BS ISO 26262-5:2018

BSI Standards Publication

Road vehicles — Functional safety

Part 5: Product development at the hardware level

Documents
Document Sharing Hub

Full document details: BS ISO 26262-5:2018

National foreword

This British Standard is the UK implementation of ISO 26262-5:2018. It supersedes BS ISO 26262-5:2011, which is withdrawn.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 89513 5

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 26262-5:2018

INTERNATIONAL STANDARD

ISO 26262-5

Second edition
2018-12-18

Road vehicles — Functional safety —

Part 5: Product development at the hardware level

Véhicules routiers — Sécurité fonctionnelle —

Partie 5: Développement du produit au niveau du matériel

Reference number
ISO 26262-5:2018(E)

Documents
Document Sharing Hub

© ISO 2018

Full document details: BS ISO 26262-5:2018

COPYRIGHT PROTECTED DOCUMENT

© ISO 2018, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO 26262-5:2018

Contents

Page

Foreword ... **v**
Introduction ... **vii**
1 Scope ... **1**
2 Normative references ... **2**
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 ... 4
5 General topics for the product development at the hardware level ... **4**
5.1 Objectives ... 4
5.2 General ... 4
6 Specification of hardware safety requirements ... **5**
6.1 Objectives ... 5
6.2 General ... 6
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
6.5 Work products ... 8
7 Hardware design ... **8**
7.1 Objectives ... 8
7.2 General ... 9
7.3 Inputs to this clause ... 9
7.3.1 Prerequisites ... 9
7.3.2 Further supporting information ... 9
7.4 Requirements and recommendations ... 9
7.4.1 Hardware architectural design ... 9
7.4.2 Hardware detailed design ... 10
7.4.3 Safety analyses ... 11
7.4.4 Verification of hardware design ... 13
7.4.5 Production, operation, service and decommissioning ... 13
7.5 Work products ... 14
8 Evaluation of the hardware architectural metrics ... **14**
8.1 Objectives ... 14
8.2 General ... 14
8.3 Inputs of this clause ... 15
8.3.1 Prerequisites ... 15
8.3.2 Further supporting information ... 15
8.4 Requirements and recommendations ... 16
8.5 Work products ... 19
9 Evaluation of safety goal violations due to random hardware failures ... **20**
9.1 Objectives ... 20
9.2 General ... 20
9.3 Inputs to this clause ... 20
9.3.1 Prerequisites ... 20
9.3.2 Further supporting information ... 20
9.4 Requirements and recommendations ... 21

AVA Documents
Document Sharing Hub

© ISO 2018 – All rights reserved

Full document details: BS ISO 26262-5:2018

9.4.1 General ... 21
9.4.2 Evaluation of Probabilistic Metric for random Hardware Failures (PMHF) ... 22
9.4.3 Evaluation of Each Cause of safety goal violation (EEC) ... 24
9.4.4 Verification review ... 29
9.5 Work products ... 30

10 Hardware integration and verification ... 30
10.1 Objectives ... 30
10.2 General ... 30
10.3 Inputs of this clause ... 30
10.3.1 Prerequisites ... 30
10.3.2 Further supporting information ... 30
10.4 Requirements and recommendations ... 30
10.5 Work products ... 32

Annex A (informative) **Overview of and workflow of product development at the hardware level ... 33**

Annex B (informative) **Failure mode classification of a hardware element ... 36**

Annex C (normative) **Hardware architectural metrics ... 38**

Annex D (informative) **Evaluation of the diagnostic coverage ... 44**

Annex E (informative) **Example calculation of hardware architectural metrics:"single-point fault metric" and "latent-fault metric" ... 66**

Annex F (informative) **Example for rationale that objectives of Clause 9 in accordance with 4.2 are met ... 75**

Annex G (informative) **Example of a PMHF budget assignment for an item consisting of two systems ... 82**

Annex H (informative) **Example of latent fault handling ... 86**

Bibliography ... 89

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-5:2018

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 26262-5:2018

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 26262-5:2018

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.

AVA Documents
Document Sharing Hub

© ISO 2018 – All rights reserved

Full document details: BS ISO 26262-5:2018

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

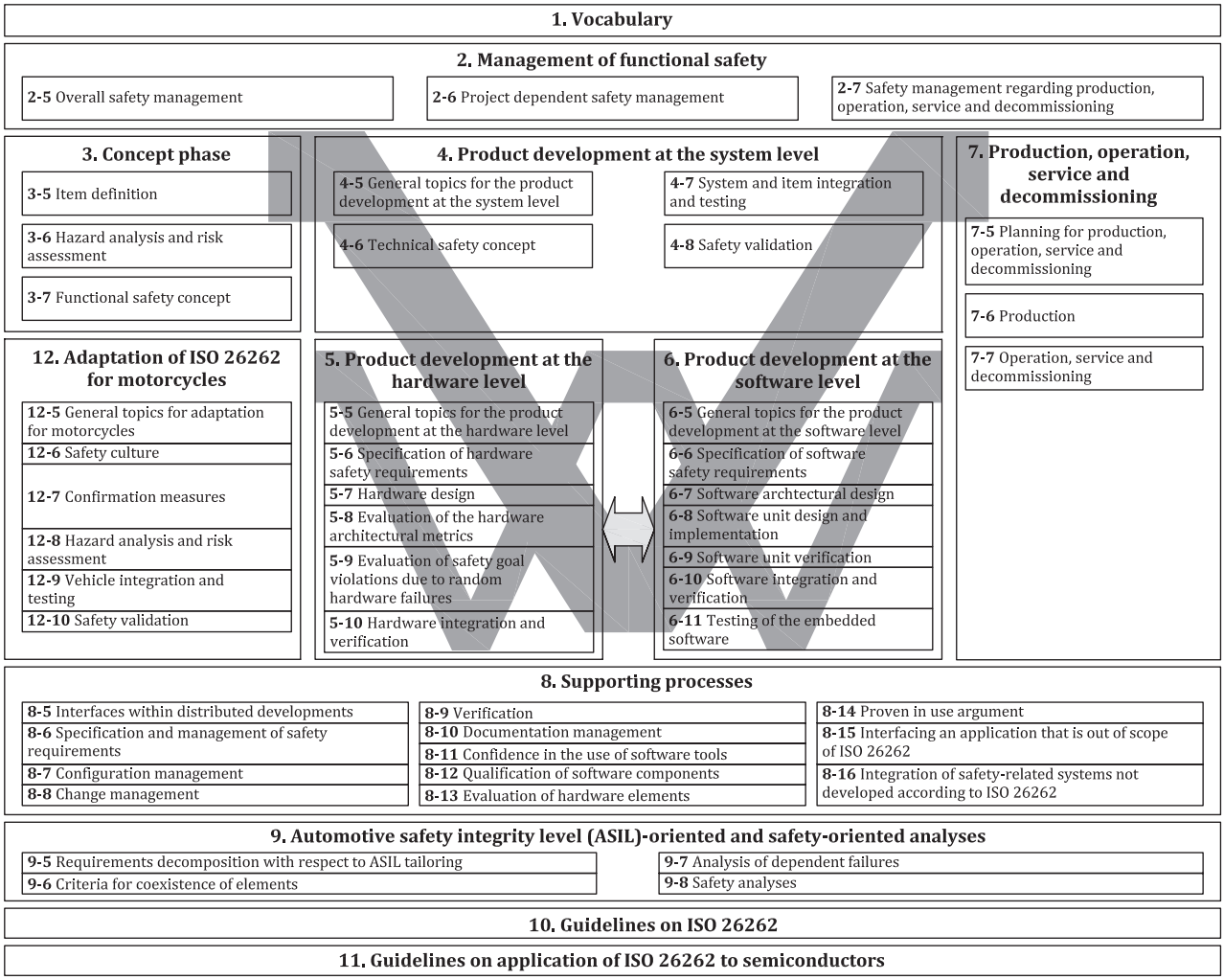


Figure 1 — Overview of the ISO 26262 series of standards

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-5:2018

INTERNATIONAL STANDARD **ISO 26262-5:2018**

Road vehicles — Functional safety —

Part 5: Product development at the hardware level

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 product development at the hardware level for automotive applications, including the following:

