INTERNATIONAL STANDARD

ISO 26262-11

First edition
2018-12

Road vehicles — Functional safety —

Part 11: Guidelines on application of ISO 26262 to semiconductors

Véhicules routiers — Sécurité fonctionnelle —

Partie 11: Lignes directrices sur l'application de l'ISO 26262 aux semi-conducteurs

Reference number
ISO 26262-11:2018(E)

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.

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.

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 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.

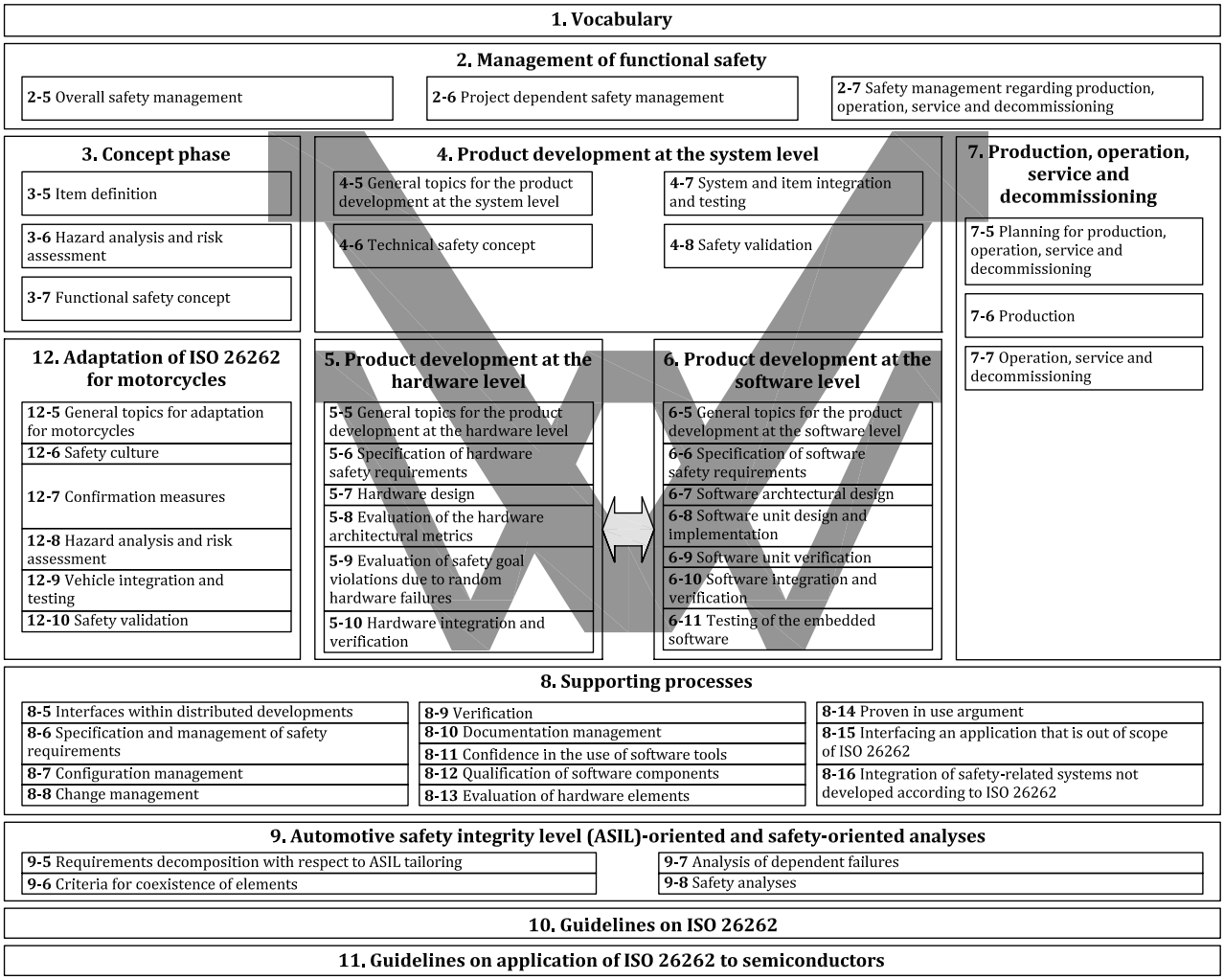

Figure 1 — Overview of the ISO 26262 series of standards

Road vehicles — Functional safety —

Part 11:
Guidelines on application of ISO 26262 to semiconductors

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 has an informative character only. It contains possible interpretations of other parts of ISO 26262 with respect to semiconductor development. The content is not exhaustive with regard to possible interpretations, i.e., other interpretations can also be possible in order to fulfil the requirements defined in other parts of ISO 26262.

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*

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 A semiconductor component and its partitioning

4.1 How to consider semiconductor components

4.1.1 Semiconductor component development

If a semiconductor component is developed as a part of an item development compliant with the ISO 26262 series of standards, it is developed based on hardware safety requirements derived from the top-level safety goals of the item, through the technical safety concept. Targets for diagnostic coverages for relevant failure modes to meet hardware architectural metrics and Probabilistic Metric for random Hardware Failures (PMHF) or Evaluation of Each Cause of safety goal violation (EEC) are allocated to the item: in this case, the semiconductor component is just one of the elements. As mentioned in the EXAMPLE of ISO 26262-5:2018 [66], 8.2, to facilitate distributed developments, target values can be assigned to the semiconductor component itself, by either deriving target values for the SPFM, LFM and PMHF at the item level or applying EEC to the HW part level. The safety analysis of a semiconductor component is performed based on the requirements and recommendations defined in ISO 26262-5:2018, 7.4.3 and in ISO 26262-9:2018 [70], Clause 8.

