DRAFT INTERNATIONAL STANDARD
ISO/DIS 21448

ISO/TC **22**/SC **32** Secretariat: **JISC**

Voting begins on:
2021-01-20

Voting terminates on:
2021-04-14

Road vehicles — Safety of the intended functionality

Véhicules routiers — Sécurité de la fonction attendue

ICS: 43.040.10

This document is circulated as received from the committee secretariat.

Reference number
ISO/DIS 21448:2021(E)

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

Published in Switzerland

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland.

Contents

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. 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. 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 on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC22/SC32/WG8

ISO 21448 consists of this document only.

Introduction

The safety of road vehicles during their operation phase is of paramount concern for the road vehicles industry. The number of advanced 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 avoidance of unreasonable risk caused by every hazard associated with the intended functionality and its implementation, especially those hazards not due to failures, but due to insufficiencies of specification or performance limitations.

For the achievement of functional safety (FuSa), ISO 26262-1 defines the functional safety as the absence of unreasonable risk due to hazards caused by malfunctioning behaviour of the E/E system. ISO 26262-3 defines how to develop a Hazard Analysis and Risk Assessment (HARA) to determine vehicle level hazards. The HARA evaluates the potential risks due to malfunctioning behaviour of the item to determine top-level safety requirements, i.e. the safety goals, necessary to mitigate the risks. The other parts of the ISO 26262 series provide requirements and recommendations to avoid and control random hardware failures and systematic failures that could violate safety goals.

For some E/E systems, which rely on sensing the external or internal environment to build situational awareness, there can be potentially hazardous behaviour caused by the intended functionality, 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.

This also applies to functions, systems or algorithms that use machine learning. The absence of unreasonable risk due to these potentially hazardous behaviours related to these functional insufficiencies is defined as the safety of the intended functionality (SOTIF). Functional safety (addressed by the ISO 26262 series) and SOTIF are distinct and complementary aspects of safety.

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

- the specification and design phase;

  EXAMPLE Modification of vehicle functionality or of sensor performance requirements, driven by identified system limitations or by previously unknown hazardous scenarios.

- the verification phase;

  EXAMPLE 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.

- the validation phase;

  EXAMPLE Long-term vehicle test, simulation-based testing.

- the operation phase;

  EXAMPLE Field monitoring of SOTIF incidents.

In many instances, triggering conditions are necessary to cause a potentially hazardous behaviour. In addition, triggering conditions include reasonably foreseeable direct misuse. 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.

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

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

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

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

EXAMPLE By opening the door, the user unintentionally obstructs a sensor's field of view.

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

Ensuring compliance with local driving laws, policies, or road norms is out of scope of this document, except in the case where not following laws and rules of the road could lead to safety hazards.

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.

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 ISO26262. Specifically, ISO 26262 assumes that the intended functionality is safe, and addresses E/E system faults that can cause hazardous behaviour due to a deviation from the intended functionality. The requirements elicitation process for the system and its elements can include aspects of both standards.

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

For a more detailed description of the articulation between ISO 26262 and this document, please refer to Annex A.2.

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	**Cause of hazardous events**	**Within scope of**
System	E/E System failures	ISO 26262
	Insufficiencies of specification, performance limitations or insufficient situational awareness, with or without reasonably foreseeable misuse	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]
	system technologies EXAMPLE: Eye damage from a laser sensor	Specific standards
External factor	Reasonably foreseeable misuse	This document
	Attack exploiting vehicle security vulnerabilities	ISO/SAE 21434 or SAE J3061
	Impact from active infrastructure and/or vehicle to vehicle communication, and external systems	This document ISO 20077; ISO 26262
	Impact from vehicle surroundings (e.g. other users, passive infrastructure, weather, Electro-Magnetic Interference)	This document ISO 26262

Road vehicles — Safety of the intended functionality

1 Scope

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

a. the insufficiencies of specification of the intended functionality at the vehicle level, or
b. the insufficiencies of specification or performance limitations in the implementation of E/E elements in the system

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

These hazards can be triggered by specific conditions of a scenario, including reasonably foreseeable misuse of the intended functionality or in combination with other functions at the vehicle level (e.g. activation of the parking brake while the automated driving function is active).

NOTE Information provided by the infrastructure (e.g. Car2x communication, maps) is also part of the evaluation of functional insufficiencies if it can have an impact on the SOTIF.

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

This document is applicable to an intended functionality where proper situational awareness is essential to safety and where such situational awareness is derived from complex sensors and processing algorithms, especially emergency intervention systems and systems having automation levels from 1 to 5.

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

This document does not apply to faults covered by the ISO 26262 series.

This document does not apply to hazards directly caused by the system technology (e.g. eye damage from a laser sensor).

