering and functional safety

In order to develop a safe product, rigorous engineering and quality management processes are essential. These are already addressed in other standards, like IATF 16949, the ISO 26262 series and ISO/IEC/IEEE 15288. This document focuses only on the SOTIF-specific aspects of these processes.

NOTE 1 During product development, activities specified in this document and the ISO 26262 series can be carried out in parallel. Implemented measures in general can have an impact on SOTIF as well as functional safety and are evaluated by both disciplines. 6.1 provides practical guidance for implementing ISO 26262 and SOTIF in parallel.

For management activities and supporting processes ISO 26262-2, ISO 26262-7 and ISO 26262-8 can be extended to the SOTIF activities. Special attention for requirements cascading and traceability is further described in 5.3 and 10.2.

For SOTIF-related activities a set of methods and measures are selected as follows.

— The SOTIF process (see Figure 10) starts with defining the specification and design of the system and its architecture (see Clause 5).

— The potentially hazardous behaviours of the intended functionality are subjected to a hazard identification and risk evaluation (see Clause 6) that identifies hazards and their corresponding hazardous events. If it is shown that these hazardous events do not lead to unreasonable risk of harm, then no additional design measures are applied.

NOTE 2 Clause 6 does not consider the causes of hazardous behaviour of the intended functionality, but only their consequences for safety. Therefore, the focus is to evaluate hazardous events that could result from hazardous behaviour, and to define the acceptance criteria to meet.

— Clause 7 identifies the possible root causes for the hazardous behaviours of the intended functionality (see Figure 1) and estimates if the risk resulting from the identified potential functional insufficiencies and triggering conditions is reasonable.

© ISO 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

— The functionality is modified (e.g. improvement of sensor capabilities, further restrictions of the ODD) to improve the SOTIF if deemed necessary as a result of the activities of Clauses 6, 7, 10, 11, 12 and 13 (see Clause 8).

— A verification and validation strategy is developed to provide evidence that the SOTIF-related vehicle-level residual risk is below an acceptable level and components meet their functional requirements (see Clause 9). Corresponding verification and validation test cases can be derived from this strategy in order to evaluate if the resulting risk is sufficiently small (see Clauses 10 and 11).

— The residual risk is evaluated (see Clause 12) considering the results from previous activities.

— A process to identify and resolve possible emerging field operation SOTIF issues is defined in the development phase and implemented during the operation phase (see Clause 13).

NOTE 3 Further explanations regarding the interactions between functional safety according to the ISO 26262:2018 series and this document can be found in A.2.

4.4.2 Distributed SOTIF development activities

In case of a distributed product development, a development interface agreement (DIA) is defined between all involved parties. The goal of the DIA is to confirm, in the early stages of a project, all responsibilities of the SOTIF activities and that adequate technical information will be exchanged between the development parties.

IATF 16949 provides a base process framework, that can also be considered within this context. This sub-clause focuses on how to extend a DIA to distributed SOTIF development and operation. The ISO 26262:2018 series provides the framework of a DIA and supply agreement regarding functional safety aspects. In order to apply this framework to SOTIF, tailoring can be applied by adding the responsibilities of each party related to SOTIF development and operation. The responsibilities of each party are considered and agreed upon to plan and perform the entire relevant SOTIF activities of Clauses 5 to 13. The information and work products that will be shared are specified. These activities can be done using processes that are described in ISO 26262-8:2018, 5.4.1, 5.4.2, 5.4.3, 5.4.4 and 5.4.6 and tailored for SOTIF activities. The documentation format is agreed at the beginning of the development project.

4.4.3 SOTIF-related element out of context

To achieve SOTIF it is essential that the interfaces between different systems [hardware (HW) and software (SW)] are described. In order to ensure that the integrated system is safe within the specified ODD, the boundaries of each system (e.g. a stand-alone sensing system) are carefully evaluated. Because environmental factors (e.g. ODD, scenario) are essential issues of SOTIF development, systems and their elements have different concerns depending on the hierarchical layers. As far as the development of these systems and elements are considered, they can be categorized in one of the following three types.

a) In-context development: the complete system is developed using all the SOTIF activities following a V model. For distributed parties who develop the system and its elements, requirements are determined including specification and design (see Clause 5) and other activities (see Clauses 6, 7, 8, 9, 10, 11, 12 and 13) depending on the role assignment. In ISO 26262 terms, this development would be considered as “in-context” development.

b) SOTIF-related element out of context: for these elements assumptions can be made regarding their use within the whole system and their contribution to the intended functionality. As such it is possible to make assumptions about the SOTIF-related output insufficiencies and their allowed target rate of occurrence. These assumptions are documented and used as inputs for the subsequent development of these elements. The SOTIF activities provide evidence that the corresponding target rates are met. For a SOTIF-related element out of context, the identified triggering conditions of the element and their resulting output insufficiencies are documented as well as their assumptions of use. When integrating this SOTIF-related element out of context, the

© ISO 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

validity of the assumptions is established by SOTIF activities in the context of whole vehicle-level functionalities (see ISO 26262-10:2018, Clause 9).

c) Non-specific SOTIF-related development: the functionality of these elements can contribute in too many ways to the intended functionality so that it is practically not feasible to estimate the SOTIF-related requirements a priori without the context in which these elements will be used.

EXAMPLE The requirements allocated to graphical processing units (GPUs) will depend on the system context and the SW running on these GPUs.

5 Specification and design

5.1 Objectives

The purpose of this clause is to achieve the following objectives:

a) the specification and design shall contain information sufficient to conduct the SOTIF-related activities; and

b) the specification and design shall be updated as required after each iteration of the SOTIF-related activities (see Figure 10).

5.2 Specification of the functionality and considerations for the design

The specification and design can include various aspects as listed in this subclause. Some aspects are relevant only for a specific automation level or a specific implementation. In addition, some aspects are relevant for the specification of the functionality on the vehicle level and some on the element level.

Aspects for consideration (where applicable) include, but are not limited to the following:

— the description of the intended functionality and the functionalities of the supporting subsystems and components including:

  — the ODD;

  — the level and details of the automated driving function control authority over vehicle dynamics;

  — the vehicle-level SOTIF strategy;

  — the use cases in which the function can be active or inactive, and the transitions between them; and

  — the description of decision-making logic (e.g. path planning, driving policy – see D.1);

— the design of the relevant system and its elements implementing the intended functionality;

— the performance targets of the installed sensors, controllers, actuators or other inputs and components (e.g. maps – see D.3) enabling the intended functionality;

  NOTE 1 Performance targets of an automated driving system, for example, include the detection and response to critical objects and events (e.g. pedestrians, vehicles, bicycles, motorcycles and traffic signs) within the ODD.

