INTERNATIONAL STANDARD

ISO 26262-3

First edition
2011-11-15

Road vehicles — Functional safety —

Part 3: Concept phase

Véhicules routiers — Sécurité fonctionnelle —

Partie 3: Phase de projet

Reference number
ISO 26262-3:2011(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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 drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

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.

ISO 26262-3 was prepared by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee SC 3, *Electrical and electronic equipment*.

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

— *Part 1: Vocabulary*

— *Part 2: Management of functional safety*

— *Part 3: Concept phase*

— *Part 4: Product development at the system level*

— *Part 5: Product development at the hardware level*

— *Part 6: Product development at the software level*

— *Part 7: Production and operation*

— *Part 8: Supporting processes*

— *Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses*

— *Part 10: Guideline on ISO 26262*

Introduction

ISO 26262 is the adaptation of IEC 61508 to comply with needs specific to the application sector 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. Development and integration of these functionalities will strengthen the need for safe system development processes and the need to provide evidence that all reasonable system 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. ISO 26262 includes guidance to avoid 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. ISO 26262:

a) provides an automotive safety lifecycle (management, development, production, operation, service, decommissioning) and supports tailoring the necessary activities during these lifecycle phases;

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

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

d) provides requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety being achieved;

e) provides requirements for relations with suppliers.

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 intertwined with common function-oriented and quality-oriented development activities and work products. ISO 26262 addresses the safety-related aspects of development activities and work products.

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

— 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.

