INTERNATIONAL STANDARD

ISO 26262-5

Second edition
2018-12

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 26262-5:2018
https://standards.iteh.ai/catalog/standards/sist/9db6ab73-7e07-479a-8337-77d0f7e711b6/iso-26262-5-2018

Reference number
ISO 26262-5:2018(E)

© ISO 2018

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 26262-5:2018
https://standards.iteh.ai/catalog/standards/sist/9db6ab73-7e07-479a-8337-77d0f7e711b6/iso-26262-5-2018

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

Contents

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 26262-5:2018
https://standards.iteh.ai/catalog/standards/sist/9db6ab73-7e07-479a-8337-77d0f7e711b6/iso-26262-5-2018

© ISO 2018 – All rights reserved

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 26262-5:2018
https://standards.iteh.ai/catalog/standards/sist/9db6ab73-7e07-479a-8337-77d0f7e711b6/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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

ISO 26262-5:2018
https://standards.iteh.ai/catalog/standards/sist/9db6ab73-7e07-479a-8337-77d0f7e71b6f/iso-26262-5-2018

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.

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 26262-5:2018
https://standards.iteh.ai/catalog/standards/sist/9db6ab73-7e07-479a-8337-77d0f7e711b6/iso-26262-5-2018

© ISO 2018 – All rights reserved

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 26262-5:2018
https://standards.iteh.ai/catalog/standards/sist/9db6ab73-7e07-479a-8337-77d0f7e711b6/iso-26262-5-2018

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.

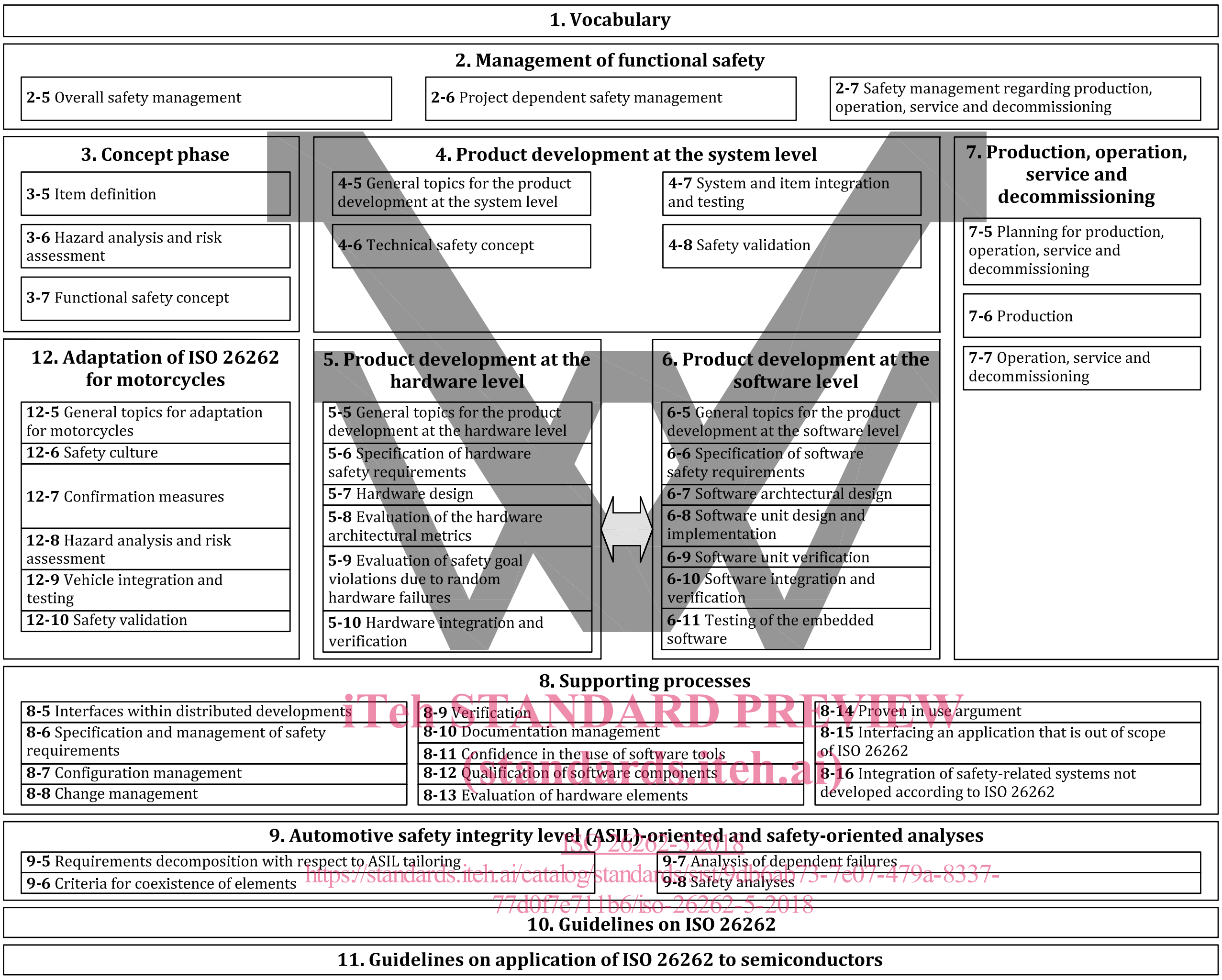
The achievement of functional safety is influenced by the development process (including such activities as requirements specification, design, implementation, integration, verification, validation and configuration), the production and service processes and the management processes.

