
Road vehicles — Safety of the intended functionality

Véhicules routiers — Sécurité de la fonction attendue



This document is a preview generated by EUS



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

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

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

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.

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).

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.

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	Specific standards
	EXAMPLE Eye damage from the beam of a lidar.	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

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*