PD ISO/PAS 21448:2019

BSI Standards Publication

Road vehicles — Safety of the intended functionality

urrently in preview, click buy full versi

bsi.

National foreword

This Published Document is the UK implementation of ISO/PAS 21448:2019.

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 secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2019
Published by BSI Standards Limited 2019

ISBN 978 0 580 94502 1

ICS 43.040.10

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

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 January 2019.

Amendments/corrigenda issued since publication

Date	Text affected

urrently in preview, click buy full versi

PD ISO/PAS 21448:2019

PUBLICLY AVAILABLE SPECIFICATION

ISO/PAS 21448

First edition
2019-01

Road vehicles — Safety of the intended functionality

Véhicules routiers - Sécurité de la fonctionnalité attendue

Reference number
ISO/PAS 21448:2019(E)

© ISO 2019

urrently in preview, click buy full versi

urrently in preview, click buy full versi

COPYRIGHT PROTECTED DOCUMENT

© ISO 2019

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
Fax: +41 22 749 09 47
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 **1**
4 Overview of this document's activities in the development process **6**
5 Functional and system specification (intended functionality content) **11**
5.1 Objectives 11
5.2 Functional description 11
5.3 Consideration on system design and architecture 12
6 Identification and Evaluation of hazards caused by the intended functionality **13**
6.1 Objectives 13
6.2 Hazard identification 14
6.3 Hazard analysis 15
6.4 Risk evaluation of the intended function 16
6.5 Specification of a validation target 16
7 Identification and Evaluation of triggering events **17**
7.1 Objectives 17
7.2 Analysis of triggering events 17
7.2.1 Triggering events related to algorithm 17
7.2.2 Triggering events related to sensors and actuators 18
7.3 Acceptability of the triggering events 19
8 Functional modifications to reduce SOTIF related risks **19**
8.1 Objectives 19
8.2 General 19
8.3 Measures to improve the SOTIF 20
8.4 Updating the system specification 22
9 Definition of the verification and validation strategy **22**
9.1 Objectives 22
9.2 Planning and specification of integration and testing 23
10 Verification of the SOTIF (Area 2) **23**
10.1 Objectives 23
10.2 Sensor verification 24
10.3 Decision algorithm verification 24
10.4 Actuation verification 25
10.5 Integrated system verification 25
11 Validation of the SOTIF (Area 3) **26**
11.1 Objectives 26
11.2 Evaluation of residual risk 26
11.3 Validation test parameters 26
12 Methodology and criteria for SOTIF release **27**
12.1 Objectives 27
12.2 Methodology for evaluating SOTIF for release 27
12.3 Criteria for SOTIF release 28
Annex A (informative) **Examples of the application of SOTIF activities** **30**
Annex B (informative) **Example for definition and validation of an acceptable false alarm rate in AEB systems** **33**
Annex C (informative) **Validation of SOTIF applicable systems** **41**

urrently in preview, click buy full versi

© ISO 2019 – All rights reserved

Annex D (informative) **Automotive perception systems verification and validation** 43
Annex E (informative) **Method for deriving SOTIF misuse scenarios** 46
Annex F (informative) **Example construction of scenario for SOTIF safety analysis method** 49
Annex G (informative) **Implications for off-line training** 52
Bibliography 54

urrently in preview, click buy full versi

© ISO 2019 – All rights reserved

Foreword

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

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

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

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

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

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

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Currently in preview, click buy full version

Introduction

The safety of road vehicles during their operation phase is of paramount concern for the road vehicles industry. Recent years have seen a large increase in the number of advanced functionalities included in vehicles. These rely on sensing, processing of complex algorithms and actuation implemented by electrical and/or electronic (E/E) systems.

An acceptable level of safety for road vehicles requires the avoidance of unreasonable risk caused by every hazard associated with the intended functionality and its implementation, especially those not due to failures, e.g. due to performance limitations. ISO 26262-1 defines the vehicle safety as the absence of unreasonable risks that arise from malfunctions of the E/E system. ISO 26262-3 specifies a Hazard Analysis and Risk Assessment to determine vehicle level hazards. This evaluates the potential risks due to malfunctioning behaviour of the item and enables the definition of top-level safety requirements i.e. the safety goals, necessary to mitigate the risks. The other parts of the ISO 26262 series provide requirements and recommendations to avoid and control random hardware failures and systematic failures that could violate safety goals.

