INTERNATIONAL STANDARD

ISO 26262-2

First edition
2011-11-15

Road vehicles — Functional safety —

Part 2: Management of functional safety

Véhicules routiers — Sécurité fonctionnelle —

Partie 2: Gestion de la sécurité fonctionnelle

Reference number
ISO 26262-2:2011(E)

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 26262-2 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.

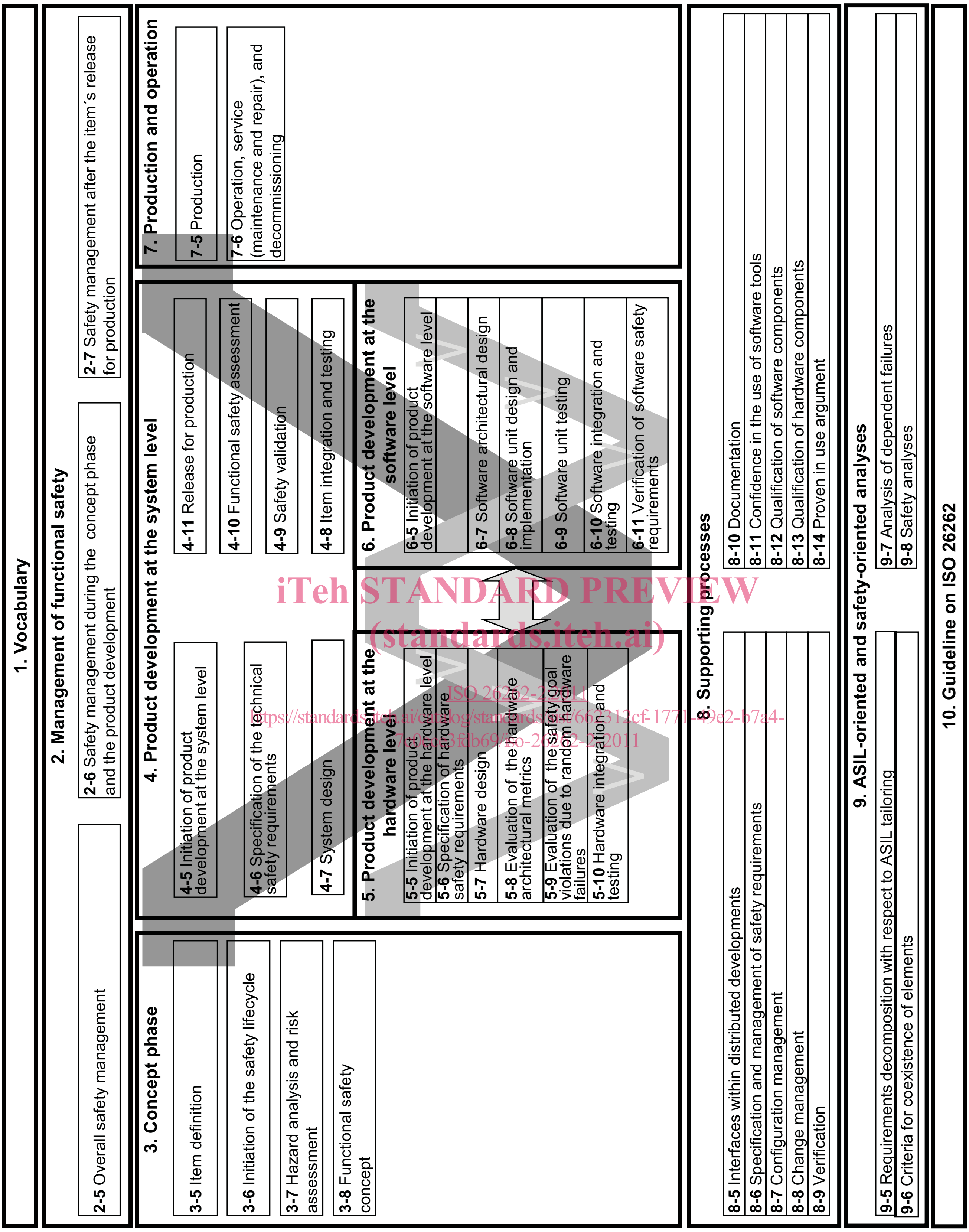


Figure 1 — Overview of ISO 26262

Road vehicles — Functional safety —

Part 2:
Management of functional safety

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 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 product development, and after the release for production).

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

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

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

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

ISO 26262-7:2011, *Road vehicles — Functional safety — Part 7: Production and operation*

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 this part of ISO 26262 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 this part of ISO 26262.

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 Overall safety management

5.1 Objective

The objective of this clause is to define the requirements for the organizations that are responsible for the safety lifecycle, or that perform safety activities in the safety lifecycle.

This clause serves as a prerequisite to the activities in the ISO 26262 safety lifecycle.