— the dependencies of the intended functionality on, and interactions or interfaces with:

  — the driver;

  — the driver interface (e.g. HMI), and how the interface is used to mitigate known reasonably foreseeable misuses;

  — the remote/back office operator;

© ISO 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

  - the passengers, pedestrians, cyclists and other road users;
  - the relevant environmental conditions;
  - the road infrastructure and road furniture;
  - the data exchange to and from the cloud, inter-vehicle or other communication infrastructures (e.g. V2X/X2V – see D.4) and in-service telematics involving diagnostics and parameter updates;
  - the remote flashing of software updates; and
  - the other functions of the vehicle that might interfere with the intended functionality, including the exchange of information, and the corresponding assumptions of use;
- the reasonably foreseeable misuse (direct and indirect);
- the potential performance insufficiencies, identified triggering conditions and countermeasures of the system and its elements;

  NOTE 2 Some potential performance insufficiencies and risks identified during SOTIF activities can be accepted and have no "countermeasures". In such cases these can be documented as part of the specification and design.

- the system and vehicle architectures implementing the intended functionality;
- the warning and degradation concept:
  - the warning strategies;
  - the DDT fallback: takeover/fallback conditions and schemes for transitioning control from the automated driving system to the driver or another system within their respective use cases;
  - the minimal risk condition schemes (e.g. autonomously exit lane and park, stop in path, fallback-ready user); and
  - the driver monitoring system and its operational effect on the fallback strategy;
- the procedures supporting data collection and monitoring during and after development of the intended functionality:
  - the objectives and requirements for the data collection;
  - the architecture, implementation and mechanisms supporting the required data collection before SOTIF release; and
  - the requirements, design and mechanisms that support data collection during the operation phase for SOTIF analysis (see 13.5), including possible cloud based, "Over The Air", or RF communication technologies;
- the mechanism, design and requirements that support risk mitigation abilities during operation.

5.3 System design and architecture considerations

The specification and design provide an adequate understanding of the system, its elements, its functionality and the performance targets, so that the activities in subsequent phases can be performed. This includes an exhaustive list of known functional insufficiencies, related triggering conditions and, where applicable, their countermeasures. Some potential functional insufficiencies, triggering conditions and countermeasures are known and documented before the SOTIF-related process begins while others are revealed as a result of the SOTIF activities. The system is designed such that countermeasures are implemented to mitigate the effect of known functional insufficiencies on the overall system.

© ISO 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

Each iteration of the SOTIF-related activity (see Figure 10) can result in engineering activities which can lead to updates in the specification and design at any relevant level. Each iteration relies on the specification and design being updated at any relevant level, such that it reflects all information discovered in previous iterations.

Cooperation among development parties (OEM, Tier 1, Tier N) is necessary to discover potential functional insufficiencies of the integrated system, component or element, and to develop countermeasures to these insufficiencies during the development phases (see 4.4). Relevant sections of design and specification are communicated to lower-level system and component developers. Assumptions of use, foreseeable misuse and potential performance insufficiencies are communicated from one tier to the next hierarchical levels, up to and including the OEM, after each development cycle/iteration.

As the SOTIF activities identify new functional insufficiencies and triggering conditions (see Clause 7), and measures to improve the SOTIF are defined (see Clause 8), the specification and design is updated as part of each development cycle as seen in Figure 10.

SOTIF work products are linked with the specification and design if they impact the specification and design (as defined in 5.2), including pre-existing relevant content. This ensures that all information from previous iterations is captured, and that the specification is ready for the next iteration cycle.

NOTE Traceability and completeness of the specification and design (work products 5.5) can be demonstrated by linking to SOTIF measures (work products 8.5) which can be further linked with:

— the relevant design document(s);

— the work products from:

  — Clause 6 - risk evaluation of hazardous behaviours (e.g. to achieve an S=0, C=0, or to obtain less constraining acceptance criteria);

  — Clause 7 - evaluation of the system's response to the identified triggering conditions (e.g. link to the analysis of a triggering condition showing unacceptable risk);

  — Clauses 9 and 10 - verification and validation results for known hazardous scenarios (e.g. link to a verification test report showing unacceptable performance with respect to the requirements);

  — Clauses 9 and 11 - validation results for unknown hazardous scenarios (e.g. link to a validation test report showing unacceptable performance with respect to a hazardous scenario or the validation targets);

  — Clause 12 - SOTIF release argument (e.g. link to report documenting reasons for rejecting release request); and

  — Clause 13 - field monitoring process (e.g. link to report documenting new hazardous scenario discovered during field monitoring);

The SOTIF technical assumptions related to risk evaluation in Clauses 6 (6.4) and 7 (7.4) are not necessarily associated with SOTIF measures in Clause 8 (8.3) but can still be traced to the specification and design. Design tools offering model-based design and supporting traceability between different model artefacts (requirements, components, interfaces, analysis, test cases and results) can support this process.

5.4 Performance insufficiencies and countermeasures considerations

The design includes considerations on potential performance insufficiencies that can result from an element output value which can potentially lead to hazardous behaviour at the vehicle level. A non-exhaustive list of examples of potential performance insufficiencies includes:

— insufficient classification,

— insufficient measurements,

— insufficient tracking,

— insufficient target selection,

© ISO 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

— insufficient kinematic estimation,

— false positive detections (e.g. ghosts, phantom objects),

— false negative detections, and

— driving policy level limitations such as considering occluded areas.

Guidance on possible methods to identify functional insufficiencies and the corresponding vehicle-level hazardous behaviour can be found in B.3. Functional insufficiencies are most relevant when the system operates within its specified ODD. The way the system detects leaving its specified ODD, and how it operates during transitions, is relevant to support the complete analysis.

The system development is based on the assumptions made about the performance insufficiencies in the design. Measures are implemented to cope with these performance insufficiencies to ensure the SOTIF. The design and measures, integrated into the specification and design, decrease the residual risk and increase overall robustness (see Figures 5 and 6).

NOTE 1 Methods and measures to discover potential functional insufficiencies and their triggering conditions are detailed in Clause 7.

NOTE 2 Methods and measures to address functional insufficiencies such as (but not limited to) redundancy, diversity, complementary elements are described in Clause 8.

NOTE 3 The SOTIF content of the specification and design is verified as elaborated in Clause 10.

The following are examples of performance insufficiencies and possible countermeasures. This is content that is included in the specification and design document(s):

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 automated driving functionalities 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 due to its speed being implausible. A collision with the skateboarder can be mitigated, in this case, by a system with an abstraction between the object-detection algorithm and the sensing and processing algorithms and using other different plausibility checks.

EXAMPLE 3 A pedestrian crossing drawn as a three-dimensional optical illusion (see Figure 11) is used to alert drivers in some areas. The image is drawn on the road 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 that result from classification limitations.

© ISO 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

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

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

5.5 Work products

The work product is the specification and design, fulfilling objectives 5.1 a) and 5.1 b).

NOTE 1 The specification and design can be split into or linked to several documents such as: requirement specifications, functional specifications and design specifications of the SOTIF-related systems.

NOTE 2 The SOTIF specification of mitigation measures can be integrated into existing functional safety design documentation such as functional safety concept and/or technical safety concept.

