INTERNATIONAL STANDARD

ISO 26262-2

Second edition
2018-12

Road vehicles — Functional safety —

Part 2: Management of functional safety

Véhicules routiers — Sécurité fonctionnelle —

Partie 2: Gestion de la sécurité fonctionnelle

Reference number
ISO 26262-2:2018(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*.

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.

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.

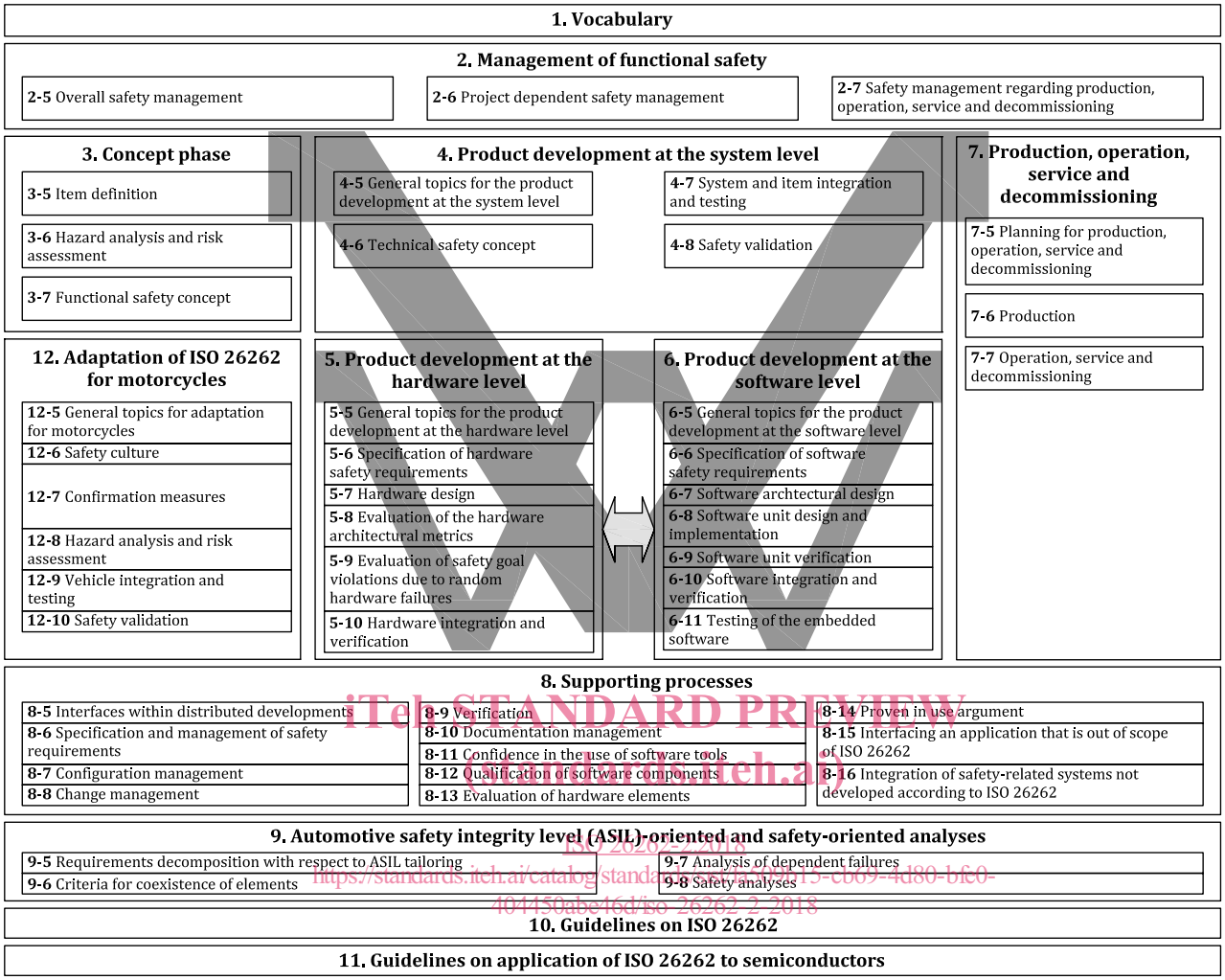


Figure 1 — Overview of the ISO 26262 series of standards

Road vehicles — Functional safety —

Part 2:
Management of functional safety

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 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 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 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 26262-3:2018, *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 26262-8:2018, *Road vehicles — Functional safety — Part 8: Supporting processes*

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:

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).

4.2 General requirements

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

a) tailoring of the safety activities in accordance with this document 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 this document.