NOTE If an element has not been developed in compliance with the ISO 26262 series of standards, the requirements in ISO 26262-8:2018 [69], Clause 13 can be considered.

The semiconductor component can be developed as a SEooC, as described in ISO 26262-10 [61]. In this case, the development is done based on assumptions on the conditions of the semiconductor component usage (Assumptions of Use or AoU, see 4.4), and then the assumptions are verified at the next higher level of integration considering the semiconductor component requirements derived from the safety goals of the item in which the semiconductor component is to be used.

The descriptions and methods in this part are provided assuming the semiconductor component is a SEooC, but the described methods (e.g. the method for failure rate computation of a semiconductor component) are still valid if the semiconductor component is not considered as an SEooC. When those methods are conducted considering the stand-alone semiconductor component, appropriate assumptions are made. Sub-clause 4.4 describes how to adapt and verify those methods and assumptions at the system or element level. At the stand-alone semiconductor component level, the requirements of ISO 26262-2 [63], ISO 26262-5, ISO 26262-6[67], ISO 26262-7[68], ISO 26262-8 and ISO 26262-9 (e.g. related to safety analyses, dependent failure analysis, verification, etc.) can be applied.

4.2 Dividing a semiconductor component in parts

As shown in Figure 2 and according to the definitions in ISO 26262-1:2018, 3.21, a semiconductor component can be divided into parts: the whole semiconductor hierarchy can be seen as a component, the second level of hierarchy (e.g. a CPU) as a part, the following levels of hierarchy (e.g. the CPU register bank) as subparts, till the elementary subparts (its internal registers and the related logic).

NOTE The level of detail (e.g. whether to stop at part level or go down to subpart or elementary subpart level) as also the definition of the elementary subpart (e.g. flip-flop, analogue transistor) can depend on the safety concept, the stage of the analysis and on the safety mechanisms used (inside the semiconductor component or at the system or element level).

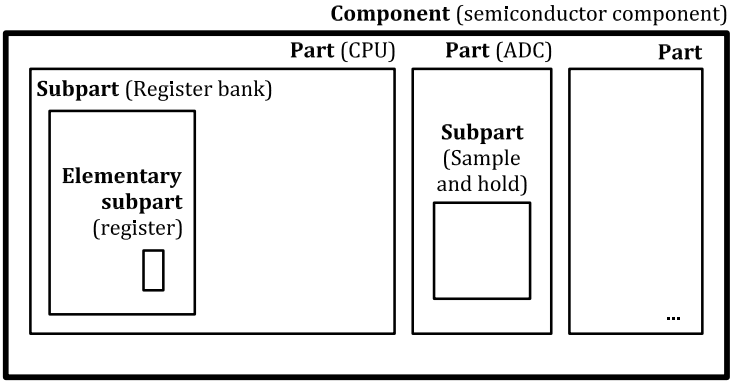

Figure 2 — A semiconductor, its parts and subparts

4.3 About hardware faults, errors and failure modes

Random hardware faults and failure modes of an integrated circuit are linked together as shown in Figure 3 below.

NOTE 1 The failure mode can be abstract or tailored to a specific implementation, e.g. related to a pin of a component, part or subpart.

In general, failure modes are described in this document as functional failure modes. Further characterisation of failure modes are possible.

EXAMPLE An example of failure modes for digital circuits is given in Annex A.

Faults and errors described in this document are related to the physical implementation of a given semiconductor component.

NOTE 2 The terms fault, error, and failure are used according to the ISO 26262-1 definitions, i.e. faults create errors which can lead to a failure. In many reliability modelling standards the terms fault and failure are used interchangeably.

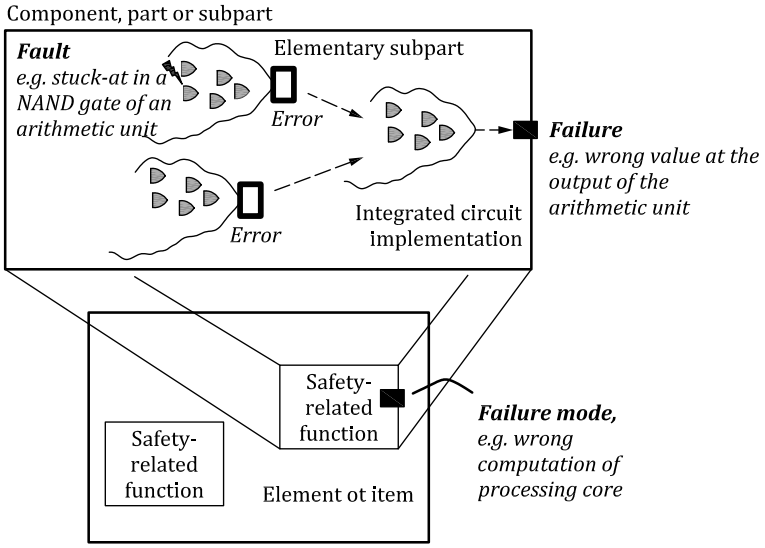

Figure 3 — Relationship between hardware faults and failure modes

4.3.1 Fault models

Fault models are an abstract representation of physical faults.