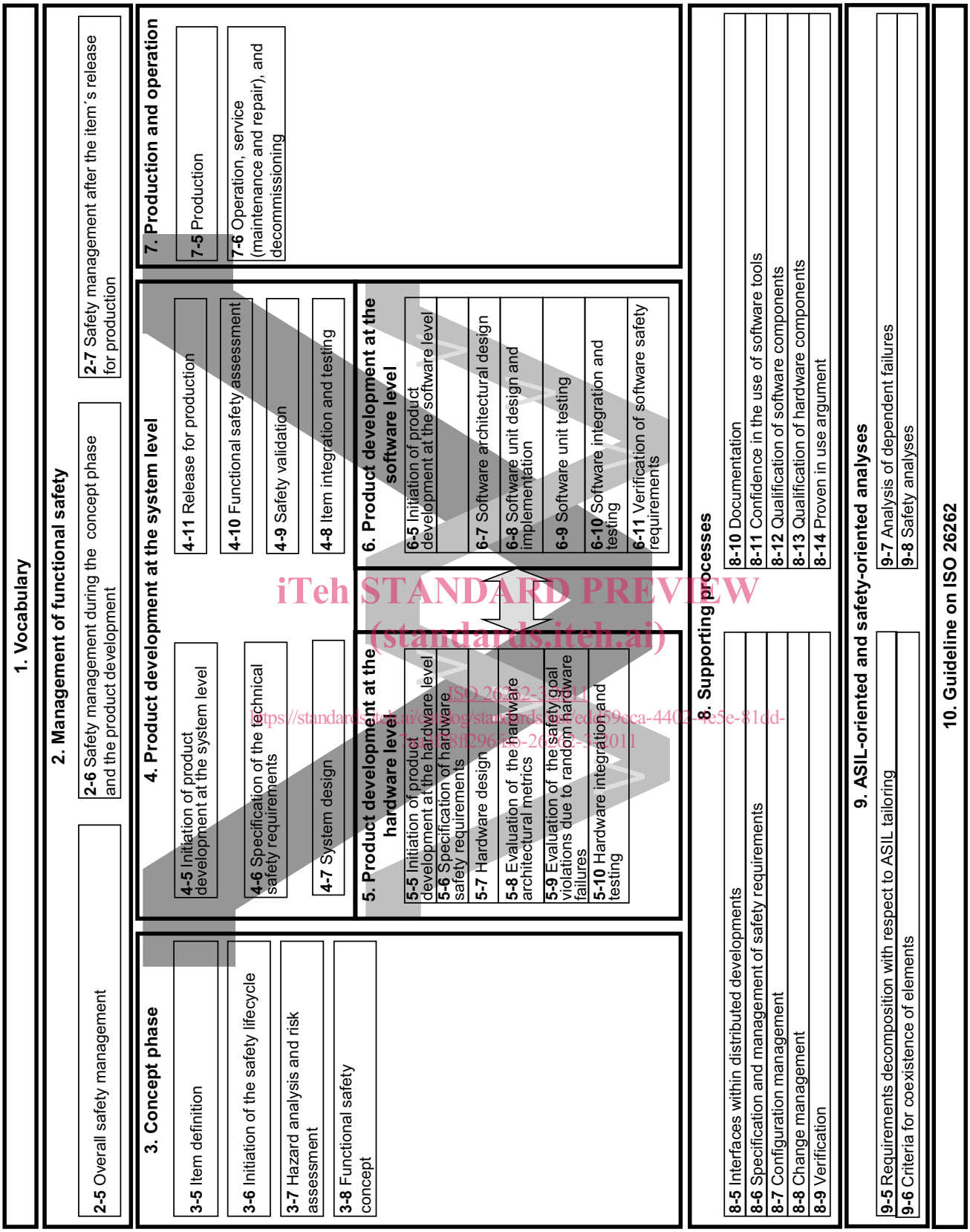

Figure 1 — Overview of ISO 26262

Road vehicles — Functional safety —

Part 3:
Concept phase

1 Scope

ISO 26262 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. ISO 26262 does not address unique E/E systems in special purpose vehicles such as vehicles designed for drivers with disabilities.

Systems and their components released for production, or systems and their components already under development prior to the publication date of ISO 26262, are exempted from the scope. For further development or alterations based on systems and their components released for production prior to the publication of ISO 26262, only the modifications will be developed in accordance with ISO 26262.

ISO 26262 addresses possible hazards caused by malfunctioning behaviour of E/E safety-related 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 systems.

ISO 26262 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 specifies the requirements for the concept phase for automotive applications, including the following:

— item definition,

— initiation of the safety lifecycle,

— hazard analysis and risk assessment, and

— functional safety concept.

2 Normative references

The following referenced documents are indispensable for the application 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 26262-2:2011, *Road vehicles — Functional safety — Part 2: Management of functional safety*

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

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

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

3 Terms, definitions and abbreviated terms

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

4 Requirements for compliance

4.1 General requirements

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

a) tailoring of the safety activities in accordance with ISO 26262-2 has been planned and 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 in accordance with ISO 26262-2.

Information marked as a “NOTE” or “EXAMPLE” 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 ISO 26262 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 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 in accordance with the ASIL. If methods other than those listed are to be applied, a rationale shall be given that these fulfil the corresponding requirement.

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 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;

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

4.3 ASIL-dependent requirements and recommendations

The requirements or recommendations of each subclause shall be complied with 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, Clause 5, the ASIL resulting from the decomposition shall be complied with.

If an ASIL is given in parentheses in ISO 26262, the corresponding subclause 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.

5 Item definition

5.1 Objectives

The first objective is to define and describe the item, its dependencies on, and interaction with, the environment and other items.

The second objective is to support an adequate understanding of the item so that the activities in subsequent phases can be performed.

5.2 General

This clause lists the requirements and recommendations for establishing the definition of the item with regard to its functionality, interfaces, environmental conditions, legal requirements, hazards, etc. This definition serves to provide sufficient information about the item to the persons who conduct the subsequent subphases: “Initiation of safety lifecycle” (see Clause 6), “Hazard analysis and risk assessment” (see Clause 7) and “Functional safety concept” (see Clause 8).

NOTE Table A.1 provides an overview of objectives, prerequisites and work products of the concept phase.

5.3 Inputs to this clause

5.3.1 Prerequisites

None.

5.3.2 Further supporting information

The following information can be considered:

— any information that already exists concerning the item, e.g. a product idea, a project sketch, relevant patents, the results of pre-trials, the documentation from predecessor items, relevant information on other independent items.

5.4 Requirements and recommendations

5.4.1 The functional and non-functional requirements of the item as well as the dependencies between the item and its environment shall be made available.

NOTE 1 Requirements can be classified as safety-related after safety goals and their respective ASIL have been defined.

NOTE 2 The required information is a necessary input for the item definition although it is not safety-related. If not already available, its generation can be triggered by the requirements of this clause.

This information includes:

a) the functional concept, describing the purpose and functionality, including the operating modes and states of the item;

b) the operational and environmental constraints;

c) legal requirements (especially laws and regulations), national and international standards;

d) behaviour achieved by similar functions, items or elements, if any;

e) assumptions on behaviour expected from the item; and

f) potential consequences of behaviour shortfalls including known failure modes and hazards.

NOTE This can include known safety-related incidents on similar items.

