BS ISO 21448:2022

BSI Standards Publication

Road vehicles — Safety of the intended functionality

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 It supersedes PD ISO/PAS 21448:2019, which is withdrawn.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.

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

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)

Contents

Page

Foreword

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

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

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

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

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

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

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 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