
**Road vehicles — Functional safety —
Part 8:
Supporting processes**

*Véhicules routiers — Sécurité fonctionnelle —
Partie 8: Processus d'appui*

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO 26262-8:2018

<https://standards.iteh.ai/catalog/standards/iso/19b11366-be38-4f97-8f99-9523c72ff1ff/iso-26262-8-2018>



iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO 26262-8:2018

<https://standards.iteh.ai/catalog/standards/iso/19b11366-be38-4f97-8f99-9523c72ff1ff/iso-26262-8-2018>



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

Page

Foreword	vi
Introduction	viii
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	4
4.6 Adaptation for trucks, buses, trailers and semi-trailers	4
5 Interfaces within distributed developments	4
5.1 Objectives	4
5.2 General	4
5.3 Inputs to this clause	4
5.3.1 Prerequisites	4
5.3.2 Further supporting information	5
5.4 Requirements and recommendations	5
5.4.1 Application of requirements	5
5.4.2 Supplier selection criteria	5
5.4.3 Initiation and planning of distributed development	6
5.4.4 Execution of distributed development	7
5.4.5 Functional safety assessment activities in a distributed development	8
5.4.6 Agreement for production, operation, service and decommissioning	8
5.5 Work products	8
6 Specification and management of safety requirements	9
6.1 Objectives	9
6.2 General	9
6.3 Inputs to this clause	10
6.3.1 Prerequisites	10
6.3.2 Further supporting information	10
6.4 Requirements and recommendations	11
6.4.1 Specification of safety requirements	11
6.4.2 Attributes and characteristics of safety requirements	11
6.4.3 Management of safety requirements	13
6.5 Work products	14
7 Configuration management	14
7.1 Objectives	14
7.2 General	14
7.3 Inputs to this clause	15
7.3.1 Prerequisites	15
7.3.2 Further supporting information	15
7.4 Requirements and recommendations	15
7.5 Work products	15
8 Change management	16
8.1 Objectives	16
8.2 General	16
8.3 Inputs to this clause	16
8.3.1 Prerequisites	16
8.3.2 Further supporting information	16

8.4	Requirements and recommendations.....	16
8.4.1	Planning and initiating change management.....	16
8.4.2	Change requests.....	17
8.4.3	Change request analysis.....	17
8.4.4	Change request evaluation.....	17
8.4.5	Implementing and documenting the change.....	18
8.5	Work products.....	18
9	Verification.....	18
9.1	Objectives.....	18
9.2	General.....	19
9.3	Inputs to this clause.....	19
9.3.1	Prerequisites.....	19
9.3.2	Further supporting information.....	19
9.4	Requirements and recommendations.....	20
9.4.1	Verification planning.....	20
9.4.2	Verification specification.....	20
9.4.3	Verification execution and evaluation.....	21
9.5	Work products.....	22
10	Documentation management.....	22
10.1	Objectives.....	22
10.2	General.....	22
10.3	Inputs to this clause.....	23
10.3.1	Prerequisites.....	23
10.3.2	Further supporting information.....	23
10.4	Requirements and recommendations.....	23
10.5	Work products.....	24
11	Confidence in the use of software tools.....	24
11.1	Objectives.....	24
11.2	General.....	24
11.3	Inputs to this clause.....	26
11.3.1	Prerequisites.....	26
11.3.2	Further supporting information.....	26
11.4	Requirements and recommendations.....	27
11.4.1	General requirement.....	27
11.4.2	Validity of predetermined Tool Confidence Level or qualification.....	27
11.4.3	Software tool compliance with its evaluation criteria or its qualification.....	27
11.4.4	Planning of usage of a software tool.....	27
11.4.5	Evaluation of a software tool by analysis.....	28
11.4.6	Qualification of a software tool.....	30
11.4.7	Increased confidence from use.....	30
11.4.8	Evaluation of the tool development process.....	31
11.4.9	Validation of the software tool.....	32
11.5	Work products.....	32
12	Qualification of software components.....	32
12.1	Objectives.....	32
12.2	General.....	32
12.3	Inputs to this clause.....	33
12.3.1	Prerequisites.....	33
12.3.2	Further supporting information.....	33
12.4	Requirements and recommendations.....	33
12.4.1	General.....	33
12.4.2	Specification of software component qualification.....	33
12.4.3	Verification of qualification of a software component.....	35
12.5	Work products.....	35
13	Evaluation of hardware elements.....	35
13.1	Objectives.....	35