— general topics for the product development at the hardware level;

— specification of hardware safety requirements;

— hardware design;

— evaluation of the hardware architectural metrics;

— evaluation of safety goal violations due to random hardware failures; and

— hardware integration and verification.

The requirements of this document for hardware elements are applicable to both non-programmable and programmable elements, such as ASIC, FPGA and PLD. Further guidelines can be found in ISO 26262-10:2018 and ISO 26262-11:2018.

Annex A provides an overview on objectives, prerequisites and work products of this document.

AVA Documents
Document Sharing Hub

© ISO 2018 – All rights reserved

Full document details: BS ISO 26262-5:2018

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 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 26262-6:2018, *Road vehicles — Functional safety — Part 6: Product development at the software level*

ISO 26262-7:2018, *Road vehicles — Functional safety — Part 7: Production and operation*

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 26262-1:2018 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.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-5:2018

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.

4.3 Interpretations of tables

Tables are normative or informative depending on their context. The different methods listed in a table contribute to the level of confidence in achieving compliance with the corresponding requirement. Each method in a table is either:

a) a consecutive entry (marked by a sequence number in the leftmost column, e.g. 1, 2, 3), or

b) an alternative entry (marked by a number followed by a letter in the leftmost column, e.g. 2a, 2b, 2c).

For consecutive entries, all listed highly recommended and recommended methods in accordance with the ASIL apply. It is allowed to substitute a highly recommended or recommended method by others not listed in the table, in this case, a rationale shall be given describing why these comply with the corresponding requirement. If a rationale can be given to comply with the corresponding requirement without choosing all entries, a further rationale for omitted methods is not necessary.

For alternative entries, an appropriate combination of methods shall be applied in accordance with the ASIL indicated, independent of whether they are listed in the table or not. If methods are listed with different degrees of recommendation for an ASIL, the methods with the higher recommendation should be preferred. A rationale shall be given that the selected combination of methods or even a selected single method complies with the corresponding requirement.

NOTE A rationale based on the methods listed in the table is sufficient. However, this does not imply a bias for or against methods not listed in the table.

For each method, the degree of recommendation to use the corresponding method depends on the ASIL and is categorized as follows:

— “++” indicates that the method is highly recommended for the identified ASIL;

— “+” indicates that the method is recommended for the identified ASIL; and

— “o” indicates that the method has no recommendation for or against its usage for the identified ASIL.

4.4 ASIL-dependent requirements and recommendations

The requirements or recommendations of each sub-clause shall be met for ASIL A, B, C and D, if not stated otherwise. These requirements and recommendations refer to the ASIL of the safety goal. If ASIL decomposition has been performed at an earlier stage of development, in accordance with ISO 26262-9:2018, Clause 5, the ASIL resulting from the decomposition shall be met.

If an ASIL is given in parentheses in the ISO 26262 series of standards, the corresponding sub-clause shall be considered as a recommendation rather than a requirement for this ASIL. This has no link with the parenthesis notation related to ASIL decomposition.

4.5 Adaptation for motorcycles

For items or elements of motorcycles for which requirements of ISO 26262-12 are applicable, the requirements of ISO 26262-12 supersede the corresponding requirements in this document. Requirements of ISO 26262-2 that are superseded by ISO 26262-12 are defined in Part 12.

Documents
Document Sharing Hub

© ISO 2018 – All rights reserved

Full document details: BS ISO 26262-5:2018

4.6 Adaptation for trucks, buses, trailers and semi-trailers

Content that is intended to be unique for trucks, buses, trailers and semi-trailers (T&B) is indicated as such.

5 General topics for the product development at the hardware level

5.1 Objectives

The objective of this clause is to describe the functional safety activities during the individual sub-phases of hardware development.

5.2 General

The necessary activities and processes needed to develop hardware that meets the safety requirements are planned according to ISO 26262-2:2018, 6.4.6.

Figure 2 illustrates the hardware level product development process steps in order to comply with the requirements of this document, and the integration of these steps within the ISO 26262 framework.

The necessary activities and processes for the product development at the hardware level include:

— the hardware implementation of the technical safety concept;

— the analysis of potential hardware faults and their effects; and

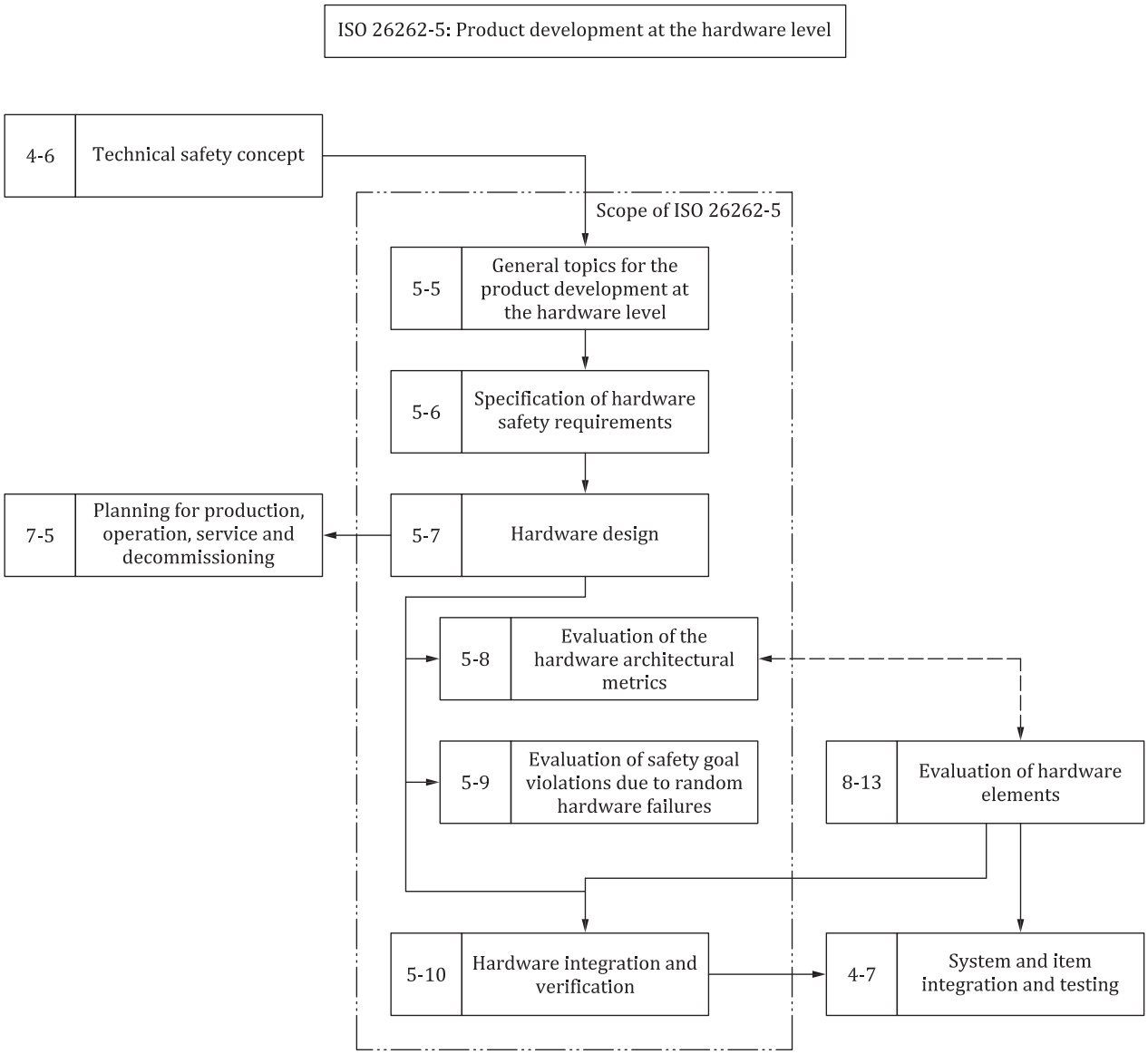
— the coordination with software development.