5.4.2 The boundary of the item, its interfaces, and the assumptions concerning its interaction with other items and elements, shall be defined considering:

a) the elements of the item;

NOTE The elements could also be based on other technology

b) the assumptions concerning the effects of the item's behaviour on other items or elements, that is the environment of the item;

c) interactions of the item with other items or elements;

d) functionality required by other items, elements and the environment;

e) functionality required from other items, elements and the environment;

f) the allocation and distribution of functions among the involved systems and elements; and

g) the operating scenarios which impact the functionality of the item.

5.5 Work products

Item definition resulting from the requirements of 5.4.

6 Initiation of the safety lifecycle

6.1 Objectives

The first objective of the initiation of the safety lifecycle is to make the distinction between a new item development and a modification to an existing item (see ISO 26262-2:2011, Figure 2).

The second objective is to define the safety lifecycle activities (see ISO 26262-2:2011, Figure 2) that will be carried out in the case of a modification.

6.2 General

Based on the item definition, the safety lifecycle is initiated by distinguishing between either a new development, or a modification of an existing item. In the case of a modification, the tailoring of the safety-related activities takes place.

6.3 Inputs to this clause

6.3.1 Prerequisites

The following information shall be available:

— item definition in accordance with 5.5.

6.3.2 Further supporting information

The following information can be considered:

— any existing information, not already covered by the item definition, being useful for conducting the impact analysis.

EXAMPLE Product concept, requests for change, implementation planning, proven in use argument.

6.4 Requirements and recommendations

6.4.1 Determination of the development category

6.4.1.1 It shall be determined whether the item is either a new development, or if it is a modification of an existing item or its environment:

a) in the case of a new development, the development shall be continued with the hazard analysis and risk assessment in accordance with Clause 7;

b) in the case of a modification of the item or its environment the applicable lifecycle subphases and activities shall be determined in accordance with 6.4.2.

NOTE A proven in use argument can be applied to modification (see ISO 26262-8:2011, Clause 14).

6.4.2 Impact analysis and possible tailored safety lifecycle, in the case of modification

6.4.2.1 An impact analysis shall be carried out in order to identify and describe the intended modification applied to the item or its environment and to assess the impact of these modifications.

NOTE 1 Modifications to the item include design modifications and implementation modifications. Design modification can result from requirements modifications (e.g. functional or performance enhancement or cost optimisation). Implementation modifications do not affect the specification or performance of the item, but only the implementation features.

EXAMPLE Implementation modifications can result from corrections of software, or the use of new development or production tools.

NOTE 2 Modifications to configuration data or calibration data are considered as modifications to the item if they impact the functional behaviour of the item.

NOTE 3 Modifications to the environment of the item can result from the installation of the item in a new target environment (e.g. another vehicle variant) or by the upgrading of other items or elements interacting with (or in the vicinity of) the item.

6.4.2.2 The impact analysis shall identify and address areas affected by the modifications to the item and modifications between previous and future conditions of use of the item, including:

a) operational situations and operating modes;

b) interfaces with the environment;

c) installation characteristics such as location within the vehicle, vehicle configurations and variants; and

d) a range of environmental conditions e.g. temperature, altitude, humidity, vibrations, Electromagnetic Interference (EMI) and fuel types.

6.4.2.3 The implication of the modification with regard to functional safety shall be identified and described.

6.4.2.4 The affected work products that need to be updated shall be identified and described.

6.4.2.5 The safety activities shall be tailored in accordance with the applicable lifecycle phases.

6.4.2.6 Tailoring shall be based on the results of the impact analysis.

6.4.2.7 The results of tailoring shall be included in the safety plan in accordance with ISO 26262-2:2011, 6.4.3.

6.4.2.8 The affected work products shall be reworked.

NOTE The affected work products include the validation plan (see ISO 26262-4).

6.4.2.9 In the case of missing work products or work products that do not comply with ISO 26262, the necessary activities to reach ISO 26262 compliance shall be determined.

6.5 Work products

6.5.1 **Impact analysis** resulting from the requirements of 6.4.2.1 to 6.4.2.4.

6.5.2 **Safety plan (refined)** resulting from the requirements 6.4.2.5 to 6.4.2.9.

7 Hazard analysis and risk assessment

7.1 Objectives

The objective of the hazard analysis and risk assessment is to identify and to categorise the hazards that malfunctions in the item can trigger and to formulate the safety goals related to the prevention or mitigation of the hazardous events, in order to avoid unreasonable risk.