6 Identification and evaluation of hazards

6.1 Objectives

The purpose of this clause is to achieve the following objectives.

a) The hazards arising from the intended functionality, defined at the vehicle level, shall be systematically identified.

b) The risk that arises from the hazardous behaviour of the intended functionality, and the corresponding scenarios in which the hazardous behaviour can lead to harm, shall be systematically identified and evaluated. The parameters that define the circumstances in which the behaviour of the intended functionality is considered hazardous shall be specified.

EXAMPLE Such parameters can be a speed deviation or the minimum distances to other objects.

c) The acceptance criteria for the residual risk shall be specified.

© ISO 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

6.2 General

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

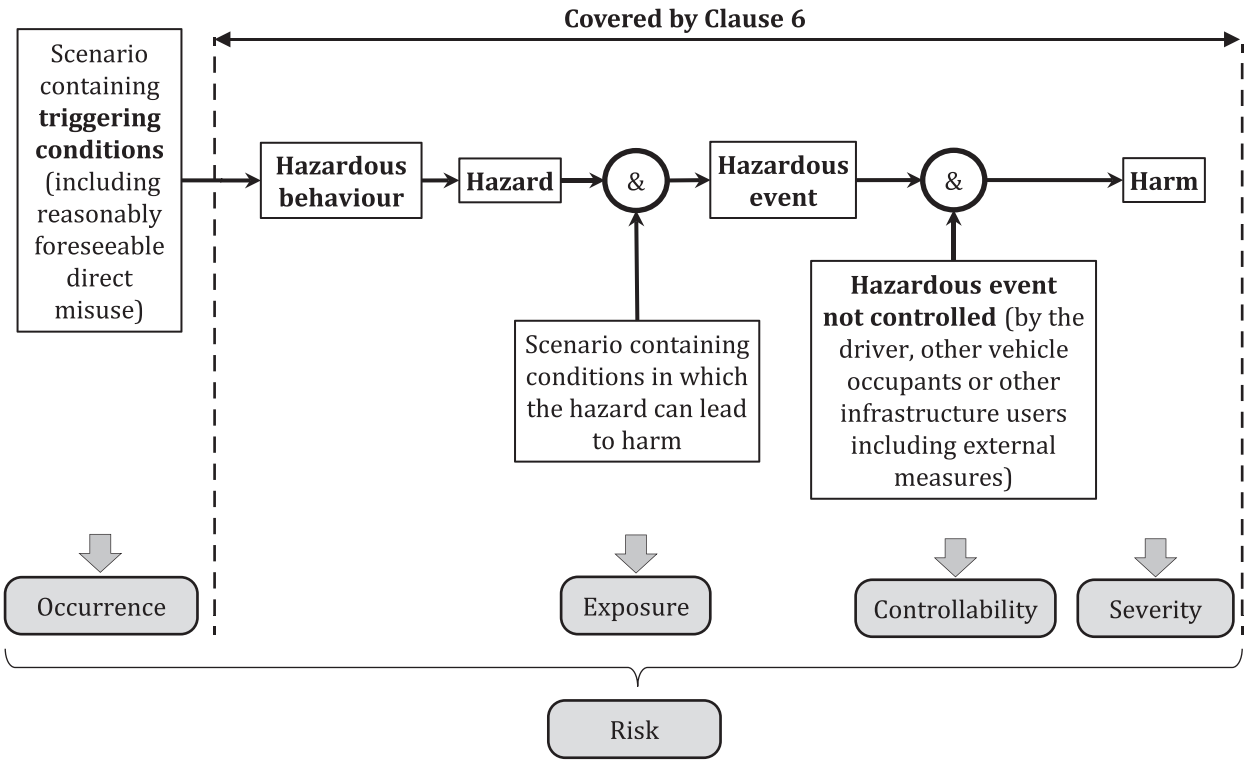
— specification and design in accordance with 5.5; and

— available data for the derivation of acceptance criteria.

6.3 Hazard identification

The hazards resulting from functional insufficiencies are determined systematically at the vehicle level. This systematic identification is primarily based on knowledge about the function and its possible deviations resulting from functional insufficiencies. This can be achieved by applying the methods specified in ISO 26262-3. An illustration of the common elements of the hazard analysis required by both the ISO 26262 series and by this subclause can be found in Figure 12. Figure 13 uses an AEB system as an example to show how the terms from Figure 12 are used. The example shows two hazards resulting from the same hazardous behaviour. The application of hazard analysis is further elaborated in A.2.5 using AEB as an example.

EXAMPLE 1 An AEB system can cause hazards originating from both hazardous behaviour of the intended functionality and malfunctioning behaviour. The hazard resulting from unintended braking, inside and outside the functional limits, can be analysed from a functional safety perspective in a hazard analysis and risk assessment. The same hazard related to unintended braking inside the functional limits is also subject to analysis of the SOTIF.



Key

→ result in

⇩ has characteristics of

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

© ISO 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

NOTE 1 Unlike in ISO 26262-3, when analysing a SOTIF-related hazard, no automotive safety integrity level (ASIL) is determined for a hazardous event. However, the parameters severity (S), exposure (E) and controllability (C) can be used to adjust the validation effort.

NOTE 2 The occurrence reflects the probability of encountering triggering conditions during the operating phase of the functionality.

There is an important difference between the occurrence of a triggering condition and the exposure to a scenario in which the hazard can lead to harm. In general, triggering conditions are not independent from scenarios. Therefore, in order to use the exposure to a scenario within an argument for risk reduction, the statistical dependence between the probability of being in a scenario and the probability of encountering a triggering condition is taken into account in the evaluation.