In contrast to the software development sub-phases, this document contains two clauses describing quantitative evaluations of the overall hardware architecture of the item.

Clause 8 describes two metrics to evaluate the effectiveness of the hardware architecture of the item and the implemented safety mechanisms to cope with random hardware failures.

As a complement to Clause 8, Clause 9 describes two alternative methods to evaluate whether the residual risk of safety goal violations is sufficiently low, either by using a global probabilistic approach (see 9.4.2, PMHF method) or by using a cut-set analysis (see 9.4.3, EEC method) to study the impact of each identified fault of a hardware element upon the violation of the safety goals.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-5:2018



NOTE Within the figure, the specific clauses of each part of ISO 26262 are indicated in the following manner: "m-n", where "m" represents the number of the part and "n" indicates the number of the clause, e.g. "4-7" represents ISO 26262-4:2018, Clause 7.

Figure 2 — Reference phase model for the product development at the hardware level

6 Specification of hardware safety requirements

6.1 Objectives

The objectives of this clause are:

a) to specify the hardware safety requirements. They are derived from the technical safety concept and the system architectural design specification;

b) to refine the hardware-software interface (HSI) specification initiated in ISO 26262-4:2018, 6.4.7; and

c) to verify that the hardware safety requirements and the hardware-software interface (HSI) specification are consistent with the technical safety concept and the system architectural design specification.

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-5:2018

6.2 General

The technical safety requirements are allocated to hardware and software. The requirements that are allocated to both are further partitioned to yield hardware-only safety requirements. The hardware safety requirements are further detailed considering design constraints and the impact of these design constraints on the hardware.

6.3 Inputs to this clause

6.3.1 Prerequisites

The following information shall be available:

— technical safety concept in accordance with ISO 26262-4:2018, 6.5.2;

— system architectural design specification in accordance with ISO 26262-4:2018, 6.5.3; and

— hardware-software interface (HSI) specification in accordance with ISO 26262-4:2018, 6.5.4.

6.3.2 Further supporting information

The following information can be considered:

— software safety requirements specification (see ISO 26262-6:2018, 6.5.1); and

— hardware specifications (from an external source).

6.4 Requirements and recommendations

6.4.1 A hardware safety requirements specification for the hardware elements of the item shall be derived from the technical safety requirements allocated to hardware (resulting from ISO 26262-4:2018, 6.5.2).

6.4.2 The hardware safety requirements specification shall include each hardware requirement that relates to functional safety, including the following:

a) the hardware safety requirements and relevant properties of safety mechanisms to control internal failures of the hardware of the element. These include internal safety mechanisms to cover transient faults when shown to be relevant due to, for instance, the technology used;

EXAMPLE 1 Properties can include the timing and detection abilities of a watchdog.

b) the hardware safety requirements and relevant properties of safety mechanisms to control or tolerate failures external to the element;

EXAMPLE 2 The functional behaviour required for an ECU in the event of an external failure, such as an open-circuit on an input of the ECU.

c) the hardware safety requirements and relevant properties of safety mechanisms to comply with the safety requirements of other elements;

EXAMPLE 3 Diagnosis of sensors or actuators.

d) the hardware safety requirements and relevant properties of safety mechanisms to detect and signal internal or external failures; and

NOTE 1 The hardware safety requirements described in d) include safety mechanisms to prevent faults from being latent.

EXAMPLE 4 The specified fault reaction time interval for the hardware part of a safety mechanism, so as to be consistent with the fault tolerant time interval.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-5:2018

e) the hardware safety requirements not specifying safety mechanisms.

EXAMPLE 5 Examples are:

— requirements on the hardware elements to meet the target values for random hardware failures as described in 6.4.3 and 6.4.4;

— requirements for the avoidance of a specific behaviour (for instance, "a particular sensor shall not produce an unstable output signal");

— requirements allocated to hardware elements implementing the intended functionality; and

— requirements specifying design measures on harnesses or connectors.

NOTE 2 Safety mechanisms can be implemented in hardware, in software, or as a combination of both.

6.4.3 This requirement applies to ASIL (B), C, and D of the safety goal. The target values specified to comply with ISO 26262-4:2018, 6.4.5, for the metrics of Clause 8 of this document shall be considered when deriving values for the hardware elements of the item.

6.4.4 This requirement applies to ASIL (B), C, and D of the safety goal. The target values specified to comply with ISO 26262-4:2018, 6.4.5, for the procedures of Clause 9 of this document shall be considered when deriving values for the hardware elements of the item.

NOTE This activity can include an apportionment of PMHF target values in the case of a distributed development as given in ISO 26262-8:2018, Clause 5, unless the use of EEC of 9.4.3 is agreed.

6.4.5 The hardware safety requirements shall be specified in accordance with ISO 26262-8:2018, Clause 6.

6.4.6 The criteria for design verification of the hardware elements of the item shall be specified, including environmental conditions (temperature, vibration, EMI, etc.), specific operational environment (supply voltage, mission profile, etc.) and component specific requirements:

a) for verification by evaluation of hardware elements, the criteria shall meet the needs of ISO 26262-8:2018, Clause 13; and

b) for verification by testing, the criteria shall meet the needs of Clause 10 of this document.

6.4.7 The hardware safety requirements shall comply with the fault tolerant time interval, or with the maximum fault handling time interval, for safety mechanisms as specified in ISO 26262-4:2018, 6.4.2.

