INTERNATIONAL STANDARD

ISO 26262-2

Redline version
compares Second edition to
First edition

Road vehicles — Functional safety —

Part 2:
Management of functional safety

Véhicules routiers — Sécurité fonctionnelle —

Partie 2: Gestion de la sécurité fonctionnelle

Reference number
ISO 26262-2:redline:2018(E)

IMPORTANT

This marked-up version uses the following colour-coding in the marked-up text:

Text example 1 — Text has been added (in green)

~~Text example 2~~ — Text has been deleted (in red)

 — Graphic figure has been added

 — Graphic figure has been deleted

1.x ... — If there are changes in a clause/subclause, the corresponding clause/subclause number is highlighted in yellow in the Table of contents

DISCLAIMER

This marked-up version highlights the main changes in this edition of the document compared with the previous edition. It does not focus on details (e.g. changes in punctuation).

This marked-up version does not constitute the official ISO document and is not intended to be used for implementation purposes.

COPYRIGHT PROTECTED DOCUMENT

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

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.

~~International Standards are~~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 ~~rules given in~~editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

~~The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.~~

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.

~~ISO 26262-2~~This document was prepared by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee, SC ~~3~~32, *Electrical and electronic ~~equipment~~components and general system aspects*.

~~ISO 26262 consists of the following parts, under the general title~~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 ~~*Road vehicles — Functional safety*~~following main changes:

— ~~*Part 1: Vocabulary*~~requirements for trucks, buses, trailers and semi-trailers;

— ~~*Part 2: Management of functional safety*~~extension of the vocabulary;

— ~~*Part 3: Concept phase*~~more detailed objectives;

— ~~*Part 4: Product development at the system level*~~objective oriented confirmation measures;

— ~~*Part 5: Product development at the hardware level*~~management of safety anomalies;

— references to cybersecurity;

— updated target values for hardware architecture metrics;

— ~~*Part 6: Product development at the software level*~~guidance on model based development and software safety analysis;

— ~~*Part 7: Production and operation*~~evaluation of hardware elements;

— ~~*Part 8: Supporting processes*~~additional guidance on dependent failure analysis;

— ~~*Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses*~~guidance on fault tolerance, safety related special characteristics and software tools;

— ~~*Part 10: Guideline on ISO 26262*~~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.

Introduction

The ISO 26262 series of standards is the adaptation of IEC 61508 series ~~to comply with needs specific to the application sector~~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 ~~of future automobile development. New functionalities not only in areas such as driver assistance, propulsion, in vehicle dynamics control and active and passive safety systems increasingly touch the domain of system safety engineering~~in the development of road vehicles. Development and integration of ~~these~~automotive functionalities ~~will~~ strengthen the need for ~~safe system development processes~~functional safety and the need to provide evidence that ~~all reasonable system~~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 ~~avoid~~mitigate these risks by providing appropriate requirements and processes.

~~System safety is achieved through a number of safety measures, which are implemented in a variety of technologies (e.g. mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic) and applied at the various levels of the development process. Although ISO 26262 is concerned with functional safety of E/E systems, it provides a framework within which safety-related systems based on other technologies can be considered.~~To achieve functional safety, ~~ISO 26262~~the ISO 26262 series of standards:

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

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

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

d) provides requirements for ~~validation and confirmation measures to ensure a sufficient and acceptable level of safety being achieved;~~functional safety management, design, implementation, verification, validation and confirmation measures; and

e) provides requirements for relations ~~with~~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.

~~Functional~~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 ~~by~~ the management processes.

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

Figure 1 shows the overall structure of ~~this edition~~the ISO 26262 series of ~~ISO 26262~~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 ~~between~~among ISO 26262-3, ISO 26262-4, ISO 26262-5, ISO 26262-6 and ISO 26262-7;