13.2	General.....	36
13.3	Inputs to this clause.....	36
13.3.1	Prerequisites.....	36
13.3.2	Further supporting information.....	36
13.4	Requirements and recommendations.....	37
13.4.1	General.....	37
13.4.2	Evaluation of class I hardware elements.....	38
13.4.3	Evaluation of class II hardware elements.....	38
13.4.4	Evaluation of class III hardware elements.....	40
13.5	Work products.....	40
14	Proven in use argument.....	40
14.1	Objectives.....	40
14.2	General.....	41
14.3	Inputs to this clause.....	41
14.3.1	Prerequisites.....	41
14.3.2	Further supporting information.....	42
14.4	Requirements and recommendations.....	42
14.4.1	General.....	42
14.4.2	Proven in use credit.....	42
14.4.3	Minimum information on candidate.....	43
14.4.4	Analysis of modifications to the candidate.....	43
14.4.5	Analysis of field data.....	43
14.5	Work products.....	45
15	Interfacing an application that is out of scope of ISO 26262.....	46
15.1	Objectives.....	46
15.2	General.....	46
15.3	Inputs to this clause.....	46
15.3.1	Prerequisites.....	46
15.3.2	Further supporting information.....	46
15.4	Requirements and recommendations.....	46
15.5	Work products.....	47
16	Integration of safety-related systems not developed according to ISO 26262.....	47
16.1	Objectives.....	47
16.2	General.....	47
16.3	Inputs to this clause.....	48
16.3.1	Prerequisites.....	48
16.3.2	Further supporting information.....	48
16.4	Requirements and recommendations.....	48
16.5	Work products.....	48
	Annex A (informative) Overview of and workflow of supporting processes.....	49
	Annex B (informative) Development Interface Agreement (DIA) example.....	53
	Bibliography.....	60

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: [Foreword - Supplementary information](http://www.iso.org/foreword)

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.

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 Standards
(<https://standards.iteh.ai>)
Document Preview

ISO 26262-8:2018

<https://standards.iteh.ai/catalog/standards/iso/19b11366-be38-4f97-8f99-9523c72ff1ff/iso-26262-8-2018>

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.