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 this document 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 Overall safety management

5.1 Objectives

The intent of this clause is to ensure the organizations involved in the execution of the safety lifecycle, i.e. those that are responsible for the safety lifecycle or are performing safety activities in the safety lifecycle, achieve the following objectives:

a) to institute and maintain a safety culture that supports and encourages the effective achievement of functional safety and promotes effective communication with other disciplines related to functional safety;

b) to institute and maintain adequate organization-specific rules and processes for functional safety;

c) to institute and maintain processes to ensure an adequate resolution of identified safety anomalies;

d) to institute and maintain a competence management system to ensure that the competence of the involved persons is commensurate with their responsibilities; and

e) to institute and maintain a quality management system to support functional safety.

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

5.2 General

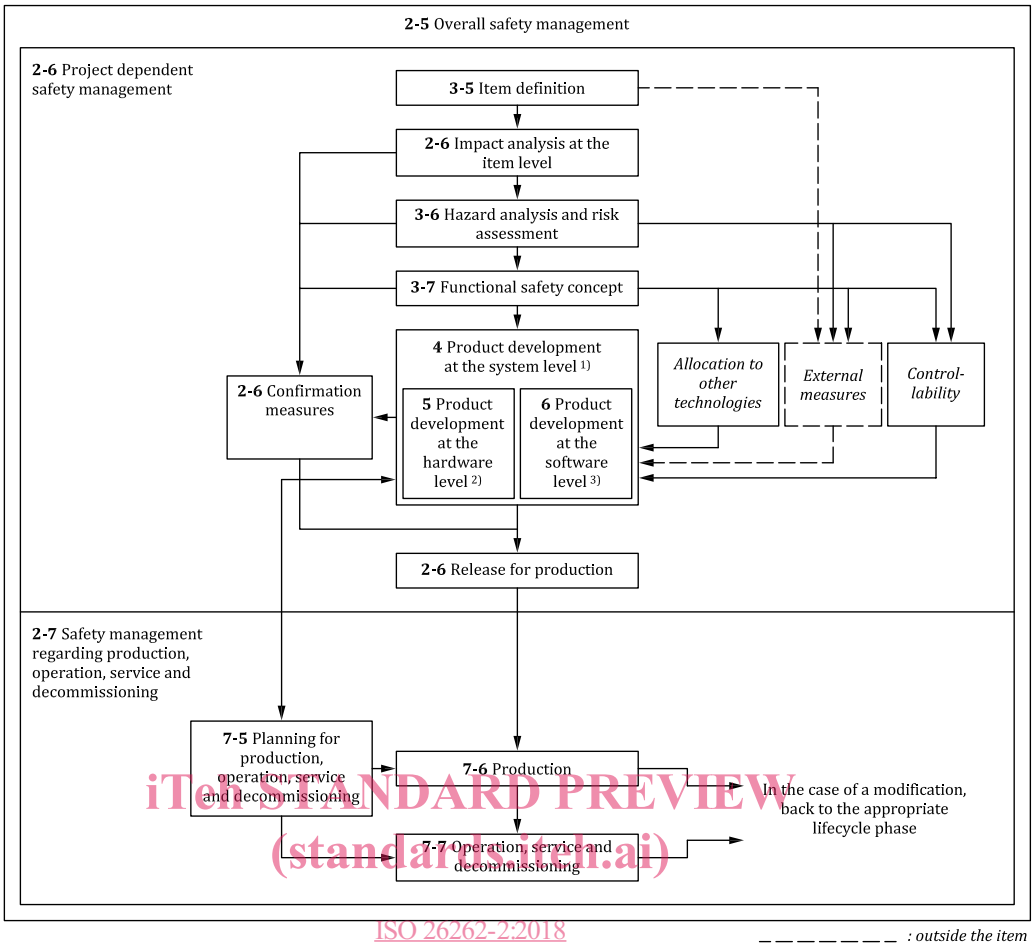
5.2.1 Overview of the safety lifecycle

The ISO 26262 reference safety lifecycle encompasses the principal safety activities during the concept phase, product development, production, operation, service and decommissioning. Planning, coordinating and monitoring the progress of the safety activities, as well as the responsibility to ensure that the confirmation measures are performed, are key management tasks and are performed throughout the lifecycle. The safety lifecycle may be tailored (see Clause 6).

NOTE 1 The safety activities during the concept phase, the product development, production, operation, service and decommissioning are described in detail in ISO 26262-3, ISO 26262-4, ISO 26262-5, ISO 26262-6 and ISO 26262-7.

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

Figure 2 illustrates the management activities in relation to the safety lifecycle.



NOTE 3 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 ISO 26262-3:2018, Clause 6.