5.2 General

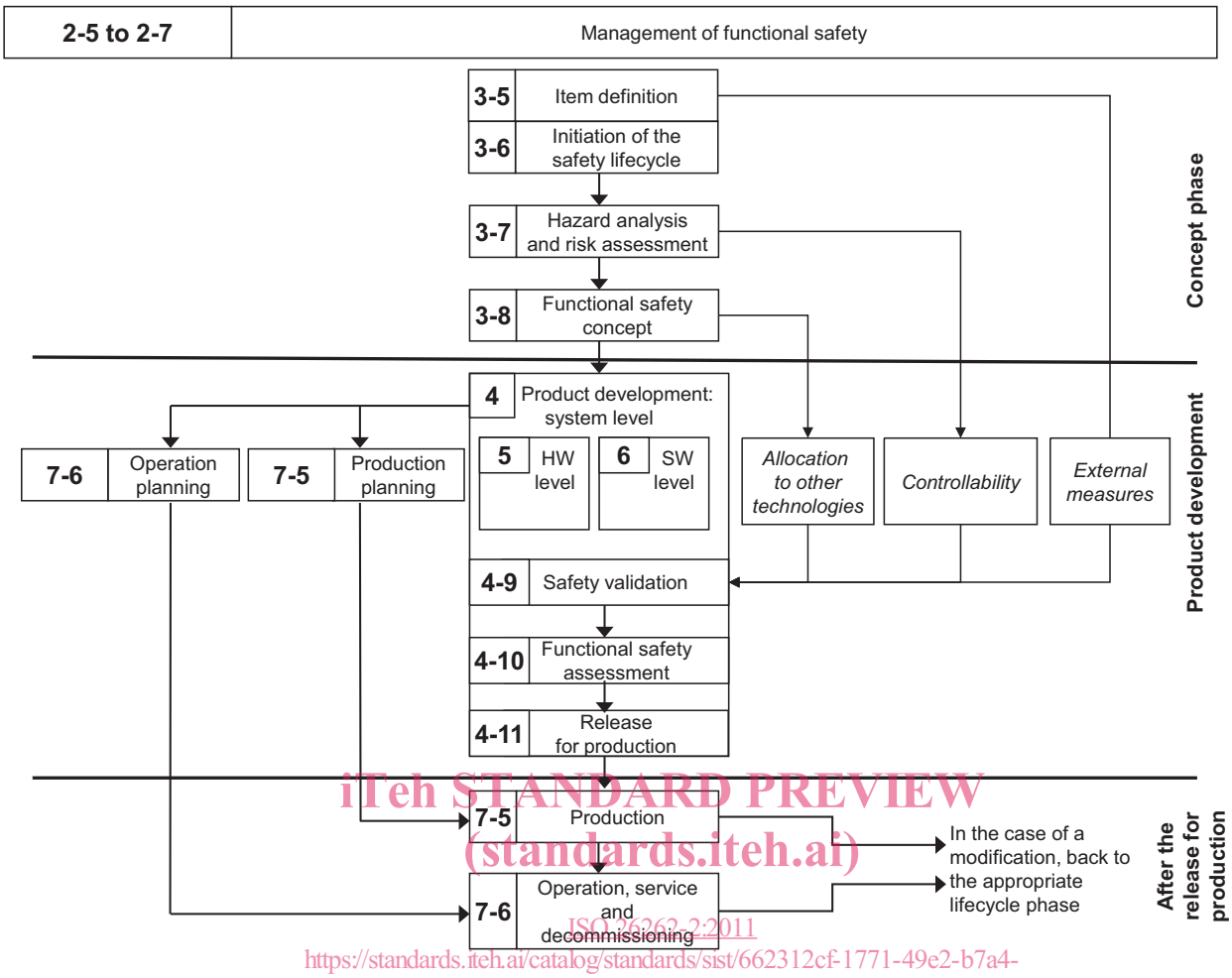
5.2.1 Overview of the safety lifecycle

The ISO 26262 safety lifecycle (see Figure 2) encompasses the principal safety activities during the concept phase, product development, production, operation, service and decommissioning. Planning, coordinating and documenting the safety activities of all phases of the safety lifecycle are key management tasks.

Figure 2 represents the reference safety lifecycle model. Tailoring of the safety lifecycle, including iterations of subphases, is allowed.

NOTE 1 The activities during the concept phase and the product development, and after the release for production are described in detail in ISO 26262-3 (concept phase), ISO 26262-4 (product development at the system level), ISO 26262-5 (product development at the hardware level), ISO 26262-6 (product development at the software level) and ISO 26262-7 (production and operation).

NOTE 2 Table A.1 provides an overview of the objectives, prerequisites and work products of the particular phases of the management of functional safety.



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. “3-6” represents Clause 6 of ISO 26262-3.

Figure 2 — Safety lifecycle

5.2.2 Explanatory remarks on the safety lifecycle

ISO 26262 specifies requirements with regard to specific phases and subphases of the safety lifecycle, but also includes requirements that apply to several, or all, phases of the safety lifecycle, such as the requirements for the management of functional safety.

The key management tasks are to plan, coordinate and track the activities related to functional safety. These management tasks apply to all phases of the safety lifecycle. The requirements for the management of functional safety are given in this part, which distinguishes:

— overall safety management (see this clause);

— safety management during the concept phase and the product development (see Clause 6);

— safety management after the item's release for production (see Clause 7).

