



Road vehicles — Functional safety —

Part 2: Management of functional safety

Véhicules routiers — Sécurité fonctionnelle —

Partie 2: Gestion de la sécurité fonctionnelle

ICS 43.040.10

In accordance with the provisions of Council Resolution 15/1993 this document is circulated in the English language only.

Conformément aux dispositions de la Résolution du Conseil 15/1993, ce document est distribué en version anglaise seulement.

To expedite distribution, this document is circulated as received from the committee secretariat. ISO Central Secretariat work of editing and text composition will be undertaken at publication stage.

Pour accélérer la distribution, le présent document est distribué tel qu'il est parvenu du secrétariat du comité. Le travail de rédaction et de composition de texte sera effectué au Secrétariat central de l'ISO au stade de publication.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

Copyright notice

This ISO document is a Draft International Standard and is copyright-protected by ISO. Except as permitted under the applicable laws of the user's country, neither this ISO draft nor any extract from it may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission being secured.

Requests for permission to reproduce should be addressed to either ISO at the address below or ISO's member body in the country of the requester.

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

Reproduction may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

Contents

Page

Foreword	iv
Introduction.....	v
1 Scope	1
2 Normative references	1
3 Terms, definitions, abbreviated terms	2
4 Requirements for compliance.....	2
4.1 General requirements	2
4.2 Interpretations of tables.....	2
4.3 ASIL dependent requirements and recommendations.....	2
5 Overall safety management.....	3
5.1 Objectives	3
5.2 General	3
5.3 Inputs to this Clause	6
5.4 Requirements and recommendations	6
5.5 Work products	8
6 Safety management during item development	8
6.1 Objectives	8
6.2 General	9
6.3 Inputs to this Clause	9
6.4 Requirements and recommendations	9
6.5 Work products	16
7 Safety management after release for production	16
7.1 Objectives	16
7.2 General	16
7.3 Inputs to this Clause	16
7.4 Requirements and recommendations	16
7.5 Work products	17
Annex A (informative) Overview on and document flow of management of functional safety.....	18
Annex B (informative) Examples of leading indicators of a safety culture.....	19
Annex C (informative) Aim of confirmation measures	20
Annex D (informative) Overview of verification reviews and confirmation measures.....	22
Annex E (informative) Example of an agenda for an assessment of functional safety for ASIL D	23
Bibliography.....	26

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: system level*
- *Part 5: Product development: hardware level*
- *Part 6: Product development: software level*
- *Part 7: Production and operation*
- *Part 8: Supporting processes*
- *Part 9: 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 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 elements that provide safety-related functions.

Safety is one of the key issues of future automobile development. New functionality not only in the area of driver assistance but also in vehicle dynamics control and active and passive safety systems increasingly touches the domain of safety engineering. Future development and integration of these functionalities will even strengthen the need of safe system development processes and the possibility to provide evidence that all reasonable safety objectives are satisfied.

With the trend of increasing 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 feasible requirements and processes.

System safety is achieved through a number of safety measures, which are implemented in a variety of technologies (for example: mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic etc). Although ISO 26262 is concerned with E/E systems, it provides a framework within which safety-related systems based on other technologies can be considered.

ISO 26262:

- provides an automotive safety lifecycle (management, development, production, operation, service, decommissioning) and supports tailoring the necessary activities during these lifecycle phases;
- provides an automotive specific risk-based approach for determining risk classes (Automotive Safety Integrity Levels, ASILs);
- uses ASILs for specifying the item's necessary safety requirements for achieving an acceptable residual risk; and
- provides requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety being achieved.

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 the development activities and work products.

Figure 1 shows the overall structure of ISO 26262. ISO 26262 is based upon a V-Model as a reference process model for the different phases of product development. The shaded "V"s represents the relations between ISO 26262-3, ISO 26262-4, ISO 26262-5, ISO 26262-6 and ISO 26262-7.

