BS ISO 26262-3:2018

BSI Standards Publication

Road vehicles — Functional safety

Part 3: Concept phase

Documents
Document Sharing Hub

Full document details: BS ISO 26262-3:2018

National foreword

This British Standard is the UK implementation of ISO 26262-3:2018. It supersedes BS ISO 26262-3:2011, which is withdrawn.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 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 2018
Published by BSI Standards Limited 2018

ISBN 978 0 580 89511 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 December 2018.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO 26262-3:2018

INTERNATIONAL STANDARD

ISO 26262-3

Second edition
2018-12

Road vehicles — Functional safety —

Part 3: Concept phase

Véhicules routiers — Sécurité fonctionnelle —

Partie 3: Phase de projet

Reference number
ISO 26262-3:2018(E)

Documents
Document Sharing Hub

© ISO 2018

Full document details: BS ISO 26262-3:2018

COPYRIGHT PROTECTED DOCUMENT

© ISO 2018

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

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO 26262-3:2018

Contents

Page

Foreword ... **iv**
Introduction ... **vi**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **2**
4 Requirements for compliance ... **2**
4.1 Purpose ... 2
4.2 General requirements ... 2
4.3 Interpretations of tables ... 3
4.4 ASIL-dependent requirements and recommendations ... 3
4.5 Adaptation for motorcycles ... 3
4.6 Adaptation for trucks, buses, trailers and semi-trailers ... 3
5 Item definition ... **4**
5.1 Objectives ... 4
5.2 General ... 4
5.3 Inputs to this clause ... 4
5.3.1 Prerequisites ... 4
5.3.2 Further supporting information ... 4
5.4 Requirements and recommendations ... 4
5.5 Work products ... 5
6 Hazard analysis and risk assessment ... **5**
6.1 Objectives ... 5
6.2 General ... 5
6.3 Inputs to this clause ... 6
6.3.1 Prerequisites ... 6
6.3.2 Further supporting information ... 6
6.4 Requirements and recommendations ... 6
6.4.1 Initiation of the hazard analysis and risk assessment ... 6
6.4.2 Situation analysis and hazard identification ... 6
6.4.3 Classification of hazardous events ... 7
6.4.4 Determination of safety goals ... 10
6.4.5 Management of variances of T&B in hazard analysis and risk assessment ... 11
6.4.6 Verification ... 12
6.5 Work products ... 12
7 Functional safety concept ... **12**
7.1 Objectives ... 12
7.2 General ... 13
7.3 Inputs to this clause ... 13
7.3.1 Prerequisites ... 13
7.3.2 Further supporting information ... 13
7.4 Requirements and recommendations ... 14
7.4.1 General ... 14
7.4.2 Derivation of functional safety requirements ... 14
7.4.3 Safety validation criteria ... 16
7.4.4 Verification of the functional safety concept ... 16
7.5 Work products ... 17
Annex A (informative) **Overview of and workflow of concept phase** ... **18**
Annex B (informative) **Hazard analysis and risk assessment** ... **19**
Bibliography ... **28**

Documents
Document Sharing Hub

© ISO 2018 – All rights reserved

Full document details: BS ISO 26262-3:2018

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 on 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 the following URL: 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 edition of ISO 26262 series of standards cancels and replaces the edition ISO 26262:2011 series of standards, which has been technically revised and includes the following main changes:

— requirements for trucks, buses, trailers and semi-trailers;

— extension of the vocabulary;

— more detailed objectives;

— objective oriented confirmation measures;

— management of safety anomalies;

— references to cyber-security;

— updated target values for hardware architecture metrics;

— guidance on model based development and software safety analysis;

— evaluation of hardware elements;

— additional guidance on dependent failure analysis;

— guidance on fault tolerance, safety related special characteristics and software tools;

— guidance for semiconductors;

— requirements for motorcycles; and

— general restructuring of all parts for improved clarity.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-3:2018

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.

A list of all parts in the ISO 26262 series can be found on the ISO website.

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-3:2018

Introduction

The ISO 26262 series of standards is the adaptation of IEC 61508 series of standards to address the sector specific needs of electrical and/or electronic (E/E) systems within road vehicles.

This adaptation applies to all activities during the safety lifecycle of safety-related systems comprised of electrical, electronic and software components.

Safety is one of the key issues in the development of road vehicles. Development and integration of automotive functionalities strengthen the need for functional safety and the need to provide evidence that functional safety objectives are satisfied.

With the trend of increasing technological complexity, software content and mechatronic implementation, there are increasing risks from systematic failures and random hardware failures, these being considered within the scope of functional safety. ISO 26262 series of standards includes guidance to mitigate these risks by providing appropriate requirements and processes.