NOTE 4 1) Sub-phases of the product development at the system level are shown in ISO 26262-4:2018, Figure 2.

NOTE 5 2) Sub-phases of the product development at the hardware level are shown in ISO 26262-5:2018, Figure 2.

NOTE 6 3) Sub-phases of the product development at the software level are shown in ISO 26262-6:2018, Figure 2.

Figure 2 — Management activities in relation to the safety lifecycle

5.2.2 Explanatory remarks on the safety lifecycle

5.2.2.1 General

The ISO 26262 series of standards specifies requirements with regard to specific phases and sub-phases 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 safety 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 Clause 5);

— project dependent safety management, regarding the concept phase and the product development phases at the system, hardware and software level (see Clause 6); and

— safety management regarding production, operation, service and decommissioning (see Clause 7).

The planning of the safety activities regarding development is initiated at the concept phase and is refined as necessary through the product development phases (system, hardware and software) until the decision to release the item, or element, for production. The planning of the activities regarding production, operation, service, and decommissioning is initiated during the product development at the system level.

Sub-clause 5.2.2.2 explains the definitions of different phases and sub-phases of the safety lifecycle. Other key concepts to take into consideration during the safety lifecycle are explained in sub-clause 5.2.2.3.

5.2.2.2 Phases and sub-phases of the safety lifecycle

a) item definition (a sub-phase of the concept phase):

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, or external measures are determined (see ISO 26262-3:2018, Clause 5).

b) hazard analysis and risk assessment (a sub-phase of the concept phase):

The hazard analysis and risk assessment is performed as given in ISO 26262-3:2018, Clause 6. 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. The assumptions regarding human behaviour, including controllability and human response, in the hazard analysis and risk assessment, the functional safety concept and the technical safety concept, as well as the technical assumptions relevant for the ASIL classification are validated (see ISO 26262-3:2018, Clause 6, ISO 26262-3:2018, Clause 7 and ISO 26262-4:2018, Clause 8).

During the subsequent phases and sub-phases, detailed safety requirements are derived from the safety goals. A safety requirement inherits the ASIL of the corresponding safety goal, or receives the ASIL after decomposition in the case requirements decomposition with respect to ASIL tailoring has been applied (see ISO 26262-9:2018, Clause 5).

c) functional safety concept (a sub-phase of the concept phase):

Based on the safety goals, a functional safety concept (see ISO 26262-3:2018, Clause 7) is developed considering the preliminary architectural assumptions. The functional safety concept is developed by deriving functional safety requirements from the safety goals and by allocating these functional safety requirements to the elements of the item. The functional safety concept may also include other technologies or rely on external measures (see ISO 26262-3:2018, Clause 7). In those cases, the corresponding assumptions or expected behaviours are validated (see ISO 26262-4:2018, Clause 8). The implementation of other technologies is outside the scope of the ISO 26262 series of standards and the implementation of the external measures is outside the scope of the item development.

d) product development at the system level

After the functional safety concept is specified, the item is developed at the system level, 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 side and the integration, verification and the safety validation on the right side.

The hardware-software interface is specified in this phase. The interfaces between hardware and software are updated during the hardware and software development.

ISO 26262-4:2018, Figure 2 provides an overview of the sub-phases of the system development.

The system development incorporates safety validation tasks for activities occurring within other safety lifecycle phases, including:

— the technical assumptions relevant for the ASIL classification;

— the validation of the assumptions concerning human behaviour, including controllability and human response;

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

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

e) product development at the hardware level

Based on the system design specification, the hardware is developed (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 side and the hardware integration and verification on the right side.

ISO 26262-5:2018, Figure 2 provides an overview of the sub-phases of the hardware development.

f) product development at the software level

Based on the system design specification, the software is developed (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 side, and the software integration and the verification on the right side.

ISO 26262-6:2018, Figure 2 provides an overview of the sub-phases of the software development.

g) production, operation, service and decommissioning

The planning of this phase (see ISO 26262-7:2018, Clause 5), and the specification of the associated requirements, starts during the product development at the system level (see ISO 26262-4) and takes place in parallel with the system, hardware and software development. Such planning can be enabled by exchanging information or requirements e.g. safety-related special characteristics or requirements that improve the ability to produce the product.

This phase addresses the processes, means and instructions to ensure functional safety regarding production, operation, service and decommissioning of the item or element. The safety-related special characteristics and the development and management of instructions for the production, operation, service (maintenance and repair) and decommissioning of the item or element (see ISO 26262-7:2018, Clauses 6 and 7) are considered.

5.2.2.3 Other key concepts

a) Confirmation measures