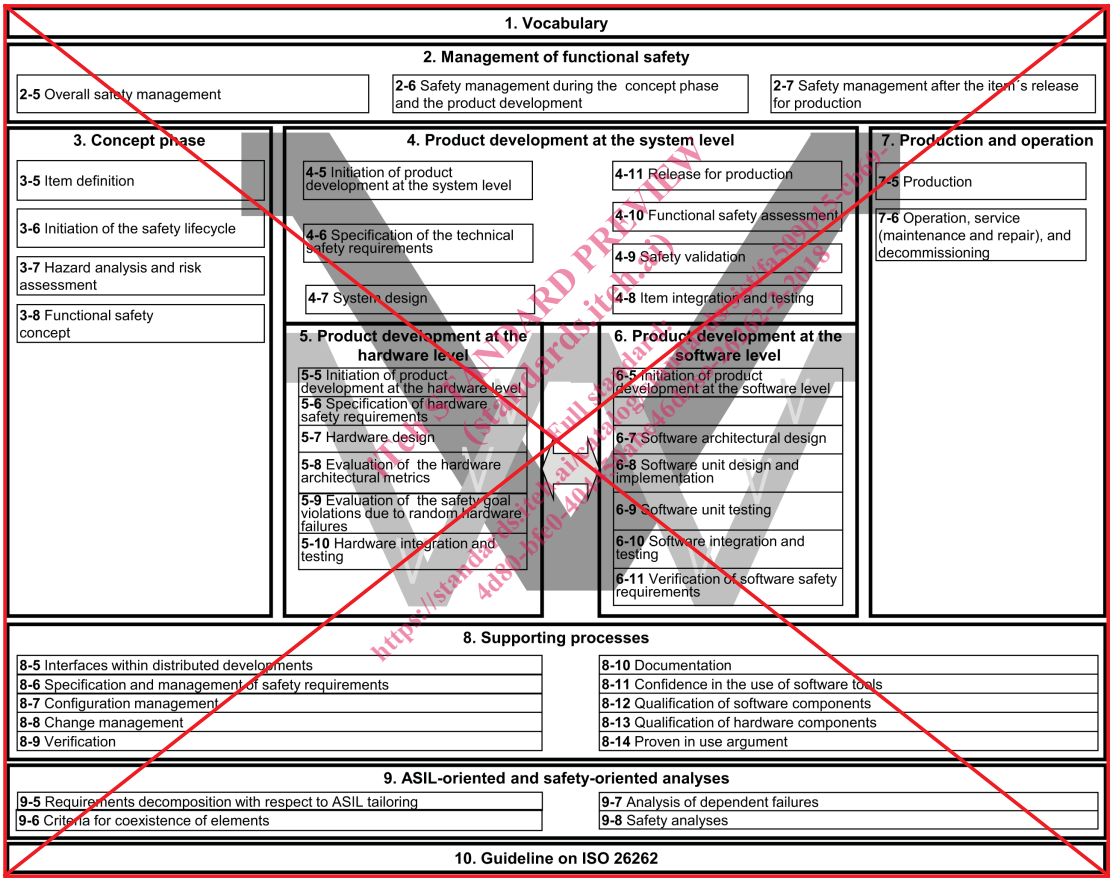
— for motorcycles:

  — 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 ~~Clause 6 of ISO 26262-2~~ISO 26262-2:2018, Clause 6.