NOTE A mechanism able to control a fault, but not able to comply with the fault tolerant time interval or with the maximum fault handling time interval, can be specified in the HW design. In such a case, it cannot be considered within the metrics of Clause 8 and Clause 9 of this document and it cannot be considered in an ASIL decomposition scheme.

6.4.8 The hardware safety requirements shall comply with the multiple-point fault detection interval as specified in ISO 26262-4:2018, 6.4.2.

NOTE 1 In the case of ASIL C and D safety goals, and if the corresponding safety concept does not prescribe specific values, the multiple-point fault detection intervals can be specified to be equal to or lower than the item's "power-up to power-down" cycle.

NOTE 2 Appropriate multiple-point fault detection intervals can also be justified by the quantitative analysis of the occurrence of random hardware failures (see Clause 9).

6.4.9 The hardware safety requirements shall be verified in accordance with ISO 26262-8:2018, Clause 9, in order to provide evidence of their:

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-5:2018

a) consistency with the technical safety concept, the system design specification and the hardware specifications;

b) completeness with respect to the technical safety requirements allocated to the hardware element;

c) consistency with the relevant software safety requirements; and

d) correctness and accuracy.

6.4.10 The HSI specification initiated in ISO 26262-4:2018, 6.4.7, shall be refined sufficiently to allow for the correct control and usage of the hardware by the software and shall describe each safety-related dependency between hardware and software.

6.4.11 The persons responsible for hardware and software development shall be jointly responsible for the verification of the adequacy of the refined HSI specification.

6.5 Work products

6.5.1 Hardware safety requirements specification (including test and evaluation criteria) resulting from requirements 6.4.1 to 6.4.8.

6.5.2 Hardware-software interface specification (HSI) (refined) resulting from requirement 6.4.10.

NOTE This work product refers to the same work product as given in ISO 26262-6:2018, 6.5.2.

6.5.3 Hardware safety requirements verification report resulting from requirements 6.4.9 and 6.4.11.

7 Hardware design

7.1 Objectives

The objectives of this clause are:

a) to create a hardware design that:

— supports the safety-oriented analyses;

— considers the results of the safety-oriented analyses;

— fulfils the hardware safety requirements;

— fulfils the hardware-software interface (HSI) specification;

— is consistent with system architectural design specification; and

— satisfies the required hardware design properties; and

b) to specify requirements and to provide information regarding functional safety of the hardware during production, operation, service and decommissioning; and

c) to verify:

— that the hardware design can fulfil the hardware safety requirements and the hardware-software interface (HSI) specification;

— the validity of the assumptions used to develop each SEooC integrated in the developed hardware; and

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-5:2018

— the suitability of the safety-related special characteristics to achieve functional safety during production and service.

7.2 General

Hardware design includes hardware architectural design and hardware detailed design. Hardware architectural design represents all hardware components and their interactions with one another. Hardware detailed design is at the level of electrical/electronic schematics representing the interconnections between hardware parts composing the hardware components.

In order to develop a single hardware design, both hardware safety requirements as well as all non-safety requirements are complied with. Hence, in this sub-phase, safety and non-safety requirements are handled within one development process.

7.3 Inputs to this clause

7.3.1 Prerequisites

The following information shall be available:

— hardware safety requirements specification in accordance with 6.5.1;

— hardware-software interface specification (HSI) (refined) in accordance with 6.5.2; and

— system architectural design specification in accordance with ISO 26262-4:2018, 6.5.3.

7.3.2 Further supporting information

The following information can be considered:

— software safety requirements specification (see ISO 26262-6:2018, 6.5.1); and

— specification of non-safety-related requirements of the hardware (from an external source).

7.4 Requirements and recommendations

7.4.1 Hardware architectural design

7.4.1.1 The hardware architecture shall implement the hardware safety requirements defined in Clause 6.

7.4.1.2 The hardware safety requirements shall be allocated to the hardware elements. As a result, each hardware element shall be developed in compliance with the highest ASIL of any of the requirements allocated to it.

NOTE Each characteristic of the hardware element will inherit the highest ASIL of the hardware safety requirements that it implements.

7.4.1.3 If ASIL decomposition is applied to the hardware safety requirements during hardware architectural design, it shall be applied in accordance with ISO 26262-9:2018, Clause 5.

7.4.1.4 If a hardware element is made of sub-elements that have an ASIL lower than the ASIL of the element or no ASIL assigned, then each of these shall be treated in accordance with the highest ASIL, unless the criteria for coexistence in accordance with ISO 26262-9:2018, Clause 6 are met.

7.4.1.5 The traceability between hardware safety requirements and hardware architectural design elements shall be established down to the lowest level of hardware components.

Documents
Document Sharing Hub

© ISO 2018 – All rights reserved

Full document details: BS ISO 26262-5:2018

NOTE The traceability of hardware safety requirements is not required down to the hardware detailed design. No hardware safety requirements are allocated to hardware parts that cannot be divided into sub-parts. For example, it is neither meaningful nor beneficial to try to establish hardware traceability down to each capacitor and resistor, etc.

7.4.1.6 In order to avoid systematic faults the hardware architectural design shall exhibit the following properties by use of the principles listed in Table 1:

a) modularity;

NOTE 1 Modularity enables the re-use of the design of HW elements without modification (e.g. temperature detection circuit block, ECC block in microcontroller).

b) adequate level of granularity; and

NOTE 2 The intent is that the architectural representation provides the necessary information at the necessary level of detail to show the effectiveness of the safety mechanisms.

c) simplicity.

Table 1 — Properties of hardware architectural design

Properties		ASIL			
		A	B	C	D
1	Hierarchical design	+	+	+	+
2	Precisely defined interfaces of safety-related hardware components	++	++	++	++
3	Avoidance of unnecessary complexity of interfaces	+	+	+	+
4	Avoidance of unnecessary complexity of hardware components	+	+	+	+
5	Maintainability (service)	+	+	++	++
6	Testability[a]	+	+	++	++

[a] Testability includes testability during development, production, service and operation.

7.4.1.7 Non-functional causes for failure of a safety-related hardware component shall be considered during hardware architectural design, including the following influences, if applicable: temperature, vibrations, water, dust, EMI, noise factor, or cross-talk originating either from other hardware components of the hardware architecture or from its environment.

7.4.2 Hardware detailed design

7.4.2.1 In order to avoid common design faults, relevant lessons learned shall be applied in accordance with ISO 26262-2:2018, 5.4.2.6.

7.4.2.2 Non-functional causes for failure of a safety-related hardware part shall be considered during hardware detailed design, including the following influences, if applicable: temperature, vibrations, water, dust, EMI, noise factor, or cross-talk originating either from other hardware parts of the hardware component or from its environment.

7.4.2.3 The mission profile and the operating conditions of the hardware part or hardware component, according to the hardware detailed design, shall be considered to ensure that the hardware part or hardware component is operated within its specification in order to avoid failures due to its intended use.

7.4.2.4 Robust design principles should be considered.

NOTE Robust design principles can be shown by use of hardware design guidelines.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-5:2018

EXAMPLE Conservative specification of components regarding their robustness against environmental and operational stress factors.