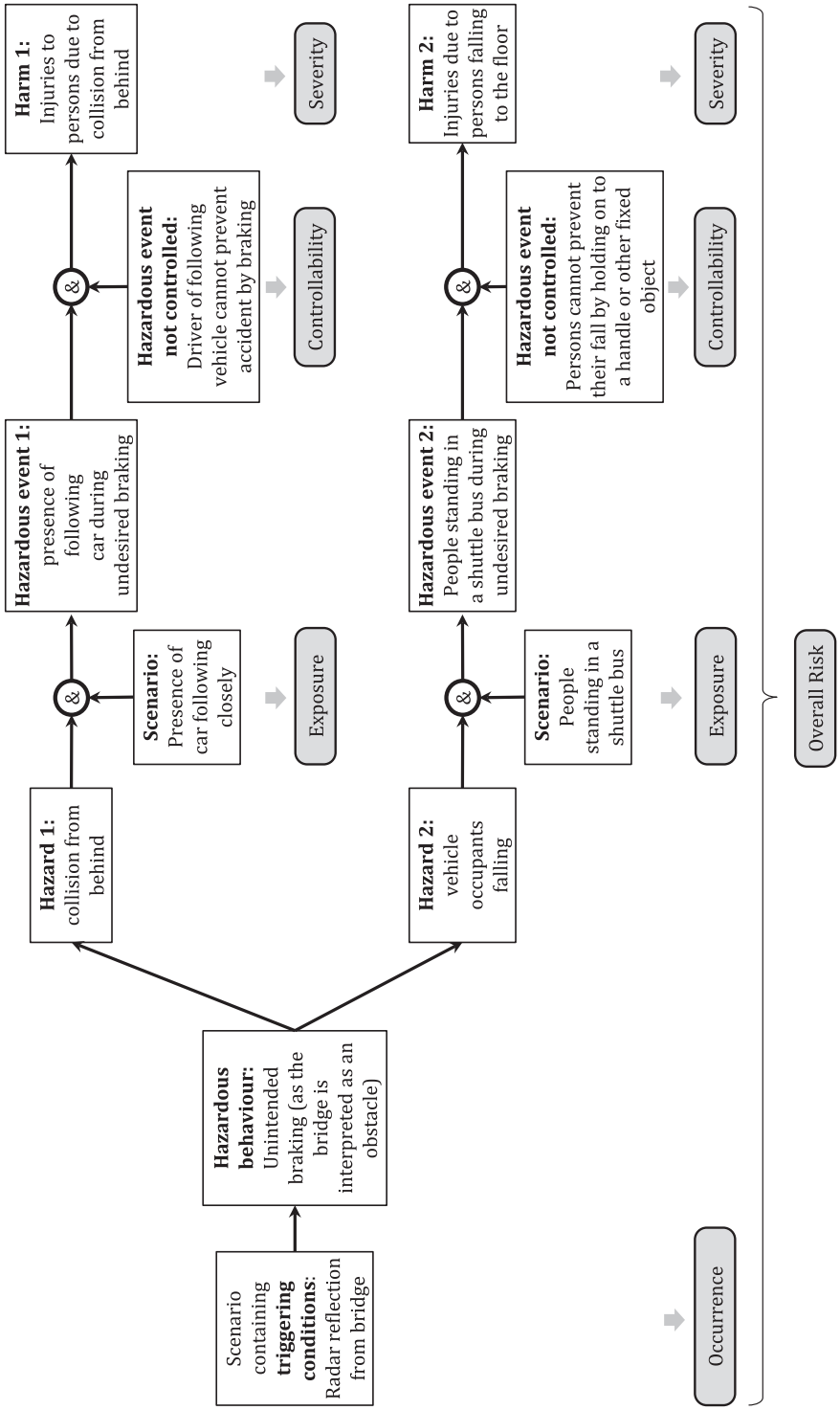
EXAMPLE 2 No statistical independence can be assumed for a triggering condition of a highway pilot where the scenario is driving on a highway.

In some specific cases, statistical independence can be assumed as it is shown in Figure 13.

The C parameter can be used to evaluate whether SOTIF-related hazards are controllable (see 10.6 and Table 10). Studies or assumptions about the reaction of road participants can be used to support controllability ratings.

© ISO 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022



Key

→ results in

⇩ has characteristics of

Figure 13 — An AEB example using terms from Figure 12

NOTE 3 The example in Figure 13 shows that the resulting risk can be assessed on two levels: first the risk relating to a specific hazard in a given scenario, and second the overall risk that is related to the hazardous behaviour and includes the evaluation of several hazards and the corresponding scenarios.

In addition to the systematic identification resulting from possible function deviations, further hazards can be identified by considering the interaction of the driver or user with the system [illegible]

© ISO 2022 – All rights reserved

AVA Documents Document Sharing Hub

Full document details: BS ISO 21448:2022

reasonably foreseeable misuse. Reasonably foreseeable misuse is differentiated by its causal link with the hazard. A direct misuse of the intended functionality results in a triggering condition while an indirect misuse of the intended functionality causes a reduction in controllability or an increase in severity of a hazardous event resulting from a hazardous behaviour (e.g. an inattentive driver or a driver misunderstanding the limitations of a function).

The identification of reasonably foreseeable indirect misuse, and the analysis of its effects, are covered by Clause 7.

NOTE 4 7.3.4 and B.1 provide general guidance for the analysis of reasonably foreseeable misuse.

6.4 Risk evaluation

The risk evaluation aims to evaluate the risk due to hazardous behaviour in given scenarios; this helps to specify the acceptance criteria of a SOTIF-related risk.

NOTE 1 The hazardous behaviour resulting from a functional insufficiency on the vehicle level, if any, is part of this evaluation.

The severity of harm, and the controllability of hazardous events, can be estimated using the method described in ISO 26262-3:2018, Clause 6. Despite sharing the analysis method, the observed outcome and the estimated parameters for a specific hazard can be different for the SOTIF analysis.

NOTE 2 ISO 26262-3 introduces classes for controllability, severity, and exposure. In the context of Clause 6, it is only relevant whether a hazardous event is or is not controllable in general, or, does or does not result in harm. Exposure is not a determining parameter for risk evaluation in Clause 6. As the risk is evaluated in scenarios, their selection already implies that the exposure to them is SOTIF-related, otherwise they would not be considered for analysis.

NOTE 3 The exposure to specific scenarios can be considered for the specification of validation targets (see Clause 9).

EXAMPLE 1 The severity of a rear collision with the host vehicle, caused by automated emergency braking, can be reduced by limiting the brake intervention magnitude. The magnitude limit can be seen as a safety measure to increase controllability, or as a functional modification to the intended behaviour. When analysing the hazard, the limit is considered as part of the intended behaviour; in contrast, 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 hazardous event are considered to determine if the resulting risk is unreasonable in a given scenario. The severity and controllability evaluation considers the functional specification (according to the specification and design resulting from Clause 5). The absence of unreasonable risk is established if the controllability is rated as "controllable in general" (i.e. C=0) or the severity is rated as "no resulting harm" (i.e. S=0). In all other cases a hazardous event is considered SOTIF-related. The corresponding hazardous behaviour is described using measurable parameters like speed deviations and minimum distances to other objects. The controllability evaluation includes “no reaction”, or “delayed reaction” by the involved persons to control the hazard, e.g. resulting from reasonably foreseeable indirect misuse. This evaluation can also consider external measures.

EXAMPLE 2 An environmental condition that is not handled by an advanced driver assistance system (ADAS) in a safe manner and therefore, requires the driver to resume control can be considered for hazardous event classification.

A delayed or inappropriate reaction by the driver, including the time necessary for the driver to achieve sufficient situational awareness and recovery, can impact the controllability evaluation and is a topic of the SOTIF-related analysis.

If after a functional modification (see Figure 10) a hazardous event is judged as S=0 or C=0 then the hazard has been sufficiently addressed.

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

© ISO 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

Table 3 — Example of a hazardous event

Hazardous behaviour	Potential consequence	Severity		Controllability		unreasonable risk?
		Rating	Note	Rating	Note	
Unintended AEB activation at x m/s^2 for y seconds while operating on a highway	Rear collision with following vehicle	S > 0	Effective impact speed: $v \geq x$ km/h	C > 0	The following vehicle might not be able to brake to avoid collision.	Yes

6.5 Specification of acceptance criteria for the residual risk

If the risk parameters are not evaluated as S=0 or C=0, then acceptance criteria are specified for the risks associated with the hazardous behaviour and the activities continue with Clause 7.