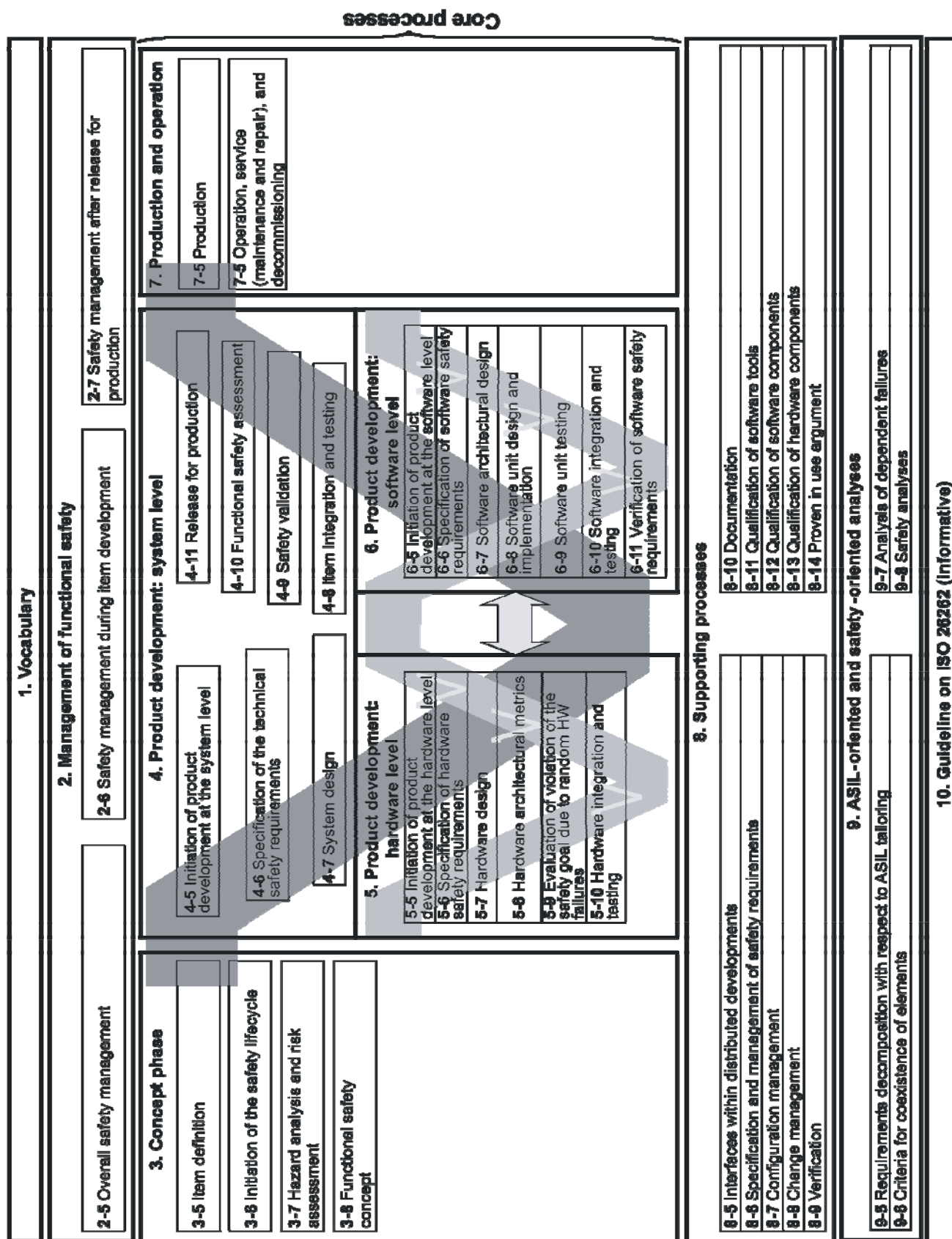


Figure 1 — Overview of ISO 26262

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 E/E systems and that are installed in series production passenger cars with a max gross weight up to 3,5 t. ISO 26262 does not address unique E/E systems in special purpose vehicles such as vehicles designed for drivers with disabilities. Systems developed prior to the publication date of ISO 26262 are exempted from the scope.

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 as 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 (for example active and passive safety systems, brake systems, ACC).