7.4.3 Safety analyses

7.4.3.1 Safety analyses of the hardware design to identify the causes of failures and the effects of faults shall be applied in accordance with Table 2 and ISO 26262-9:2018, Clause 8.

NOTE 1 The initial purpose of the safety analyses is to support the specification of the hardware design. Subsequently, the safety analyses can be used for verification of the hardware design (see 7.4.4).

NOTE 2 In order to support the specifications of the hardware design, qualitative analysis is appropriate and can be sufficient.

Table 2 — Hardware design safety analysis

Methods		ASIL			
		A	B	C	D
1	Deductive analysis	o	+	++	++
2	Inductive analysis	++	++	++	++

NOTE The level of detail of the analysis is commensurate with the level of detail of the design. Both methods can, in certain cases, be carried out at different levels of detail.

EXAMPLE An FMEA is done on hardware component level and provides the basic events of an FTA conducted at a higher abstraction level.

7.4.3.2 This requirement applies to ASIL (B), C, and D of the safety goal. For each safety-related hardware component or part, the safety analyses shall identify the following for the safety goal under consideration:

a) safe faults;

b) single-point faults or residual faults; and

c) multiple-point faults (either perceived, detected, or latent).

NOTE 1 The intention of the identification of multiple-point faults is not to require a systematic analysis of every possible combination of hardware faults but, as a minimum, to consider combinations that derive from the technical safety concept (for instance, the combination of two faults where one fault affects a safety-related element and another fault affects the corresponding safety mechanism intended to achieve or maintain a safe state).

NOTE 2 In most of the cases, the analysis can be limited to dual-point faults. However, multiple-point faults of a higher order than two can be shown to be relevant in the technical safety concept (e.g. when implementing redundant safety mechanisms).

7.4.3.3 This requirement applies to ASIL (A), (B), C, and D of the safety goal. Evidence of the effectiveness of implemented safety mechanisms to prevent faults from leading to single-point failures or to reduce residual faults shall be made available.

For that purpose:

a) evidence of the ability of the safety mechanisms to achieve and maintain a safe state shall be made available (in particular, appropriate failure mitigation ability within the fault tolerant time interval and within the maximum fault handling time interval); and

b) the diagnostic coverage, with respect to residual faults that is achieved by the safety mechanisms, shall be evaluated.

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-5:2018

NOTE 1 A fault that can occur at any time (e.g. not only at power-up) cannot be considered as being effectively covered if the fault detection time interval plus the fault reaction time interval, of the associated safety mechanism, is longer than the relevant fault tolerant time interval or the specified maximum fault handling time interval.

NOTE 2 If it can be demonstrated that a particular failure mode can only occur at power-up and that its probability of occurrence during the vehicle trip is negligible, then a test for those failure modes at start-up only is acceptable.

NOTE 3 An analysis such as FMEA or FTA can be used to structure the rationale.

NOTE 4 Depending on the knowledge of the failure modes of the hardware elements and their consequences at higher levels, the evaluation can be either an overall diagnostic coverage of the hardware element, or a more detailed failure mode coverage evaluation.

NOTE 5 Annex D can be used as a starting point for determining the diagnostic coverage provided by the planned safety mechanisms. The claimed DC is supported with a proper rationale (examples can be found in the clause concerning the evaluation of residual failure rate of ISO 26262-10:2018 and in ISO 26262-11:2018, Annex A).

NOTE 6 This requirement applies to safety mechanisms implemented in hardware, software, or a combination of both.

7.4.3.4 This requirement applies to ASIL (A), (B), C, and D of the safety goal. Evidence of the effectiveness of implemented safety mechanisms to prevent a fault from being latent shall be made available.

For that purpose:

a) evidence of the ability of the safety mechanism to detect failures and to achieve or maintain a safe state or to notify them to the driver, within the acceptable multiple-point fault detection time interval for latent faults, shall be made available in order to determine which faults will remain latent and which faults are detectable; and

b) the diagnostic coverage, with respect to latent faults, achieved by the safety mechanisms shall be evaluated.

NOTE 1 A fault cannot be considered covered if the fault handling time interval of the associated safety mechanism is longer than the relevant multiple-point fault detection time interval for latent faults.

NOTE 2 An analysis such as FMEA or FTA can be used to structure the rationale.

NOTE 3 Depending on the knowledge of the failure modes of the hardware elements and their consequences at higher levels, the evaluation can be either an overall diagnostic coverage of the hardware element or a more detailed failure mode coverage evaluation.

NOTE 4 Annex D can be used as a starting point for determining the diagnostic coverage provided by the planned safety mechanisms. The claimed DC is supported with a proper rationale (examples can be found in the clause concerning the evaluation of residual failure rate of ISO 26262-10:2018 and in ISO 26262-11:2018, Annex A).

NOTE 5 This requirement applies to safety mechanisms implemented in hardware, software, or a combination of both.

7.4.3.5 Evidence that the hardware elements in the design are compliant with their requirements for independence shall be provided, if applicable, based on an analysis of dependent failures in accordance with ISO 26262-9:2018, Clause 7.

NOTE 1 See also ISO 26262-9:2018, Annex C.

NOTE 2 See also ISO 26262-11:2018, 4.7.

7.4.3.6 If new hazards introduced by the hardware design are not already covered by an existing HARA report, they shall be introduced and evaluated in accordance with the change management process in ISO 26262-8:2018, Clause 8.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-5:2018

NOTE Newly identified hazards not already covered by an existing safety goal are usually non-functional hazards. Non-functional hazards are outside the scope of ISO 26262, but they can be annotated in the hazard analysis and risk assessment with the following statement: "No ASIL is assigned to this hazard as it is not within the scope of ISO 26262". However, an ASIL can be assigned for reference purposes.

7.4.4 Verification of hardware design

7.4.4.1 The hardware design shall be verified in accordance with ISO 26262-8:2018, Clause 9, and by using the hardware design verification methods listed in Table 3 to provide evidence for the following:

a) that it fulfils the hardware safety requirements;

b) that it is compatible with the hardware-software interface specification; and

c) the suitability of the safety-related special characteristics to achieve functional safety during production and service.

Table 3 — Hardware design verification

Methods		ASIL			
		A	B	C	D
1a	Hardware design walk-through[a]	++	++	o	o
1b	Hardware design inspection[a]	+	+	++	++
2	Safety analyses	In accordance with 7.4.3			
3a	Simulation[b]	o	+	+	+
3b	Development by hardware prototyping[b]	o	+	+	+

NOTE The scope of this verification review is technical correctness and completeness with regards to the HW safety requirements.

[a] Methods 1a and 1b serve as a check of the complete and correct implementation of the hardware safety requirements in the hardware design.

[b] Methods 3a and 3b serve as a check of particular points of the hardware design (e.g. fault injection as described in ISO 26262-11:2018, 4.8) for which analytical methods 1 and 2 are not considered to be sufficient.

7.4.4.2 If it is discovered, during hardware design, that the implementation of any hardware safety requirement is not feasible, a request for change shall be issued in accordance with the change management process in ISO 26262-8:2018, Clause 8.

7.4.4.3 The validity of the assumptions used to develop a SEooC that is integrated into the hardware shall be verified against the hardware safety requirements and the hardware design specification.