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.

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


1. Vocabulary
2. Management of functional safety
2-5 Overall safety management
2-6 Project dependent safety management
2-7 Safety management regarding production, operation, service and decommissioning
3. Concept phase
3-5 Item definition
3-6 Hazard analysis and risk assessment
3-7 Functional safety concept
4. Product development at the system level
4-5 General topics for the product development at the system level
4-6 Technical safety concept
4-7 System and item integration and testing
4-8 Safety validation
7. Production, operation, service and decommissioning
7-5 Planning for production, operation, service and decommissioning
7-6 Production
7-7 Operation, service and decommissioning
12. Adaptation of ISO 26262 for motorcycles
12-5 General topics for adaptation for motorcycles
12-6 Safety culture
12-7 Confirmation measures
12-8 Hazard analysis and risk assessment
12-9 Vehicle integration and testing
12-10 Safety validation
5. Product development at the hardware level
5-5 General topics for the product development at the hardware level
5-6 Specification of hardware safety requirements
5-7 Hardware design
5-8 Evaluation of the hardware architectural metrics
5-9 Evaluation of safety goal violations due to random hardware failures
5-10 Hardware integration and verification
6. Product development at the software level
6-5 General topics for the product development at the software level
6-6 Specification of software safety requirements
6-7 Software archtectural design
6-8 Software unit design and implementation
6-9 Software unit verification
6-10 Software integration and verification
6-11 Testing of the embedded software
8. Supporting processes
8-5 Interfaces within distributed developments
8-6 Specification and management of safety requirements
8-7 Configuration management
8-8 Change management
8-9 Verification
8-10 Documentation management
8-11 Confidence in the use of software tools
8-12 Qualification of software components
8-13 Evaluation of hardware elements
8-14 Proven in use argument
8-15 Interfacing an application that is out of scope of ISO 26262
8-16 Integration of safety-related systems not developed according to ISO 26262
9. Automotive safety integrity level (ASIL)-oriented and safety-oriented analyses
9-5 Requirements decomposition with respect to ASIL tailoring
9-6 Criteria for coexistence of elements
9-7 Analysis of dependent failures
9-8 Safety analyses
10. Guidelines on ISO 26262
11. Guidelines on application of ISO 26262 to semiconductors

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 26262-5:2018
https://standards.iteh.ai/catalog/standards/sist/9db6ab73-7e07-479a-8337-77d0f7e711b6/iso-26262-5-2018

Figure 1 — Overview of the ISO 26262 series of standards

© ISO 2018 – All rights reserved

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 26262-5:2018
https://standards.iteh.ai/catalog/standards/sist/9db6ab73-7e07-479a-8337-77d0f7e711b6/iso-26262-5-2018

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.

© ISO 2018 – All rights reserved

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 26262-5:2018
https://standards.iteh.ai/catalog/standards/sist/9db6ab73-7e07-479a-8337-77d0f7e711b6/iso-26262-5-2018

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.

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 26262-5:2018
https://standards.iteh.ai/catalog/standards/sist/9db6ab73-7e07-479a-8337-77d0f7e711b6/iso-26262-5-2018

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.

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.