For some systems, which rely on sensing the external or internal environment, there can be potentially hazardous behaviour caused by the intended functionality or performance limitation of a system that is free from the faults addressed in the ISO 26262 series. Examples of such limitations include:

— The inability of the function to correctly comprehend the situation and operate safely; this also includes functions that use machine learning algorithms;

— Insufficient robustness of the function with respect to sensor input variations or diverse environmental conditions.

The absence of unreasonable risk due to these potentially hazardous behaviours related to such limitations is defined as the safety of the intended functionality (SOTIF). Functional safety (addressed by the ISO 26262 series) and SOTIF are distinct and complementary aspects of safety.

To address the SOTIF, activities are implemented during the following phases:

— Measures in the design phase;

EXAMPLE Requirement on sensor performance.

— Measures in the verification phase;

EXAMPLE Technical Review, test cases with a high coverage of relevant scenarios, injection of potential triggering events, in the loop testing (e.g. SIL/HIL/MIL) of selected SOTIF are relevant use cases.

— Measures in the Validation phase.

EXAMPLE Long term vehicle test, simulations.

A proper understanding of the function by the user, its behaviour and its limitations (including the human/machine interface) is the key to ensuring safety.

In many instances, a triggering event is necessary to cause a potentially hazardous behaviour; hence the importance of analysing hazards in the context of particular use cases.

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

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

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

urrently in preview, click buy full versi

 © ISO 2019 – All rights reserved

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

It is assumed that the E/E random hardware faults and systematic faults of the E/E system are addressed using the ISO 26262 series. The activities mentioned in this document are complementary to those given in the ISO 26262 series.

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

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

Source	Cause of hazardous event	Within scope of
System	E/E System failures	ISO 26262 series
	Performance limitations or insufficient situational awareness, with or without reasonably foreseeable misuse	ISO/PAS 21448
	Reasonably foreseeable misuse, incorrect HMI (e.g. user confusion, user overload)	ISO/PAS 21448 ISO 26262 series European statement of principal on the design of human-machine-interface
	Hazards caused by the system technology	Specific standards
External factor	successful attack exploiting vehicle security vulnerabilities	ISO 21434[a] or SAE J3061
	Impact from active Infrastructure and/or vehicle to vehicle communication, external devices and cloud services.	ISO 20077 series; ISO 26262 series
	Impact from car surroundings (other users, “passive” infrastructure, environmental conditions: weather, Electro Magnetic Interference…)	ISO/PAS 21448 ISO 26262 series
[a] Under preparation. Stage at the time of publication: ISO/SAE CD 21434.		

NOTE Options for automated driving level definitions (from NHTSA, SAE and OICA, etc.) are discussed in the ITS-Informal Group ECE/TRANS/WP.29.

urrently in preview, click buy full versi

urrently in preview, click buy full versi

Road vehicles — Safety of the intended functionality

1 Scope

The absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or by reasonably foreseeable misuse by persons is referred to as the Safety Of The Intended Functionality (SOTIF). This document provides guidance on the applicable design, verification and validation measures needed to achieve the SOTIF. This document does not apply to faults covered by the ISO 26262 series or to hazards directly caused by the system technology (e.g. eye damage from a laser sensor).

This document is intended to be applied to intended functionality where proper situational awareness is critical to safety, and where that situational awareness is derived from complex sensors and processing algorithms; especially emergency intervention systems (e.g. emergency braking systems) and Advanced Driver Assistance Systems (ADAS) with levels 1 and 2 on the OICA/SAE standard J3016 automation scales. This edition of the document can be considered for higher levels of automation, however additional measures might be necessary. This document is not intended for functions of existing systems for which well-established and well-trusted design, verification and validation (V&V) measures exist at the time of publication (e.g. Dynamic Stability Control (DSC) systems, airbag, etc.). Some measures described in this document are applicable to innovative functions of such systems, if situational awareness derived from complex sensors and processing algorithms is part of the innovation.

Intended use and reasonably foreseeable misuse are considered in combination with potentially hazardous system behaviour when identifying hazardous events.

Reasonably foreseeable misuse, which could lead directly to potentially hazardous system behaviour, is also considered as a possible event that could directly trigger a SOTIF-related hazardous event.

Intentional alteration to the system operation is considered feature abuse. Feature abuse is not in scope of this document.

2 Normative references

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

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

3 Terms and definitions

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

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

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

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

© ISO 2019 – All rights reserved