To achieve functional safety, the ISO 26262 series of standards:

a) provides a reference for the automotive safety lifecycle and supports the tailoring of the activities to be performed during the lifecycle phases, i.e., development, production, operation, service and decommissioning;

b) provides an automotive-specific risk-based approach to determine integrity levels [Automotive Safety Integrity Levels (ASILs)];

c) uses ASILs to specify which of the requirements of ISO 26262 are applicable to avoid unreasonable residual risk;

d) provides requirements for functional safety management, design, implementation, verification, validation and confirmation measures; and

e) provides requirements for relations between customers and suppliers.

The ISO 26262 series of standards is concerned with functional safety of E/E systems that is achieved through safety measures including safety mechanisms. It also provides a framework within which safety-related systems based on other technologies (e.g. mechanical, hydraulic and pneumatic) can be considered.

The achievement of functional safety is influenced by the development process (including such activities as requirements specification, design, implementation, integration, verification, validation and configuration), the production and service processes and the management processes.

Safety is intertwined with common function-oriented and quality-oriented activities and work products. The ISO 26262 series of standards addresses the safety-related aspects of these activities and work products.

Figure 1 shows the overall structure of the ISO 26262 series of standards. The ISO 26262 series of standards is based upon a V-model as a reference process model for the different phases of product development. Within the figure:

— the shaded “V”s represent the interconnection among ISO 26262-3, ISO 26262-4, ISO 26262-5, ISO 26262-6 and ISO 26262-7;

— for motorcycles:

  — ISO 26262-12:2018, Clause 8 supports ISO 26262-3;

  — ISO 26262-12:2018, Clauses 9 and 10 support ISO 26262-4;

— the specific clauses are indicated in the following manner: “m-n”, where “m” represents the number of the particular part and “n” indicates the number of the clause within that part.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-3:2018

EXAMPLE "2-6" represents ISO 26262-2:2018, Clause 6.