7.4.5 Production, operation, service and decommissioning

7.4.5.1 Safety-related special characteristics shall be specified if safety analysis has shown these characteristics to be relevant. Specification of safety-related special characteristics shall include:

a) the verification measures for production and operation; and

b) the acceptance criteria for these measures.

EXAMPLE A safety analysis of hardware design that relies on new sensor technologies (e.g., camera or radar sensors) can reveal the relevance of special installation procedures for these sensors. In such a case, additional verification measures for these components can be necessary during the production phase.

7.4.5.2 If incorrect assembly, disassembly, or decommissioning of safety-related hardware elements could have adverse effects on achieving or maintaining functional safety, then the information necessary

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-5:2018

to avoid incorrect execution shall be directed to the persons responsible for production, operation, service and decommissioning appointed in accordance with ISO 26262-2:2018, Clause 7.

7.4.5.3 The safety-related hardware elements shall be traceable, in accordance with ISO 26262-7:2018, 5.4.1.2 and 5.4.3.3 in order to:

a) enable effective field monitoring according to ISO 26262-2:2018, 7.4.2.3 and ISO 26262-7:2018, 7.4.1.1; and

b) enable recall or replacement management.

NOTE This can include adequate labelling or other identification of hardware elements to indicate that they are safety-related.

7.4.5.4 If incorrect servicing could have adverse effects on achieving or maintaining functional safety, then the information necessary to avoid such effects shall be directed to the persons responsible for production, operation, service and decommissioning appointed in accordance with ISO 26262-2:2018, Clause 7.

7.4.5.5 The requirements for production, operation, service and decommissioning of the hardware elements arising during hardware design shall be directed to the persons responsible for production, operation, service and decommissioning appointed in accordance with ISO 26262-2:2018, Clause 7.

7.5 Work products

7.5.1 Hardware design specification resulting from requirements in 7.4.1 and 7.4.2.

7.5.2 Hardware safety analysis report resulting from requirements in 7.4.3.

7.5.3 Hardware design verification report resulting from requirements in 7.4.4.

7.5.4 Specification of requirements related to production, operation, service and decommissioning resulting from requirements in 7.4.5.

8 Evaluation of the hardware architectural metrics

8.1 Objectives

The objective of this clause is to provide evidence based on the hardware architectural metrics for the suitability of the hardware architectural design of the item with respect to detection and control of safety-related random hardware failures.

8.2 General

This clause describes two hardware architectural metrics for the evaluation of the effectiveness of the architecture of the item to cope with random hardware failures.

These metrics and associated target values are evaluated on item level for the hardware elements of the item and are complementary to the evaluation of safety goal violations due to random hardware failures described in Clause 9.

The random hardware failures addressed by these metrics are limited to some of the item's safety-related electrical and electronic hardware parts, namely those that can significantly contribute to the violation or the achievement of the safety goal, and to the single-point, residual, and latent faults of

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-5:2018

those parts. For electromechanical hardware parts, only the electrical failure modes and failure rates are considered.

NOTE 1 Hardware elements whose faults are multiple-point faults with a higher order than two can be omitted from the calculations unless they are shown to be relevant in the technical safety concept.

The hardware architectural metrics can be applied iteratively during the hardware architectural design and the hardware detailed design.

The hardware architectural metrics are dependent upon the whole hardware of the item. Compliance with the target figures prescribed for the hardware architectural metrics is achieved for each safety goal in which the item is involved.

These hardware architectural metrics are intended to achieve the following objectives:

— be objectively assessable: metrics are a comprehensible means to differentiate between different architectures;

— support evaluation of the final design (i.e. calculations based on the selected detailed hardware design);

— make available ASIL dependent pass/fail criteria to evaluate the adequacy of the hardware architecture;

— reveal whether or not the coverage by the safety mechanisms, to prevent risk from single-point or residual faults in the hardware architecture, is sufficient (single-point fault metric);

— reveal whether or not the coverage by the safety mechanisms, to prevent risk from latent faults in the hardware architecture, is sufficient (latent-fault metric);

— address single-point faults, residual faults, and latent faults;

— ensure robustness concerning uncertainty of hardware failure rates;

— be limited to safety-related elements; and

— support usage on different element levels, e.g. target values can be assigned to suppliers' hardware elements.

EXAMPLE To facilitate distributed development, derived target values can be assigned to Integrated Circuits or ECUs.

NOTE 2 Items with safety-related availability requirements (i.e. the loss of a certain functionality can lead to a hazardous event) are subject to the same requirements and targets for hardware architectural metrics as items without safety related availability requirements.

8.3 Inputs of this clause

8.3.1 Prerequisites

The following information shall be available:

— hardware safety requirements specification in accordance with 6.5.1;

— hardware design specification in accordance with 7.5.1; and

— hardware safety analysis report in accordance with 7.5.2.

8.3.2 Further supporting information

The following information can be considered:

— technical safety concept (see ISO 26262-4:2018, 6.5.2); and

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-5:2018

— system architectural design specification (see ISO 26262-4:2018, 6.5.3).

8.4 Requirements and recommendations

8.4.1 This requirement applies to ASIL (B), C, and D of the safety goal. The concepts of diagnostic coverage, single-point fault metric, and latent-fault metric, in accordance with Annex C, shall apply to requirements 8.4.2 to 8.4.9.

8.4.2 This requirement applies to ASIL (B), C, and D of the safety goal. The diagnostic coverage of safety-related hardware elements by safety mechanisms shall be estimated with respect to residual faults and with respect to relevant latent faults.

NOTE 1 Annex D can be used as a starting point for determining the diagnostic coverage provided by the planned safety mechanisms. The claimed DC is supported with a proper rationale (examples can be found in clause concerning the evaluation of residual failure rate of ISO 26262-10 and in ISO 26262-11:2018, Annex A).

NOTE 2 Depending on the knowledge of the failure modes of the hardware elements and their consequences at a higher level, the evaluation can be either a diagnostic coverage of the hardware element or a more detailed failure mode coverage evaluation.

8.4.3 This requirement applies to ASIL (B), C, and D of the safety goal. The estimated failure rates for hardware parts used in the analyses shall be determined:

a) using hardware part failure rate data from a recognised industry source, or

EXAMPLE 1 Commonly recognised industry sources to determine the hardware part failure rates and the failure mode distributions include SN 29500, IEC 61709, MIL HDBK 217 F notice 2, RIAC HDBK 217 Plus, UTE C80-811, NPRD-2016, EN 50129:2003, Annex C, RIAC FMD-2016, MIL HDBK 338, and FIDES 2009 EdA. The failure mode distributions e.g. those defined by “Alessandro Birolini - Reliability Engineering” can be used.

NOTE 1 The failure rate values given in these databases are generally considered to be conservative.

NOTE 2 In applying a selected industry source the following considerations are appropriate to avoid artificial reduction of the calculated base failure rate:

— the mission profile;

— the applicability of the failure modes with respect to the operating conditions; and

— the failure rate unit (per operating hour or per calendar hour).

b) using statistics based on field returns. In this case, the estimated failure rate should have a comparable confidence level of at least 70 %, or

NOTE 3 If the confidence level for the failure rates of different hardware parts used in the SPFM and LFM evaluation is significantly different, the metrics will be biased.