This part of ISO 26262 specifies the requirements on functional safety management for automotive applications. These requirements cover the project management activities of all safety lifecycle phases and consist of project-independent requirements, project-dependent requirements to be followed during development, and requirements that apply after 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: —¹ *Road vehicles – Functional Safety — Part 1: Vocabulary*

ISO 26262-3: —¹ *Road vehicles – Functional Safety — Part 3: Concept phase*

ISO 26262-4: —¹ *Road vehicles – Functional Safety — Part 4: Product development: system level*

ISO 26262-5: —¹ *Road vehicles – Functional Safety — Part 5: Product development: hardware level*

ISO 26262-6: —¹ *Road vehicles – Functional Safety — Part 6: Product development: software level*

ISO 26262-7: —¹ *Road vehicles – Functional Safety — Part 7: Production and operation*

ISO 26262-8: —¹ *Road vehicles – Functional Safety — Part 8: Supporting processes*

ISO 26262-9: —¹ *Road vehicles – Functional Safety — Part 9: ASIL-oriented and safety-oriented analyses*

¹ To be published

3 Terms, definitions, abbreviated terms

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

- 1) Tailoring in accordance with ISO 26262-2 has been planned and shows that the requirement does not apply.
- 2) 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" is only for guidance in understanding, or for clarification of, the associated requirement and shall not be interpreted as a requirement itself.

4.2 Interpretations of tables

Tables may be normative or informative depending on their context.

The different methods listed in a table contribute to the level of confidence that the corresponding requirement shall apply.

Each method in a table is either a consecutive entry (marked by a sequence number in the leftmost column, e.g. 1, 2, 3) or an alternative entry (marked by a number followed by a letter in leftmost column, e.g., 2a, 2b, 2c).

For consecutive entries all methods are recommended in accordance with the ASIL. If methods other than those listed are to be applied a rationale shall be given that they comply with the corresponding requirement.

For alternative entries an appropriate combination of methods shall be applied in accordance with the ASIL, independently of whether they are listed in the table or not. If methods are listed with different degrees of recommendation for an ASIL the higher one should be preferred. A rationale shall be given that the selected combination of methods complies with the corresponding requirement. If all highly recommended methods listed for a particular ASIL are selected a rationale needs not to be given.

For each method, the degree of recommendation to use the corresponding method depends on the ASIL and is categorized as follows:

"++" The method is highly recommended for this ASIL.

"+" The method is recommended for this ASIL.

"o" The method has no recommendation for or against its usage for this ASIL.

4.3 ASIL dependent requirements and recommendations

The requirements or recommendations of each subclause shall apply to 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—: Clause 5, the ASIL resulting from the decomposition will apply.

If an ASIL is given in parentheses, the corresponding subclause shall be read as a recommendation rather than a requirement for this ASIL.

5 Overall safety management

5.1 Objectives

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

This clause serves as a prerequisite to all the ISO°26262 activities in the item's safety lifecycle.

5.2 General

5.2.1 Overview of the safety lifecycle concept

The safety lifecycle (see Figure°2) encompasses principal safety activities during the concept phase, product development, and after the release for production. The planning, coordination and documentation of these activities for all phases of the safety lifecycle is a key management task.

Figure 2 represents the standard safety lifecycle model, but tailoring of the safety lifecycle, including iterations of subphases, is allowed.

NOTE The activities during concept phase, product development and after release for production are described in detail in ISO°26262-3, ISO°26262-4, ISO°26262-5, ISO°26262-6 and ISO°26262-7.