The argument for the S=0 or C=0 classification is reviewed as part of the SOTIF process and includes the review of the evidence for the classification (e.g. test or analysis results).

Acceptance criteria consider:

— applicable governmental and industry regulations;

— whether a function is new or already established in the market;

— whether the risk is unreasonable for the people who might be exposed to the risk (e.g. a vehicle owner, the operator, a pedestrian or a passenger in an automated public transport system);

— acceptance criteria of already established functions; and

— the performance of a driver who acts in an exemplary fashion.

EXAMPLE 1 Such acceptance criteria could be a maximum number of accidents per hour. An appropriate verification and validation strategy is defined in Clause 9 and is based on the specified acceptance criteria.

Approaches that can be considered when specifying acceptance criteria include:

— the available traffic data for the target market (e.g. accident statistics, traffic analyses) (see C.2.2.4); and

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

EXAMPLE 2 Number of false positive events per x km produced by a similar collision warning system that is in series production (similar test distribution).

Appropriate quantitative acceptance criteria can be chosen provided that a valid rationale is given. The overall rationale can be based on one, or a combination of several, of the following individual rationales.

— A risk tolerability principle, such as the GAMAB (Globalement au moins aussi bon) or GAME (Globalement au moins équivalent); both French terms having the meaning "globally at least as good". Following this principle, the residual risk (with respect to safety) of any new system is not higher than that of existing systems having comparable functionality or hazards.

— A positive risk balance. 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. A system can be released even though the residual risk for a given hazard has increased, provided that this is compensated for by counterbalancing reductions in one or more other residual risks.

— The ALARP principle. The ALARP risk management framework can provide a useful risk reduction principle, particularly regarding the development and introduction of novel technologies where "good practice" does not currently exist. By acknowledging that a state of zero risk is not possible, the ALARP principle aims to reduce risk to a level considered "reasonably practicable" by weighing the risk against the effort needed to further reduce it.

© ISO 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

— The MEM (minimal endogenous mortality) principle. The MEM principle is based on the idea that the introduction of a technical system should not significantly increase the death rate in society. Quantitative acceptance criteria for the probability of death caused by a technological system are derived from the minimum probability of death from natural causes.

NOTE 1 A rationale in the context of this document can only include SOTIF-related risks and does not include risks from other safety domains (e.g. electrical safety).

NOTE 2 C.2 and C.6 give examples for defining and evaluating acceptance criteria and validation targets.

NOTE 3 A description of GAMAB, ALARP and MEM can be found in EN 50126-2:2017, A.1 (RAMS)[4].

NOTE 4 A valid rationale can be based on risk across a fleet or risk associated with an individual vehicle. Even if a fleet has a very low probability to encounter a triggering condition as part of a scenario, the response of the system can be unacceptable if the probability of facing such a scenario is high for a given individual vehicle.

6.6 Work products

6.6.1 Hazards at the vehicle level, fulfilling objective 6.1 a)

6.6.2 Risk evaluation of hazardous behaviours, fulfilling objective 6.1 b)

6.6.3 Acceptance criteria, fulfilling objective 6.1 c)

7 Identification and evaluation of potential functional insufficiencies and potential triggering conditions

7.1 Objectives

The purpose of this clause is to achieve the following objectives.

a) Potential insufficiencies of specification, potential performance insufficiencies and potential triggering conditions including reasonably foreseeable direct misuse shall be identified and those leading to a hazardous behaviour shall be determined.

b) The response of the system shall be evaluated for SOTIF acceptability.

NOTE 1 This includes the identification of functional insufficiencies and related triggering conditions relevant in the context of reasonably foreseeable direct and indirect misuses.

NOTE 2 This activity considers the potential insufficiencies of specification of the intended functionality at the vehicle level as well as the potential insufficiencies of specification or potential performance insufficiencies of E/E elements of the system.

7.2 General

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

— specification and design, in accordance with 5.5;

— hazards at the vehicle level, in accordance with 6.6.1;

— risk evaluation of hazardous behaviours including identified reasonably foreseeable indirect misuses, in accordance with 6.6.2;

— acceptance criteria, in accordance with 6.6.3; and

© ISO 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

— known potential functional insufficiencies of the system and its elements and known potential triggering conditions (including reasonably foreseeable direct misuse) that could lead to a hazardous behaviour based on external information or lessons learnt (e.g. 13.5).

7.3 Analysis of potential functional insufficiencies and triggering conditions

7.3.1 General

The potential functional insufficiencies and triggering conditions are systematically analysed. This analysis can consider field experience and knowledge gained from similar projects or experts.

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

— the known potential insufficiencies of specification and performance insufficiencies to determine scenarios (containing triggering conditions) leading to identified hazardous behaviour; and

— the identified environmental conditions and reasonably foreseeable misuse to determine potential insufficiencies of the specification and performance insufficiencies.

NOTE 1 Further details on SOTIF analysis techniques are given in Annex B. Also, ISO 34502 [5] can be referred to.

NOTE 2 The analysis can be supported by inductive, deductive or exploratory methods.

NOTE 3 The analysis can be performed qualitatively, quantitatively, or both.

NOTE 4 Quantitative targets can be defined down to the element level, derived from acceptance criteria or validation targets at the vehicle level.

NOTE 5 Proper abstraction (e.g. generation and use of equivalence classes or subsets) of all relevant use case parameters can be helpful to cope with a large number of use case combinations.

NOTE 6 Traffic statistics can be used to focus on plausible use cases that could lead to potentially hazardous behaviour.

NOTE 7 This analysis can be supported by simulations, e.g. using Monte-Carlo methods.

An appropriate combination of methods to identify and to assess the potential insufficiencies of specification, performance insufficiencies, output insufficiencies and triggering conditions can be applied as listed by Table 4.

Table 4 — Analysis methods of potential functional insufficiencies and triggering conditions

Methods	
A	Analysis of requirements

[a] It includes analysis of the ODD boundaries.

[b] For example, STATS19 (UK)[6], GIDAS (Germany)[7], GES (US)[8], CARE[9], IGLAD[10].

[c] Several performance insufficiencies or insufficiencies of specification can be activated by a single triggering condition (e.g. heavy rain can impact the performance of different sensors such as radar and camera).

[d] This considers analysis of comparable systems in the market, predecessor systems and projects, and customer claims.

[e] This considers technological limitations (e.g. angular resolution due to camera imager, radar antenna design limitation or lack of environmental isolation such as water sealing and vibration) as well as technical limitations due to mounting (e.g. blind areas resulting from sensor not covering the entire 360° visual field around the vehicle).

[f] For example, a camera lens that becomes dull due to ageing effects within the specified limits.