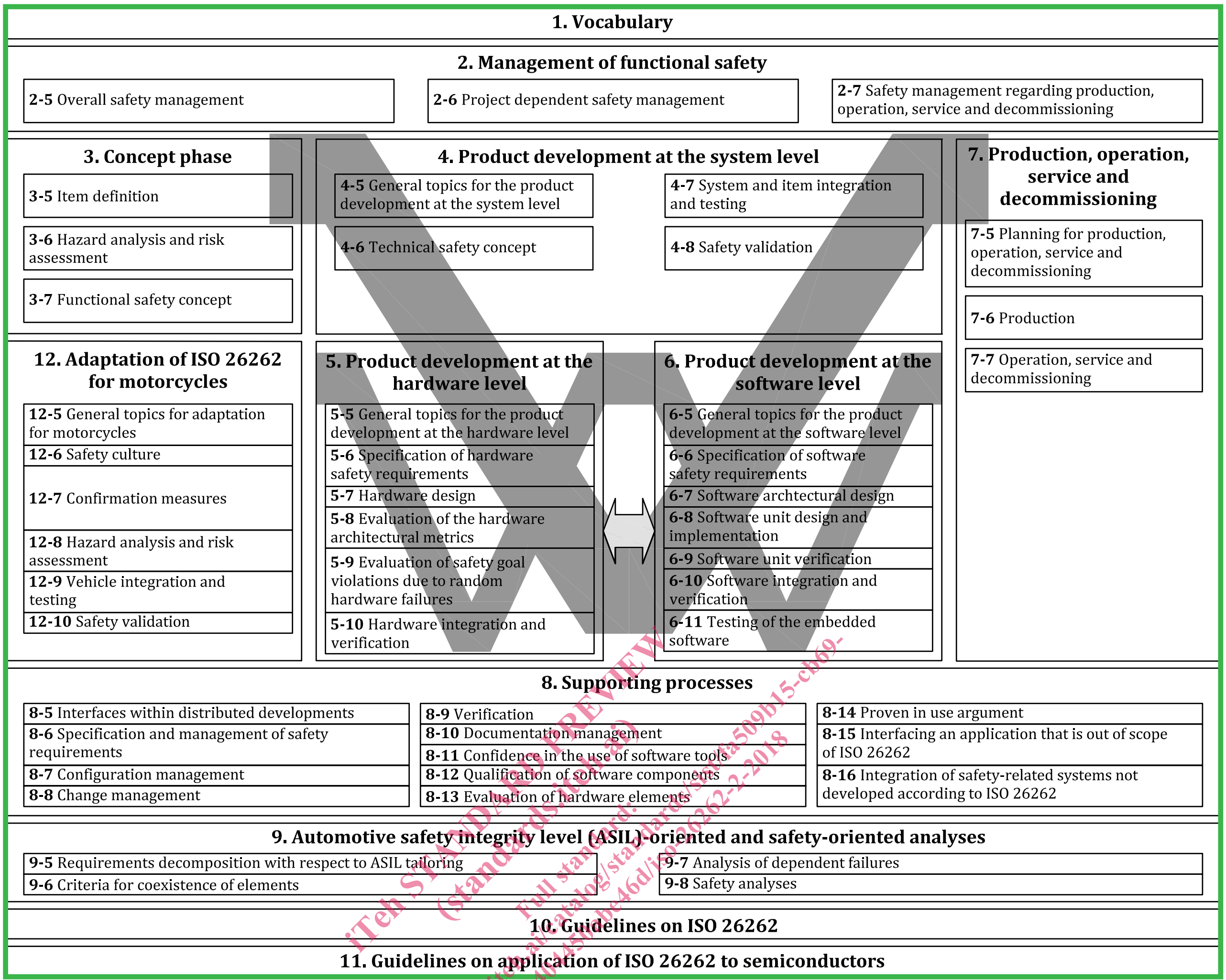


Figure 1 — Overview of ~~ISO 26262~~the ISO 26262 series of standards

Road vehicles — Functional safety —

Part 2:
Management of functional safety

1 Scope

~~ISO 26262~~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 ~~passenger cars with a maximum gross vehicle mass up to 3 500 kg~~road vehicles, excluding mopeds. ~~ISO 26262~~This document does not address unique E/E systems in special ~~purpose~~ vehicles such as ~~vehicles~~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 ~~ISO 26262~~this document, are exempted from the scope. ~~For further development or alterations based on~~ of this edition. This document addresses alterations to existing systems and their components released for production prior to the publication of ~~ISO 26262~~, ~~only the modifications will be developed in accordance with~~this document by tailoring the safety lifecycle depending on the alteration. This document addresses integration of existing systems not developed ~~ISO 26262~~according to this document and systems developed according to this document by tailoring the safety lifecycle.

~~ISO 26262~~This document addresses possible hazards caused by malfunctioning behaviour of ~~E/E~~ 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 ~~E/E~~ 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.

~~ISO 26262~~This document does not address the nominal performance of E/E systems. ~~, even if dedicated functional performance standards exist for these systems (e.g. active and passive safety systems, brake systems, Adaptive Cruise Control).~~

This ~~part of ISO 26262~~document specifies the requirements for functional safety management for automotive applications, including the following:

— project-independent requirements with regard to the organizations involved (overall safety management), and

— project-specific requirements with regard to the management activities in the safety lifecycle ~~(~~, i.e. management during the concept phase and the product development~~, and after the release for production)~~ phases (at the system, hardware and software level), and regarding production, operation, service and decommissioning.

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

2 Normative references

The following ~~referenced~~ documents are ~~indispensable for the application of~~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~~:2011~~, *Road vehicles — Functional safety — Part 1: Vocabulary*

ISO 26262-3:~~2011~~2018, *Road vehicles — Functional safety — Part 3: Concept phase*

ISO 26262-4:~~2011~~2018, *Road vehicles — Functional safety — Part 4: Product development at the system level*

ISO 26262-5:~~2011~~2018, *Road vehicles — Functional safety — Part 5: Product development at the hardware level*

ISO 26262-6:~~2011~~2018, *Road vehicles — Functional safety — Part 6: Product development at the software level*

ISO 26262-7:~~2011~~2018, *Road vehicles — Functional safety — Part 7: ~~Production and operation~~Productiond, operation, service and decommissioning*

ISO 26262-8:~~2011~~2018, *Road vehicles — Functional safety — Part 8: Supporting processes*

ISO 26262-9:~~2011~~2018, *Road vehicles — Functional safety — Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses*

3 Terms~~, definitions and abbreviated terms~~ and definitions

For the purposes of this document, the terms, definitions and abbreviated terms given in ISO 26262-1~~:2011~~ 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).

~~4.1~~4.2 General requirements

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

a) tailoring of the safety activities in accordance with this ~~part of ISO 26262~~document has been ~~planned and~~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 ~~assessed~~evaluated in accordance with this ~~part of ISO 26262~~document.

~~Information marked as a “NOTE” or “EXAMPLE”~~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.

~~4.2~~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 ~~methods shall be applied as recommended~~listed highly recommended and recommended methods in accordance with the ASIL~~. If methods other than those listed are to be applied~~ 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 ~~that these fulfil~~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.

~~4.3~~4.4 ASIL-dependent requirements and recommendations

The requirements or recommendations of each ~~subclause~~sub-clause shall be ~~complied with~~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:~~2011~~2018, Clause 5, the ASIL resulting from the decomposition shall be ~~complied with.~~met.

If an ASIL is given in parentheses in the ISO 26262 series of standards, the corresponding ~~subclause~~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.