NOTE 4 It may still be necessary to scale these statistics-based data from field returns before using them together with values from other data sources with different confidence levels. See also Note 7.

NOTE 5 Failure rates based on field returns can be calculated as described in ISO 26262-8:2018, Clause 14 (Proven in use).

c) using expert judgement founded on an engineering approach based on quantitative and qualitative arguments. Expert judgement shall be exercised in accordance with structured criteria as a basis for this judgement. These criteria shall be set before the estimation of failure rates is made.

NOTE 6 The criteria for expert judgment can include a combination of heuristic information supported by a combination of field data, testing, reliability analysis and physics-of-failure based simulation approaches while considering the novelty of the design.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-5:2018

NOTE 7 Informative references from international reliability expert bodies can be used: SAE J1211 "Robustness Validation" – Analysis, Modelling and Simulation provides physics-of-failure (PoF) based failure mechanism models, JEDEC-JESD89, JEDEC-JESD91, JEDEC-JESD94, JEDEC-JEP143, JEDEC-JESD148.

NOTE 8 If failure rates from multiple data sources (as listed in 8.4.3) are combined e.g. in the case the failure rates of different parts are not available from the same source, the failure rates can be scaled using a scaling factor such that the quality of prediction of the different failures rates is equivalent. This scaling can be used if a rationale for the scaling factor between two failure rate sources is available.

EXAMPLE 2 An element failure rate is found only in one source whereas a similar element is available in that and another source. The scaling factor is the ratio of the failure rate from these two sources utilising the same mission profile.

EXAMPLE 3 Failure rates from data handbooks are generally considered to be conservative. If a random hardware failure target value consistent with the use of handbook data is chosen, failure rate derived from field returns can be used by applying an appropriate scaling factor (corresponding to a confidence level more conservative than usual, for example).

NOTE 9 If a suitable scaling factor is not available, separate target values compliant with the SPFM and LFM requirements can be assigned to the different elements under consideration (analogous to 8.4.4).

NOTE 10 For semiconductors, see ISO 26262-11:2018, 4.6 for guidance.

8.4.4 This requirement applies to ASIL (B), C, and D of the safety goal. If the evidence that can be made available for the hardware part failure rate is insufficient, then alternative means shall be proposed (e.g. add safety mechanisms to detect and control this fault). If the alternative means consist solely of added safety mechanisms:

a) the diagnostic coverage of the hardware part with respect to residual faults shall be equal to or higher than the item SPFM target value; and

b) the diagnostic coverage of the hardware part with respect to latent faults shall be equal to or higher than the item LFM target value.

NOTE 1 Sufficient evidence means, for instance, that evidence is given that the failure rate has been determined using one of the methods listed in 8.4.3.

NOTE 2 The proportion of safe faults of the hardware part can be considered when determining the coverage of the safety mechanisms. In this case, the calculation of the coverage is done in a similar way to the calculation of the single point fault metric or the latent fault metric, at the hardware part level instead of at the item level.

8.4.5 This requirement applies to ASIL (B), C, and D of the safety goal. For each safety goal, a quantitative target value for the Single-Point Fault Metric (SPFM) as required in ISO 26262-4:2018, 6.4.5, shall be based on one of the following sources of reference target values:

a) derived from the hardware architectural metric calculation applied on a similar well-trusted design, or

NOTE 1 Two similar designs have similar functionalities and similar safety goals with the same assigned ASIL.

b) derived from Table 4.

Table 4 — Possible source for the derivation of the target "single-point fault metric" value

	ASIL B	ASIL C	ASIL D
Single-point fault metric	≥90 %	≥97 %	≥99 %

NOTE 2 This quantitative target is intended to provide:

— design guidance; and

— evidence that the design complies with the safety goals.

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-5:2018

8.4.6 This requirement applies to ASIL (B), (C), and D of the safety goal. For each safety goal, a quantitative target value for Latent-Fault Metric (LFM) as required in ISO 26262-4:2018, 6.4.5 shall be based on one of the following sources of reference target values:

a) derived from the hardware architectural metrics calculation applied on similar well-trusted design; or

NOTE 1 Two similar designs have similar functionalities and similar safety goals with the same assigned ASIL.

b) derived from Table 5.

Table 5 — Possible source for the derivation of the target "latent-fault metric" value

	ASIL B	ASIL C	ASIL D
Latent-fault metric	≥60 %	≥80 %	≥90 %

NOTE 2 This quantitative target is intended to provide:

— design guidance; and

— evidence that the design complies with the safety goals.

8.4.7 This requirement applies to ASIL (B), C, and D of the safety goal. For each safety goal, the whole hardware of the item shall comply with one of the following alternatives:

a) to meet the target "single-point fault metric" value, as described in 8.4.5, or

b) to meet the appropriate targets prescribed at the hardware element level which are sufficient to comply with the single-point fault metric's target value assigned to the whole hardware of the item as described in requirement 8.4.5 and to provide the rationale for compliance with these targets at the hardware element level.

NOTE 1 If an item contains different kinds of hardware elements with significantly different failure rate levels, the risk exists that compliance with the hardware architectural metrics only focuses on the kind of hardware elements with the highest magnitude of failure rates. One example where this can occur is for the single-point fault metric for which compliance can be achieved by considering the failure rates for failures of wires, fuses or connectors, while disregarding the failure rates of hardware parts with significantly lower failure rates. The prescription of appropriate metric target values for each kind of hardware helps to avoid this side effect.

NOTE 2 Transient faults are considered when shown to be relevant due to, for instance, the technology used. They can be addressed either by specifying and verifying a dedicated target "single-point fault metric" value to them (as explained in NOTE 1) or by a qualitative rationale based on the verification of the effectiveness of the internal safety mechanisms implemented to cover these transient faults.

NOTE 3 If the target is not met, the rationale for how the safety goal is achieved will be assessed as given in 4.2.

NOTE 4 Some or all of the applicable safety goals can be considered together for the determination of the single-point fault metric; but in this case the metric's target to be considered is that of the safety goal with the highest ASIL.

EXAMPLE If an item consists out of three hardware elements A, B and C with a failure rate λ_A, λ_B, λ_C and $\lambda_{total} = \lambda_A + \lambda_B + \lambda_C$, any combination of element SPFM target values $M_{SPFM,\,Element}$ fulfilling the following equation is acceptable: $\left(\frac{\lambda_A}{\lambda_{total}} \times M_{SPFM,A} + \frac{\lambda_B}{\lambda_{total}} \times M_{SPFM,B} + \frac{\lambda_C}{\lambda_{total}} \times M_{SPFM,C}\right) \geq M_{SPFM,Itemtarget}$.

8.4.8 This requirement applies to ASIL (B), (C), and D of the safety goal. For each safety goal, the whole hardware of the item shall comply with one of the following alternatives:

a) to meet the target "latent-fault metric" value, as described in 8.4.6;

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-5:2018

b) to meet the appropriate targets prescribed at the hardware element level which are sufficient to comply with the latent-fault metric's target value assigned to the whole hardware of the item as described in requirement 8.4.6 and to provide the rationale for compliance with these targets at the hardware element level; or

c) to meet the target values for the diagnostic coverage, with respect to latent faults, identical to the target value given in reference 8.4.6 for the latent-fault metric (treated as a diagnostic coverage), for each hardware element with faults that can lead to the unavailability of a safety mechanism (to prevent a fault from violating the safety goal). This alternative applies when each safety mechanism, whose unavailability can contribute to the violation of the safety goal, is based on fault detection.