[g] For example, vehicle-to-vehicle, vehicle-to-infrastructure, over-the-air maps.

[h] For example, based on analysis of records coming from Data Storage System for Automated Driving / Event Data Recorder (DSSAD/EDR).

[i] The analysis methods are listed in Table 5.

© ISO 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

Table 4 *(continued)*

Methods	
B	Analysis of the ODD, use cases and scenarios [a]
C	Analysis of accident statistics [b]
D	Analysis of boundary values
E	Analysis of equivalence classes
F	Analysis of functional dependencies
G	Analysis of common triggering conditions [c]
H	Analysis of potential triggering conditions from field experience and lessons learnt [d]
I	Analysis of system architecture (including redundancies)
J	Analysis of design of the sensors and potential technology limitations [e]
K	Analysis of algorithms and their output or decisions
L	Analysis of system ageing [f]
M	Analysis of possible environmental changes over vehicle operational lifetime (e.g. interference)
N	Analysis of external and internal interfaces [g]
O	Analysis of design of the actuators and potential limitations
P	Analysis of accident scenarios [h]
Q	Analysis of reasonably foreseeable misuse [i]

[a] It includes analysis of the ODD boundaries.

[b] For example, STATS19 (UK)[6], GIDAS (Germany)[7], GES (US)[8], CARE[9], IGLAD[10].

[c] Several performance insufficiencies or insufficiencies of specification can be activated by a single triggering condition (e.g. heavy rain can impact the performance of different sensors such as radar and camera).

[d] This considers analysis of comparable systems in the market, predecessor systems and projects, and customer claims.

[e] This considers technological limitations (e.g. angular resolution due to camera imager, radar antenna design limitation or lack of environmental isolation such as water sealing and vibration) as well as technical limitations due to mounting (e.g. blind areas resulting from sensor not covering the entire 360° visual field around the vehicle).

[f] For example, a camera lens that becomes dull due to ageing effects within the specified limits.

[g] For example, vehicle-to-vehicle, vehicle-to-infrastructure, over-the-air maps.

[h] For example, based on analysis of records coming from Data Storage System for Automated Driving / Event Data Recorder (DSSAD/EDR).

[i] The analysis methods are listed in Table 5.

NOTE 8 Safety analysis methods can be adapted to identify and evaluate potential functional insufficiencies and triggering conditions and their influence on the hazards (e.g. Cause Tree Analysis, Event Tree Analysis (ETA), inductive SOTIF analysis or Hazard and Operability Analysis (HAZOP)). B.3 provides examples of adaptation of safety analysis methods.

Depending on the system architecture, potential functional insufficiencies of an element can be classified into:

— single-point functional insufficiencies; or

— multiple-point functional insufficiencies.

This classification can help determine the adequate functional modification to achieve the SOTIF (see Clause 8). It can be used to derive requirements to the element level necessary to achieve the SOTIF at the vehicle level (see Clause 5).

EXAMPLE 1 Given a SOTIF specified acceptance criteria to be achieved at the vehicle level, performance targets can be allocated to different contributing elements, for example as shown in Figure 14. Each sensor can be allocated less constrictive performance targets (e.g. false positive detection rate) compared to a single sensor system.

© ISO 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

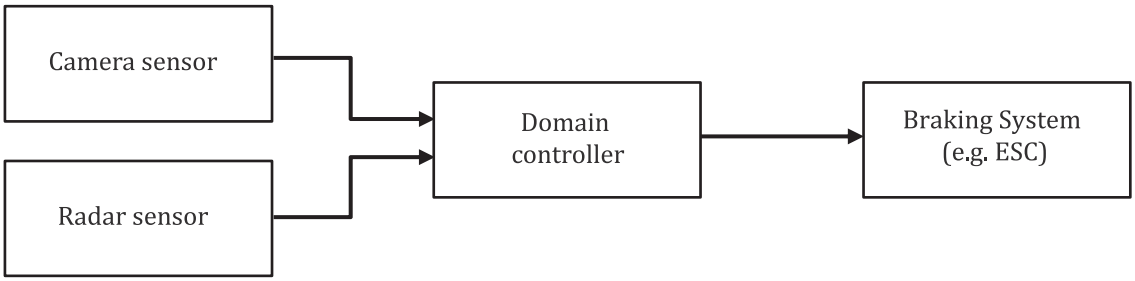
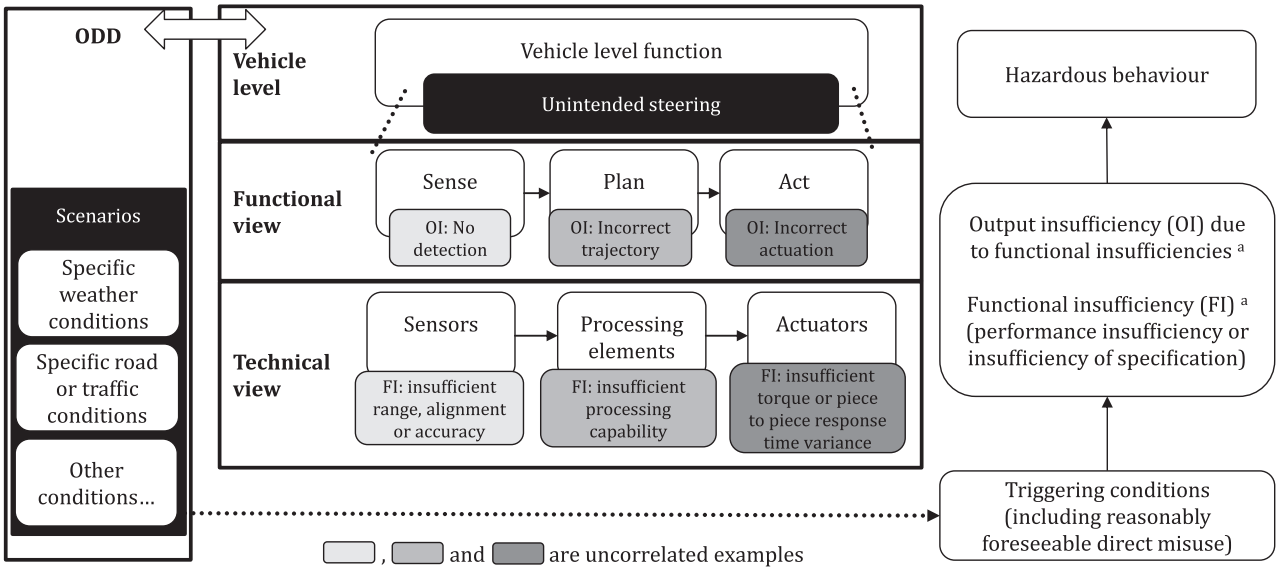


Figure 14 — Example of system architecture with the fusion of two diverse sensors

The classification can also be used during the definition of the validation strategy, where the validation targets for multiple-point functional insufficiencies can be reduced subject to independence considerations (see Clause 9 and C.6.3).