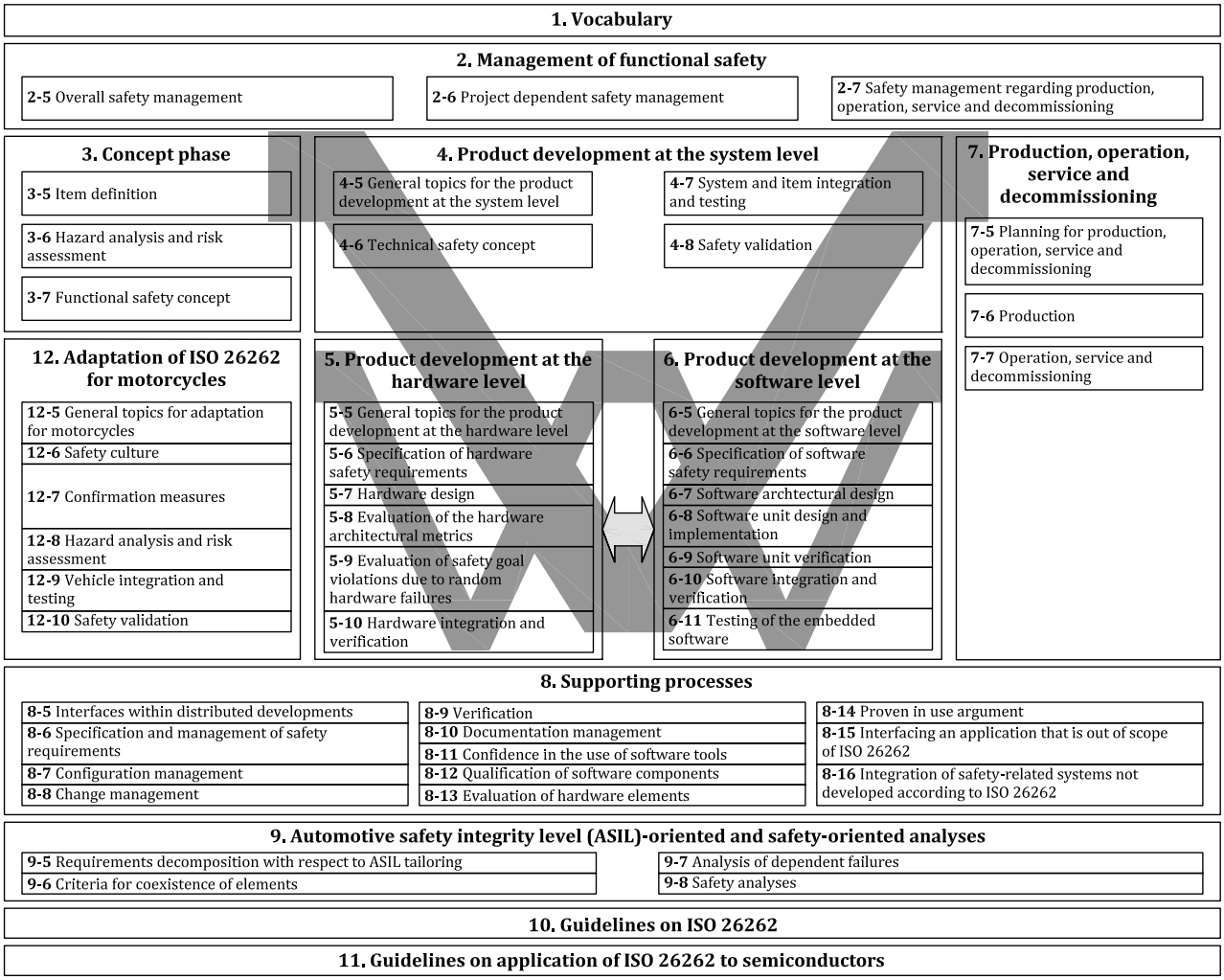

Figure 1 — Overview of the ISO 26262 series of standards

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-3:2018

Documents
Document Sharing Hub

Full document details: BS ISO 26262-3:2018

Road vehicles — Functional safety —

Part 3:
Concept phase

1 Scope

This document is intended to be applied to safety-related systems 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 address unique E/E systems in special vehicles such as E/E systems designed for drivers with disabilities.

NOTE Other dedicated application-specific safety standards exist and can complement the ISO 26262 series of standards or vice versa.

Systems and their components released for production, or systems and their components already under development prior to the publication date of this document, are exempted from the scope of this edition. This document addresses alterations to existing systems and their components released for production prior to the publication of this document by tailoring the safety lifecycle depending on the alteration. This document addresses integration of existing systems not developed according to this document and systems developed according to this document by tailoring the safety lifecycle.

This document addresses possible hazards caused by malfunctioning behaviour of safety-related E/E systems, including interaction of these systems. It 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 malfunctioning behaviour of safety-related E/E systems.

This document describes a framework for functional safety to assist the development of safety-related E/E systems. This framework is intended to be used to integrate functional safety activities into a company-specific development framework. Some requirements have a clear technical focus to implement functional safety into a product; others address the development process and can therefore be seen as process requirements in order to demonstrate the capability of an organization with respect to functional safety.

This document does not address the nominal performance of E/E systems.

This document specifies the requirements for the concept phase for automotive applications, including the following:

— item definition;

— hazard analysis and risk assessment; and

— functional safety concept.

Annex A provides an overview on objectives, prerequisites and work products 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, *Road Vehicles — Functional Safety — Part 1: Vocabulary*

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-3:2018

ISO 26262-2:2018, *Road Vehicles — Functional Safety — Part 2: Management of functional safety*

ISO 26262-4:2018, *Road vehicles — Functional safety — Part 4: Product development at the system level*

ISO 26262-8:2018, *Road vehicles — Functional safety — Part 8: Supporting processes*

ISO 26262-9:2018, *Road vehicles — Functional safety — Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses*

3 Terms and definitions

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

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

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

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

4 Requirements for compliance

4.1 Purpose

This clause describes how:

a) to achieve compliance with the ISO 26262 series of standards;

b) to interpret the tables used in the ISO 26262 series of standards; and

c) to interpret the applicability of each clause, depending on the relevant ASIL(s).

4.2 General requirements

When claiming compliance with the ISO 26262 series of standards, each requirement shall be met, unless one of the following applies:

a) tailoring of the safety activities in accordance with ISO 26262-2 has been performed that shows that the requirement does not apply; or

b) a rationale is available that the non-compliance is acceptable and the rationale has been evaluated in accordance with ISO 26262-2.

Informative content, including notes and examples, is only for guidance in understanding, or for clarification of the associated requirement, and shall not be interpreted as a requirement itself or as complete or exhaustive.

The results of safety activities are given as work products. “Prerequisites” are information which shall be available as work products of a previous phase. Given that certain requirements of a clause are ASIL-dependent or may be tailored, certain work products may not be needed as prerequisites.

“Further supporting information” is information that can be considered, but which in some cases is not required by the ISO 26262 series of standards as a work product of a previous phase and which may be made available by external sources that are different from the persons or organizations responsible for the functional safety activities.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-3:2018