This document does not address hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy and similar hazards, unless directly caused by the intended functionality of safety-related E/E systems.

This document does not apply to attacks exploiting vehicle security vulnerabilities.

This document considers local driving laws, policies, or road norms only as far as they can impact the SOTIF, specifically where not following laws and rules of the road could lead to safety hazards. However, this document does not address legal compliance to driving laws and/or policies.

Furthermore, functions of existing systems for which well-established and well-trusted design, verification and validation (V&V) measures exist (e.g. Dynamic Stability Control (DSC) systems, airbag) are exempt from the scope of this document.

EXAMPLE a system for which there is an existing standard sufficient to ensure safety

Some measures described in this document are applicable to newly designed functions or elements of existing systems, if situational awareness derived from complex sensors and processing algorithms is part of the design.

EXAMPLE Complex sensing and fusion of the road and cabin environment might replace current accelerometer (or similar) based triggering mechanisms for airbags. SOTIF activities can be relevant, due to that change requiring situational awareness.

Reasonably foreseeable misuse, which could lead directly to potentially hazardous behaviour, is in the scope of this document as a possible triggering condition. This is defined as “reasonably foreseeable direct misuse”.

Reasonably foreseeable misuse that prevents controllability by the driver of the system’s hazardous behaviour, representing an unreasonable level of risk, is in scope of this document. This is defined as “reasonably foreseeable indirect misuse”.

An intentional action that clearly violates the system’s intended use is considered feature abuse. This is out of scope of this document.

EXAMPLE: Applying a substitute hand to fool a “hands on wheel” detection safety measure.

2 Normative references

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

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

3 Terms and definitions

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

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

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

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

3.1
acceptance criterion
criterion representing the absence of an unreasonable level of risk

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, ALARP, etc.

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 (**3.26**)

Note 1 to entry: The temporal sequence of actions/events (**3.7**) and scenes (**3.26**) specify a scenario (**3.25**).

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 system or any element in interaction with the considered function.

3.3

driving policy

strategy and rules defining acceptable control actions (**3.2**) at 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 OEDR (**3.20**);
- Manoeuvre planning (tactical); and
- Enhancing conspicuity via lighting, signalling and gesturing, etc. (tactical).

[SOURCE: SAE J3016 [4], modified definition to provide an ISO conformant text with the same intent]

3.5

DDT fallback

response by the driver or automation system to either perform the DDT (**3.4**) or transition to a minimal risk condition (**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 ODD (**3.21**) exit or a sensor blocked by ice can lead to hazardous behaviour.

[SOURCE: SAE J3016 [4], modified definition to provide an ISO conformant text with the same intent]

3.6

ego vehicle

vehicle fitted with functionality that is being analysed for SOTIF (**3.24**)

3.7

event

occurrence at a point in time

Note 1 to entry: The temporal sequence of actions/events (**3.7**) and scenes (**3.26**) specify a scenario (**3.25**).

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 limitation (**3.23**)

Note 1 to entry: Functional insufficiencies include the insufficiencies of specification (**3.12**) of the intended functionality (**3.14**) at the vehicle level, or the insufficiencies of specification (**3.12**) or performance limitations (**3.23**) of the system elements.

Note 2 to entry: SOTIF (**3.24**) activities include the identification of functional insufficiencies and the evaluation of their effects. Functional insufficiencies lead to hazardous behaviours by definition (see **3.12** and **3.23**). The term "potential functional insufficiency" can be used in the document when the ability to lead to hazardous behaviour is not yet established.

3.9

functional modification

alteration of a functional specification

Note 1 to entry: Functional modification is not the same as the modification defined in ISO 26262.

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

[SOURCE: SAE J3016 [4], modified definition to provide an ISO conformant text with the same intent]

3.11

hazard

potential source of harm caused by the hazardous behaviour of the system

3.12

insufficiency of specification

specification, possibly incomplete, leading to hazardous behaviour in combination with one or more triggering conditions (**3.29**)

EXAMPLE 1 A scenario (**3.25**) where the driving function in control of the ego vehicle (**3.6**) is not keeping a safe distance to the vehicle in front can result from an insufficiency of specification.

EXAMPLE 2 System inability to handle uncommon road signs due to specification gaps

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

Note 2 to entry: SOTIF (**3.24**) activities include the identification of insufficiencies of specification and the evaluation of their effects, possibly leading to hazardous behaviour. The term "potential insufficiency of specification" can be used in the document when the ability to lead to hazardous behaviour is not yet established.

Note 3 to entry: Safety 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 (**3.24**)) may be included in formal databases to support assurance of verification. These requirements may not be designated as the "specification" in many organizations but are necessary to ensure the SOTIF (**3.24**). The usage of the term "insufficiency (insufficiencies) of specification" in this standard includes such derived requirements.