There can be multiple triggering conditions for a given performance insufficiency or insufficiency of the specification that lead to a hazardous behaviour. Additionally, known environmental conditions and reasonably foreseeable misuse can activate several vehicle or element level performance insufficiencies or insufficiencies of specification. Traceability is established and maintained between the hazardous behaviours, the triggering conditions and the potential performance insufficiencies or insufficiencies of specification on the vehicle or element level.

An illustration and an example of links between hazard, triggering conditions and the potential performance insufficiencies or insufficiencies of specification on the vehicle or element level can be found in Figure 15.



a Functional insufficiencies (as design properties) can exist within all viewpoints and on all abstraction layers.

Figure 15 — Illustration of links between potential functional insufficiencies and triggering conditions

In the following subclauses, planning algorithms, sensors and actuators are handled separately to allow a more structured presentation. If beneficial, the potential functional insufficiencies and triggering conditions in the sensors and actuators list can also be used for the planning algorithm analysis and vice versa.

© ISO 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

7.3.2 Potential functional insufficiencies and triggering conditions related to planning algorithms

The analysis can consider the following categories, among others:

— environment and location;

— road infrastructure;

— urban or rural infrastructure;

— highway infrastructure;

— driver or user behaviour (including reasonably foreseeable misuse);

— potential behaviour of other drivers or road users;

— driving scenario (e.g. a construction site, an accident, a traffic jam with emergency corridor, vehicle driving in the wrong direction);

— known planning algorithm limitation (e.g. inability to handle possible scenarios, or non-deterministic behaviour);

— known insufficiencies of the specification of machine learning;

— known insufficiencies of the measurement data for machine learning; and

— known functional insufficiencies and functional improvements.

7.3.3 Potential functional insufficiencies and triggering conditions related to sensors and actuators

The analysis can consider the following categories, among others:

— the ODD;

— weather conditions;

— mechanical disturbance (e.g. noisy sensor output resulting from vibration due to location of sensor on the vehicle);

— dirt on sensors;

— electromagnetic interference (EMI);

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

— acoustic disturbance;

— glare;

— poor-quality reflection;

— accuracy;

— range;

— response time;

— performance impact due to durability, wear, ageing;

— authority capability (applicable to actuators, e.g. maximum applicable braking pressure for a hydraulic braking system by the intended functionality);

© ISO 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

— multi-sensor data fusion; and

— alignment and installation of sensors.

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 on a pedestrian can affect the performance of ultrasonic sensors.

EXAMPLE 4 Improper alignment can affect many sensor types.

NOTE 1 A potentially hazardous behaviour can result from a combination of known potential functional insufficiencies and triggering conditions.

NOTE 2 For specific analysis categories see Annex B. For each category, a list of detailed disturbances is determined based on knowledge and experience (including knowledge gained on similar projects and field experience).

NOTE 3 If sensor input provided by infrastructure elements is relevant for the automated driving (AD) or ADAS functionality, then this subclause is also applicable for this case in order to analyse the functional insufficiencies.

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

7.3.4 Analysis of reasonably foreseeable direct or indirect misuse

A reasonably foreseeable direct and indirect misuse of the intended functionality can contribute to an unreasonable level of risk.

On the one hand, the analysis of direct misuse is covered by Clause 7 as part of the potential triggering condition analysis. On the other hand, the potential functional insufficiencies that could lead to the ineffectiveness of a measure against indirect misuses are also within the scope of Clause 7.

Causes of reasonably foreseeable direct or indirect misuse can be:

— lack of understanding of the system by the users, e.g. the driver is misled by a similar system with different operating rules in the market;

— wrong user expectations of the system, e.g. insufficient, inappropriate or incorrect information presented to the driver;

— loss of concentration;

— overreliance on the system; and

— incorrect assumption of user interaction from the system design.

The analysis of reasonably foreseeable misuse can be supported using the methods described in Table 5. In addition, B.1 describes a method for deriving SOTIF misuse scenarios.

© ISO 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

Table 5 — Methods for identification of reasonably foreseeable misuse

Methods	
A	Analysis of known misuse scenarios from field experience and other sources of lessons learnt [a]
B	Studies with test subjects
C	Analysis of use cases and scenarios
D	Analysis of users' interaction with the system [b]
E	Analysis of HMI
F	Analysis of known human patterns of lack of use, misuse and automation complacency
G	Analysis of human capability to perform or switch between certain tasks [c]
H	Application of relevant standards, regulations and guidelines [d]

[a] For example, user videos on the internet demonstrating how the system or other similar systems can be misused in a reasonably foreseeable way.

[b] For example, alertness of driver, system understanding, or operating mode confusion.

[c] For example, analysis of human capability to regain the situational awareness.

[d] For example, code of practice for the design and evaluation of ADAS[11], European statement of principles on human-machine interface[1].

NOTE 1 See detailed approach in B.1.

NOTE 2 The use of a vehicle by a driver incapable of ensuring the driving task in case of need is considered as abuse and it is outside of the scope of this document.

EXAMPLE 1 The driver is under the influence of controlled substances.

EXAMPLE 2 Driving at unreasonably high speed beyond the dynamic control capability of the vehicle on snow.

The need of additional measures dedicated to preventing or mitigating reasonably foreseeable misuse (indirect or direct), and the effectiveness of these measures, can be evaluated while estimating the acceptability of the system's response to the potential triggering conditions. The effectiveness of these measures can be demonstrated during the verification and validation phases.

7.4 Estimation of the acceptability of the system's response to the triggering conditions

The scenarios containing the identified triggering conditions are evaluated to determine whether the SOTIF is deemed to be achievable.

NOTE 1 These known scenarios are covered by the verification activities of Clause 10 to provide a final evaluation of their acceptability.

NOTE 2 Specifically, assumptions used for, or resulting from, this evaluation which are relevant for the achievement of the SOTIF are demonstrated in Clause 10.

NOTE 3 Assumptions that are considered during this evaluation can include expected behaviours of the system and its elements or assumed actions of the user.

The SOTIF is deemed as achievable without need of further functional modification (as described in Clause 8) if:

— the residual risk of the system causing a hazardous event is shown as being lower than the acceptance criteria specified in 6.5; and

NOTE 4 Evidence to be used for the risk evaluation will be generated during verification and validation activities (Clauses 9, 10 and 11).

— there is no known scenario that could lead to an unreasonable risk for specific road users.

© ISO 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

NOTE 5 Even if a fleet has a very low probability of a triggering condition as part of a scenario, the response of the system can be unacceptable if the probability to encounter such a scenario is high for a given individual vehicle.

EXAMPLE A particular structure integrated into a roundabout or a bridge pier that systematically causes the AEB system to brake in a way that could lead to unacceptable occurrences of rear collision with the following vehicle.

A system's response to the triggering conditions that is not considered as acceptable according to the conditions above initiates further functional modification (as described in Clause 8).

7.5 Work products

7.5.1 Identified potential insufficiencies of specification, performance insufficiencies and triggering conditions (including reasonably foreseeable direct misuse), fulfilling objective 7.1 a.