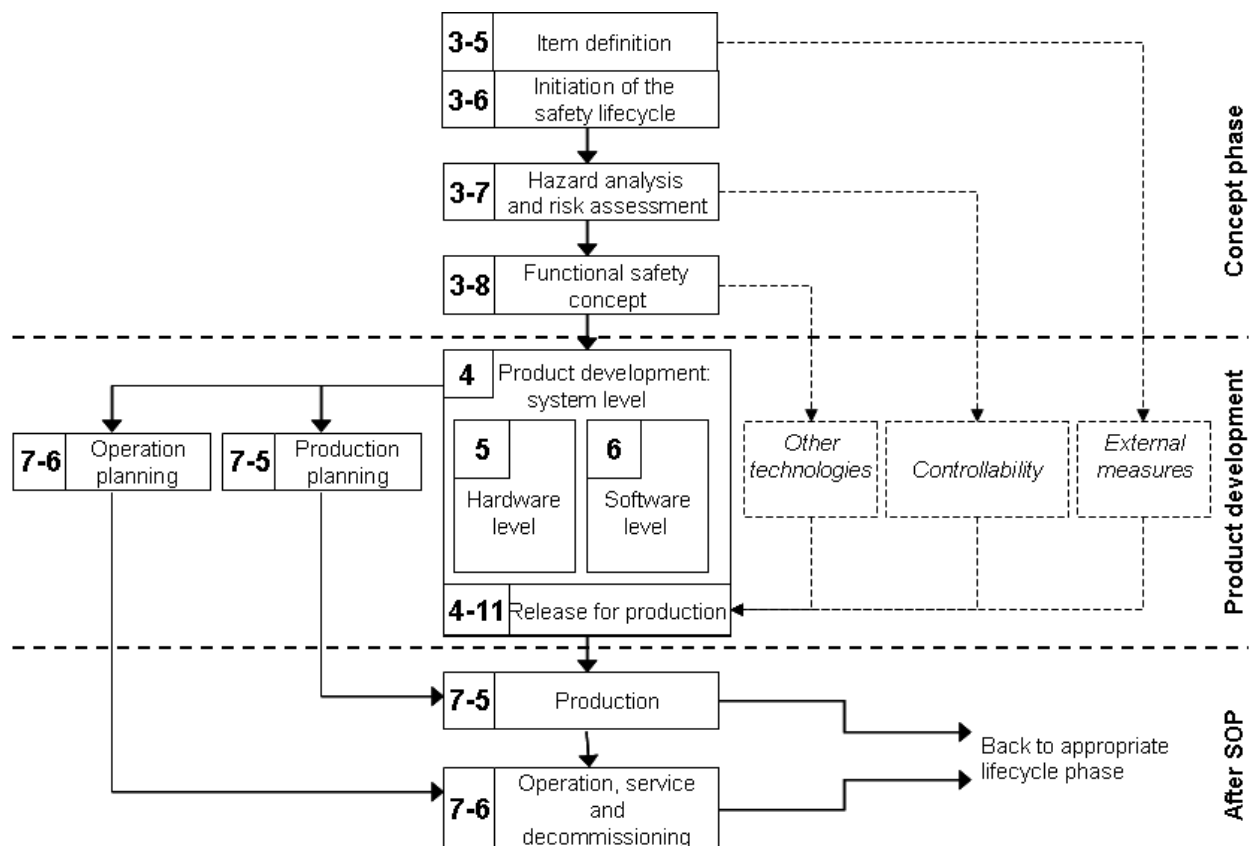


Figure 2 — Safety lifecycle

5.2.2 Explanatory remarks on the lifecycle

The organization developing safety-related systems will fulfil the requirements on functional safety, in accordance with ISO°26262, including 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 respective requirements for management of functional safety are given in this Part, which distinguishes:

- Overall safety management (see this Clause);
- Safety management during development of the item (see Clause°6);
- Safety management after release for production (see Clause°7).

The following descriptions elaborate on the definitions of the different phases of the safety lifecycle:

— 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, hazards etc. The boundary of the item and its interfaces, as well as assumptions concerning other functions, systems and components are determined (see ISO°26262-3, Clause°5).

— Initiation of the safety lifecycle

Upon the item definition, the safety lifecycle is initiated by distinguishing between either a new development, or a modification. In the case of a modification, the results of the impact analysis can be used to tailor the safety lifecycle.

— Hazard analysis and risk assessment

After the initiation of the safety lifecycle, the hazard analysis and risk assessment is performed in accordance with ISO°26262-3, Clause°7. The hazard analysis & risk assessment procedure, which considers the probability of exposure, controllability and severity, determines the ASIL of the item. In the next step, a safety goal for each hazard is derived and the respective ASIL is assigned.

— Functional safety concept

Based on the safety goals, a functional safety concept (see ISO°26262-3, Clause°8) is specified considering preliminary architectural assumptions. The functional safety concept is detailed and specified by functional safety requirements that are allocated to the elements of the item. Systems outside the item's boundary as well as other technologies can be considered as part of the functional safety concept. The requirements for implementation in other technologies or for external measures are not in the scope of ISO°26262.

— Product development at the system level

After having specified the functional safety concept, the item is developed from the system level perspective, in accordance with 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 design, and their testing, on the left-hand branch and the integration, verification, validation and assessment of functional safety on the right-hand branch.

Product development includes

- the safety validation results of those aspects of the functional safety concept implemented in other technologies;