NOTE 1 Alternative c) is limited to the cases where each relevant safety mechanism is based on fault detection. It is supposed that in this case the potentially latent faults of the intended functionality are alerted through the detection of these safety mechanisms. In other cases, this alternative cannot be applied and alternatives a) and b) are the only possibilities.

EXAMPLE 1 Annex H provides examples of different types of safety mechanisms considering latent fault handling.

NOTE 2 In the case of c), a metric is not calculated. Only the coverage of the hardware elements by safety mechanisms with respect to latent faults is evaluated.

NOTE 3 If an item contains different kinds of hardware elements with significantly different failure rate levels, the risk exists that compliance with the hardware architectural metrics only focuses on the kind of hardware elements with the highest magnitude of failure rates. One example where this can occur is for the latent fault metric for which compliance could be achieved by considering the failure rates for failures of wires, fuses or connectors, while disregarding the failure rates of hardware parts with significantly lower failure rates. The prescription of appropriate metric target values for each kind of hardware helps to avoid this side effect.

NOTE 4 If the target is not met, the rationale for how the safety goal is achieved will be assessed as given in 4.2.

NOTE 5 Some or all of the applicable safety goals can be considered together for the determination of the latent-fault metric; but in this case the metric's target to be considered is that of the safety goal with the highest ASIL.

EXAMPLE 2 If an item consists out of three hardware elements A, B and C with a failure rate λ_A, λ_B, λ_C and $\lambda_{total} = \lambda_A + \lambda_B + \lambda_C$, any combination of element LFM target values $M_{LFM,\ Element}$ fulfilling the following equation is acceptable: $\left(\frac{\lambda_A}{\lambda_{total}} \times M_{LFM,A} + \frac{\lambda_B}{\lambda_{total}} \times M_{LFM,B} + \frac{\lambda_C}{\lambda_{total}} \times M_{LFM,C}\right) \geq M_{LFM,Itemtarget}$.

8.4.9 This requirement applies to ASIL (B), C, and D of the safety goal. A verification review of the result of the applied methods in 8.4.7 and 8.4.8 shall be performed in order to provide evidence of its technical correctness and completeness in accordance with ISO 26262-8:2018, Clause 9.

NOTE Verification of the single-point fault metric ensures that only failure rates of safety-related hardware elements are taken into consideration, so that the metric is not inappropriately skewed by unnecessary safety-related hardware elements without the potential for having single-point faults or residual faults (e.g. by adding unnecessary hardware elements to a safety mechanism).

8.5 Work products

8.5.1 Analysis of the effectiveness of the architecture of the item to cope with the random hardware failures resulting from requirements 8.4.1 to 8.4.8.

8.5.2 Verification review report of evaluation of the effectiveness of the architecture of the item to cope with the random hardware failures resulting from requirement 8.4.9.

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-5:2018

9 Evaluation of safety goal violations due to random hardware failures

9.1 Objectives

The objective of this clause is to provide evidence that the residual risk of a safety goal violation, due to random hardware failures of the item, is sufficiently low.

NOTE "Sufficiently low" means "comparable to residual risks on items already in use and known to be safe".

9.2 General

Two alternative methods (see 9.4) are proposed to evaluate whether the residual risk of safety goal violations is sufficiently low.

Both methods evaluate the residual risk of violating a safety goal due to single-point faults, residual faults, and plausible dual-point faults. Multiple-point faults can also be considered if shown to be relevant to the safety concept. In this analysis, coverage of safety mechanisms will be considered for residual and dual-point faults, and exposure duration will be considered as well for dual-point faults.

The requirements for the first method are given in 9.4.2. The "Probabilistic Metric for random Hardware Failures" (PMHF) represents a quantitative analysis which evaluates the violation of the considered safety goal by random failures of the hardware elements. The quantitative result of the analysis is compared with a target value.

The requirements for the second method are given in 9.4.3. The "Evaluation of Each Cause of safety goal violation" (EEC) is based on the individual evaluation of each hardware part and its contribution to the violation of the considered safety goal with respect to residual, single-point and plausible dual-point failures.

The chosen method can be applied iteratively during the hardware architectural design and the hardware detailed design.

The scope of this clause is limited to the random hardware failures of the item. The parts considered in the analyses are the electrical and electronic hardware parts. For electromechanical hardware parts, only the electrical failure modes and failure rates are considered.

9.3 Inputs to this clause

9.3.1 Prerequisites

The following information shall be available:

— hardware safety requirements specification in accordance with 6.5.1;

— hardware design specification in accordance with 7.5.1; and

— hardware safety analysis report in accordance with 7.5.2.

9.3.2 Further supporting information

The following information can be considered:

— technical safety concept (see ISO 26262-4:2018, 6.5.2); and

— system architectural design specification (see ISO 26262-4:2018, 6.5.3).

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-5:2018

9.4 Requirements and recommendations

9.4.1 General

9.4.1.1 This requirement applies to ASIL (B), C and D of the safety goal. The item shall comply with either 9.4.2 or 9.4.3.

9.4.1.2 This requirement applies to ASIL C and D of the safety goal. A hardware part's single-point fault shall only be considered acceptable if an argument for its sufficiently low probability of occurrence is provided by one of the following options:

a) dedicated measures are taken, or

b) for a safety goal ASIL D, the following criteria are satisfied:

— a conservative data source is used;

— only a small portion of the failure rate (e.g. one particular failure mode) can violate the safety goal; and

— the resulting single-point fault failure rate is smaller than one-tenth of the value corresponding to failure rate class 1 (according to 9.4.3.3);

c) for a safety goal ASIL C, the following criteria are satisfied:

— a conservative data source is used;

— only a small portion of the failure rate (e.g. one particular failure mode) can violate the safety goal; and

— the resulting single-point fault failure rate is smaller than one-tenth of the value corresponding to failure rate class 2 (according to 9.4.3.3).

NOTE 1 Regarding this requirement, a microcontroller, an ASIC, or similar SoC can be treated as hardware parts.

NOTE 2 Dedicated measures can include:

a) design features such as hardware part over-design (e.g. electrical or thermal stress rating) or physical separation (e.g. spacing of contacts on a printed circuit board);

b) a special sample test of incoming material to reduce the risk of occurrence of this failure mode;

c) a burn-in test;

d) a dedicated control set as part of the control plan; and

e) assignment of safety-related special characteristics.

9.4.1.3 This requirement applies to ASIL C and D of the safety goal. A hardware part residual fault, with a diagnostic coverage (with respect to residual faults) lower than 90 %, shall only be considered acceptable if an argument for its sufficiently low probability of occurrence is provided by one of the following options:

a) dedicated measures are taken (NOTE 2 in 9.4.1.2 lists examples of dedicated measures), or

b) for a safety goal ASIL D, the following criteria are satisfied:

— a conservative data source is used;

— only a small portion of the failure rate (e.g. one particular failure mode) can violate the safety goal; and

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-5:2018