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

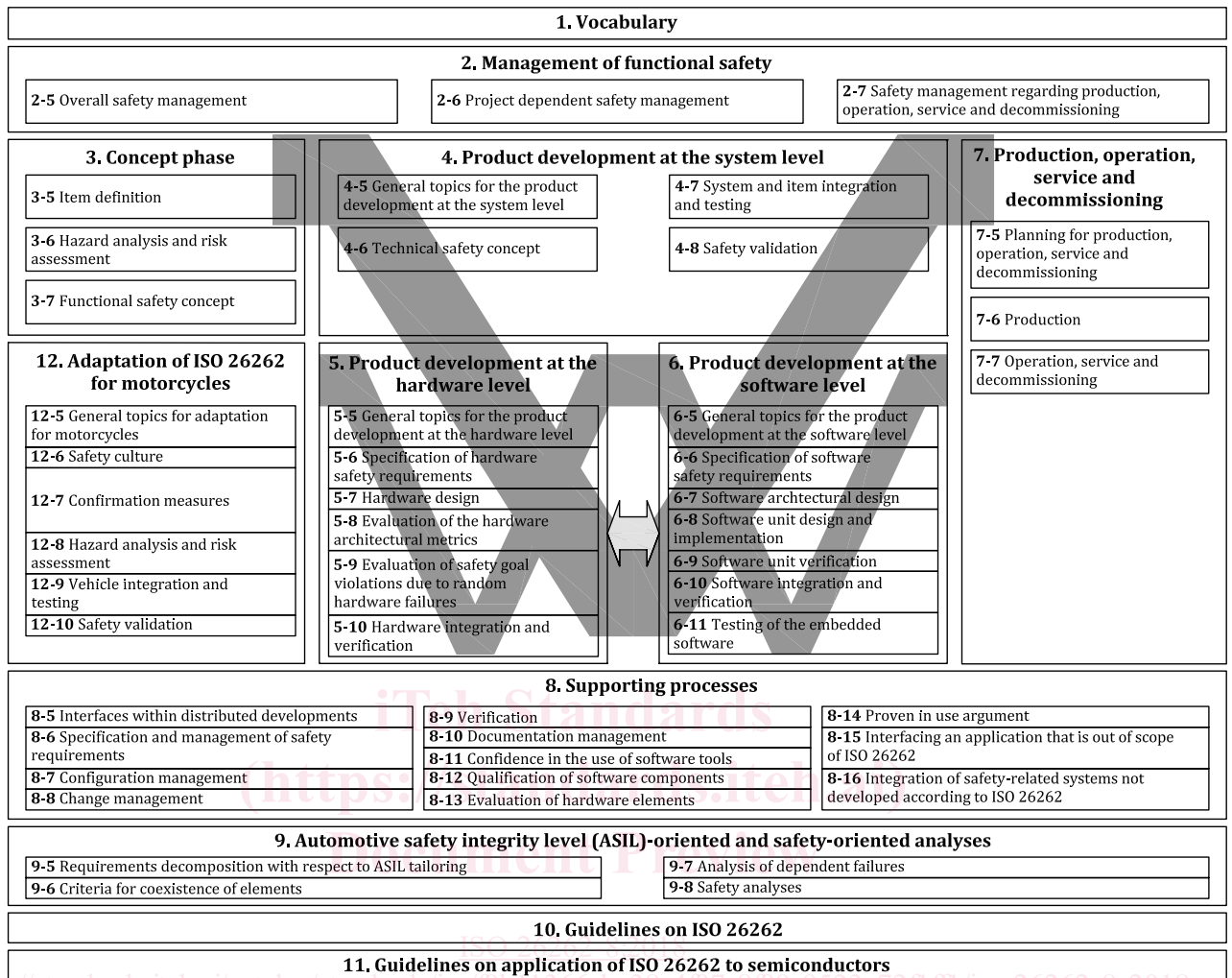


Figure 1 — Overview of ISO 26262

Road vehicles — Functional safety —

Part 8: Supporting processes

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 supporting processes, including the following:

- interfaces within distributed developments;
- overall management of safety requirements;
- configuration management;
- change management;
- verification;
- documentation management;
- confidence in the use of software tools;
- qualification of software components;
- evaluation of hardware elements;
- proven in use argument;

- interfacing an application that is out of scope of ISO 26262; and
- integration of safety-related systems not developed according to ISO 26262.

[Annex A](#) provides an overview on objectives, prerequisites and work products of this document.

2 Normative references

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

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

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

ISO 26262-3:2018, *Road vehicles — Functional safety — Part 3: Concept phase*

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

ISO 26262-5:2018, *Road vehicles — Functional safety — Part 5: Product development at the hardware 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, operation, service and decommissioning*

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

3 Terms and definitions

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

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

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <https://www.iso.org/obp>

4 Requirements for compliance

4.1 Purpose

This clause describes how:

- to achieve compliance with the ISO 26262 series of standards;
- to interpret the tables used in the ISO 26262 series of standards; and
- 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:

- 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.

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 Interfaces within distributed developments

5.1 Objectives

The objectives of this clause are:

- a) to define the interactions and dependencies between customers and suppliers for development activities;
- b) to describe the allocation of responsibilities; and
- c) to identify the work products to be exchanged for distributed developments of an item and its elements.

5.2 General

The customer (e.g. vehicle manufacturer) and the suppliers for item or element developments jointly comply with the requirements specified in the ISO 26262 series of standards for distributed developments. Responsibilities are agreed between the customer and the suppliers for the concept, development, production, operation, service and decommissioning phases of the safety lifecycle. Subcontractor relationships are permitted. The customer has safety-related procedures concerning planning, execution and documentation for in-house item developments, therefore comparable procedures apply for co-operation with the supplier on distributed item developments. The same applies for item developments where the supplier has the full responsibility for functional safety.

NOTE 1 The Development Interface Agreement (DIA) aims to describe the roles and responsibilities between the customer and supplier. Consequently the safety planning by the customer and supplier is in line with the DIA.

NOTE 2 This clause is not relevant for the procurement which do not place any responsibility for safety on the supplier, including standard components and parts or development commissions.

NOTE 3 This note applies to T&B: this clause is not relevant for body builder equipment being integrated into base vehicles. [Clause 15](#) applies when integrating body builder equipment developed according to ISO 26262 into a base vehicle which is in scope of another standard. [Clause 16](#) applies when body builder equipment developed according to another standard is integrated into a base vehicle developed according to ISO 26262.

5.3 Inputs to this clause

5.3.1 Prerequisites

See applicable prerequisites of the relevant phases of the safety lifecycle for which a distributed development is planned and carried out.