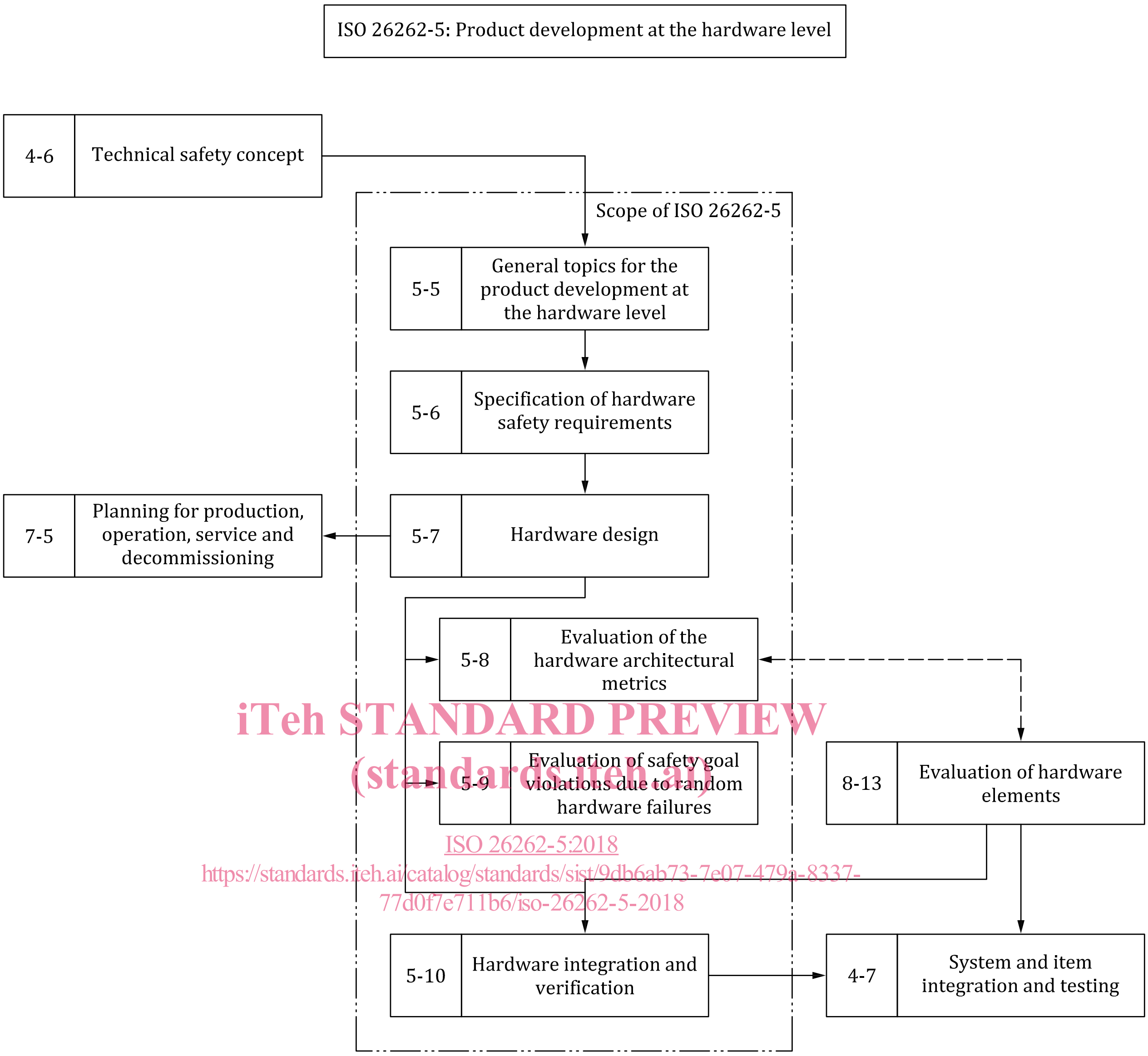
iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 26262-5:2018
https://standards.iteh.ai/catalog/standards/sist/9db6ab73-7e07-479a-8337-77d0f7e7fdb6/iso-26262-5-2018

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


ISO 26262-5: Product development at the hardware level
4-6
Technical safety concept
Scope of ISO 26262-5
5-5
General topics for the product development at the hardware level
5-6
Specification of hardware safety requirements
7-5
Planning for production, operation, service and decommissioning
5-7
Hardware design
5-8
Evaluation of the hardware architectural metrics
5-9
Evaluation of safety goal violations due to random hardware failures
8-13
Evaluation of hardware elements
5-10
Hardware integration and verification
4-7
System and item integration and testing

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 26262-5:2018
https://standards.iteh.ai/catalog/standards/sist/9db6ab73-7e07-479a-8337-77d0f7e711b6/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.

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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).

ISO 26262-5:2018
https://standards.iteh.ai/catalog/standards/sist/9db6ab73-7e07-479a-8337-77d0f7e711b6/iso-26262-5-2018

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

© ISO 2018 – All rights reserved

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.

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 26262-5:2018
https://standards.iteh.ai/catalog/standards/sist/9db6ab73-7e07-479a-8337-77d0f7e711b6/iso-26262-5-2018

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.