The following descriptions explain the definitions of the different phases and subphases of the safety lifecycle, as well as other key concepts:

a) The subphase: item definition

The initiating task of the safety lifecycle is to develop a description of the item with regard to its functionality, interfaces, environmental conditions, legal requirements, known hazards, etc. The boundary of the item and its interfaces, as well as assumptions concerning other items, elements, systems and components are determined (see ISO 26262-3:2011, Clause 5).

b) The subphase: initiation of the safety lifecycle

Based on the item definition, the safety lifecycle is initiated by distinguishing between either a new development, or a modification of an existing item.

If an existing item is modified, the results of an impact analysis are used to tailor the safety lifecycle (see ISO 26262-3:2011, Clause 6).

c) The subphase: hazard analysis and risk assessment

After the initiation of the safety lifecycle, the hazard analysis and risk assessment is performed as given in ISO 26262-3:2011, Clause 7. First, the hazard analysis and risk assessment estimates the probability of exposure, the controllability and the severity of the hazardous events with regard to the item. Together, these parameters determine the ASILs of the hazardous events. Subsequently, the hazard analysis and risk assessment determines the safety goals for the item, with the safety goals being the top level safety requirements for the item. The ASILs determined for the hazardous events are assigned to the corresponding safety goals.

During the subsequent phases and subphases, detailed safety requirements are derived from the safety goals. These safety requirements inherit the ASIL of the corresponding safety goals.

d) The subphase: functional safety concept

Based on the safety goals, a functional safety concept (see ISO 26262-3:2011, Clause 8) is specified considering preliminary architectural assumptions. The functional safety concept is specified by functional safety requirements that are allocated to the elements of the item. The functional safety concept can also include other technologies or interfaces with external measures, provided that the expected behaviours thereof can be validated (see ISO 26262-4:2011, Clause 9). The implementation of other technologies is outside the scope of ISO 26262 and the implementation of the external measures is outside the scope of the item development.

e) The phase: product development at the system level

After having specified the functional safety concept, the item is developed from the system level perspective, as given in ISO 26262-4. The system development process is based on the concept of a V-model with the specification of the technical safety requirements, the system architecture, the system design and implementation on the left hand branch and the integration, verification, validation and the functional safety assessment on the right hand branch.

The hardware-software interface is specified in this phase.

Figure 1 provides an overview of the subphases of the product development at the system level.

The product development at the system level incorporates validation tasks for activities occurring within other safety lifecycle phases, including

— the validation of the aspects of the functional safety concept that are implemented by other technologies;

— the validation of the assumptions concerning the effectiveness and the performance of external measures; and

— the validation of the assumptions concerning human response, including controllability and operational tasks.

The release for production is the final subphase of the product development and provides the item's release for series production (see ISO 26262-4:2011, Clause 11).

f) The phase: product development at the hardware level

Based on the system design specification, the item is developed from the hardware level perspective (see ISO 26262-5). The hardware development process is based on the concept of a V-model with the specification of the hardware requirements and the hardware design and implementation on the left hand branch and the hardware integration and testing on the right hand branch.

Figure 1 provides an overview of the subphases of the product development at the hardware level.

g) The phase: product development at the software level

Based on the system design specification, the item is developed from the software level perspective (see ISO 26262-6). The software development process is based on the concept of a V-model with the specification of the software requirements and the software architectural design and implementation on the left hand branch, and the software integration and testing, and the verification of the software requirements on the right hand branch.

Figure 1 provides an overview of the subphases of the product development at the software level.

h) Production planning and operation planning

The planning for production and operation, and the specification of the associated requirements, starts during the product development at the system level (see ISO 26262-4). The requirements for production and operation are given in ISO 26262-7:2011, Clauses 5 and 6.

i) The phase: production and operation, service and decommissioning

This phase addresses the production processes relevant for the functional safety goals of the item, i.e. the safety-related special characteristics, and the development and management of instructions for the maintenance, repair and decommissioning of the item to ensure functional safety after the item's release for production (see ISO 26262-7:2011, Clauses 5 and 6).

j) Controllability

In the hazard analysis and risk assessment (see ISO 26262-3:2011, Clause 7), credit can be taken for the ability of the driver, or the other persons at risk, to control hazardous situations. The assumptions regarding the controllability in the hazard analysis and risk assessment and the functional and technical safety concept are validated during the safety validation (see Figure 2 and ISO 26262-4:2011, Clause 9).

NOTE The exposure and the severity are factors that depend on the scenario. The eventual controllability through human intervention is influenced by the design of the item and is therefore evaluated during the validation (see ISO 26262-4:2011, 9.4.3.2).

k) External measures

The external measures refer to the measures outside the item, as specified in the item definition (see Figure 2 and ISO 26262-3:2011, Clause 5), that reduce or mitigate the risks resulting from the item. External measures can include not only additional in-vehicle devices such as dynamic stability controllers or run-flat tyres, but also devices external to the vehicle, like crash barriers or tunnel fire-fighting systems.