NOTE Reports of the analyses conducted to fulfil objective 7.1 a are included in 7.5.1.

7.5.2 Evaluation of the system's response to the identified triggering conditions for their acceptability with respect to the SOTIF, fulfilling objective 7.1 b.

8 Functional modifications addressing SOTIF-related risks

8.1 Objectives

The purpose of this clause is to achieve the following objectives:

a) measures addressing SOTIF-related risks shall be specified and applied;

b) the input information to specification and design (5.5) shall be updated.

8.2 General

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

— specification and design (in accordance with 5.5);

— risk evaluation of hazardous behaviours (in accordance with 6.6.2);

— identified potential insufficiencies of specification, performance insufficiencies and triggering conditions (in accordance with 7.5.1);

— verification and validation results for known scenarios (in accordance with 10.8), if any;

— validation results for unknown hazardous scenarios (in accordance with 11.4.1), if any; and

— SOTIF release argument in accordance with 12.5, if any.

8.3 Measures to improve the SOTIF

8.3.1 Introduction

The activities of Clause 8 to elaborate measures addressing SOTIF-related risks (hereinafter referred to as "SOTIF measures") can be performed when the following conditions are met:

— the intended functionality of the current specification and design (Clause 5) is identified as having a hazardous scenario that requires further analysis (evaluated as likely to cause harm in the risk evaluation of the hazardous event) (Clause 6); and

© ISO 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

— the system's response to the identified triggering condition that causes the hazardous behaviour is evaluated as unacceptable (there is a known scenario where the residual risk of causing the hazardous event does not meet the acceptance criteria and leads to an unreasonable risk) (Clause 7).

The system is refined through the iteration of considering SOTIF measures in Clause 8, updating the specification and design (Clause 5) with these SOTIF measures, and risk evaluation of the intended functionality (Clause 6 and Clause 7) is conducted by using the updated specification and design.

This refined system (including the effectiveness of the SOTIF measures) is then evaluated in the V&V phase, and iterative activities for refinement of the system in the design phase might be performed via Clause 8 if any of the following conditions are met:

— the residual risk from a known hazardous scenario is determined to be unacceptable (Clause 10);

— an unknown and hazardous scenario where the residual risk is unacceptable is encountered (Clause 11); or

— the residual risk is deemed unacceptable (Clause 12).

In the above case, Clause 5 through Clause 8, are repeated to refine the system.

An appropriate combination of "avoidance" or "mitigation" SOTIF measures are selected to achieve the SOTIF-related risk reduction.

NOTE "Avoidance measures" represent inherently safe design measures where the first priority is eliminating the risks (aiming to achieve S=0 or C=0 in the Clause 6 risk evaluation), and functional modifications (especially new functions added) are a typical approach. However, it does not necessarily mean that S=0 or C=0 will be achieved.

"Mitigation measures" are considered to reduce the risk as much as possible when there is known difficulty in avoiding the risk or when it can be judged acceptable. They are also expected to improve the risk reduction effect when combined with avoidance measures or other mitigation measures.

For implementation of SOTIF measures, the following can be considered:

— there are no adverse effects on other elements; and

— there are no interactions with other hazardous scenarios.

In addition, SOTIF measures, even if carefully designed and implemented might not produce the expected outcomes and could produce unintended consequences. Therefore, conducting monitoring and review activities as described in Clause 13 is an essential part of the SOTIF measures implementation to assure that the SOTIF measures remain effective.

The subclauses 8.3.2 through 8.3.5 describe possible SOTIF measures.

8.3.2 System modification

Measures for system modification are aimed at maintaining the intended functionality as much as possible. These measures can include, but are not limited to:

1) increased sensor performance and/or accuracy by:

   — improved sensor technology;

   EXAMPLE 1 Increase the resolution of a sensor measurement.

   EXAMPLE 2 Change to new and improved sensor that addresses known limitations.

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

   — diverse sensor types;

© ISO 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022

EXAMPLE 3 Add additional sensing devices to improve coverage with appropriate modality.

— improved sensor calibration and installation; or

EXAMPLE 4 Positioning the sensors for better coverage for certain corner cases that have potential for performance insufficiency.

EXAMPLE 5 Packaging the sensor(s) to avoid or minimize disturbances to an acceptable level.

EXAMPLE 6 Performing sensor coverage analysis and optimizing the selection of sensors (type, technology, quantity) and their relative positioning in the vehicle.

— sensor blockage detection and cleaning methods;

EXAMPLE 7 Detecting dirt on a camera using edge detection and cleaning it with fluid and wipers.

2) increased actuator performance and/or accuracy by improving the actuator technology (e.g. increase accuracy, extend or limit range of output, reduce response times, repeatability, arbitrate authority capability, utilize other functions to assist or add a new actuator to assist);

3) increased performance and/or accuracy of the recognition and decision algorithms by algorithmic modifications;

EXAMPLE 8 Improved sensor recognition algorithm [e.g. improve a feature descriptor for detecting objects in camera images, such as HOG (histograms of oriented gradients)].

EXAMPLE 9 Consider additional input information in the model.

EXAMPLE 10 Improve the algorithm to provide better robustness, better precision (e.g. switch from a linear to a non-linear model or use machine learning) (see D.2).

EXAMPLE 11 Speed up image processing with enhanced computing power (e.g. using a machine learning accelerator or operation-efficient hardware).

EXAMPLE 12 Recognition of exiting ODD[2] (e.g. approach to the exit ramp on a motorway).

EXAMPLE 13 Recognition of a known unsupported environmental condition (e.g. predict encounters with the sun glare based on geography, time of day, season, etc.).

NOTE Hardware performance improvement can be considered when implementing advanced algorithms.

4) increasing conspicuousness of the ego vehicle to enhance the controllability of other traffic participants in case of hazardous behaviour of the ego vehicle.

EXAMPLE 14 Installation of retro-reflectors, turning-on fog lights, turn indicators, active sounds, etc., as long as they are permitted by local regulations.

8.3.3 Functional restrictions

Measures for functional restriction are aimed at maintaining a partial functionality by degrading (or limiting) the intended functionality. These measures can include, but are not limited to:

1) restriction of the intended functionality for specific use cases;

EXAMPLE 1 Lane keeping assist functionality restricts the steering assist torque to avoid an undesired steering intervention when lane detection devices cannot clearly detect the lane.

EXAMPLE 2 Limitation of the ODD including environmental, geographical or time-of-day restrictions.

EXAMPLE 3 Restrict or constrain the driving policy (see D.1) to ensure safety of decision making.

EXAMPLE 4 Camera blinded by reflection of surrounding light caused by the afternoon sun; operation continues with restricted authority (e.g. reduced allowed maximum vehicle speed, limiting the maximal steering torque applied by a lane keep assist function) using radar and other sensors.

2) removal of authority for the intended functionality for specific use cases.

© ISO 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21448:2022