

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 2011



COPYRIGHT PROTECTED DOCUMENT

© ISO 2011

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from 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

Published in Switzerland

Contents

Page

Foreword	iv
Introduction.....	v
1 Scope.....	1
2 Normative references.....	1
3 Terms, definitions and 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	3
5 Overall safety management.....	3
5.1 Objective	3
5.2 General	3
5.3 Inputs to this clause.....	7
5.4 Requirements and recommendations	7
5.5 Work products	9
6 Safety management during the concept phase and the product development.....	9
6.1 Objectives	9
6.2 General	9
6.3 Inputs to this clause.....	10
6.4 Requirements and recommendations	10
6.5 Work products	17
7 Safety management after the item's release for production.....	17
7.1 Objective	17
7.2 General	17
7.3 Inputs to this clause.....	17
7.4 Requirements and recommendations	18
7.5 Work products	18
Annex A (informative) Overview of and workflow of functional safety management.....	19
Annex B (informative) Examples for evaluating a safety culture.....	20
Annex C (informative) Aim of the confirmation measures	21
Annex D (informative) Overview of the verification reviews	23
Annex E (informative) Example of a functional safety assessment agenda (for items that have an ASIL D safety goal).....	24
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 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.

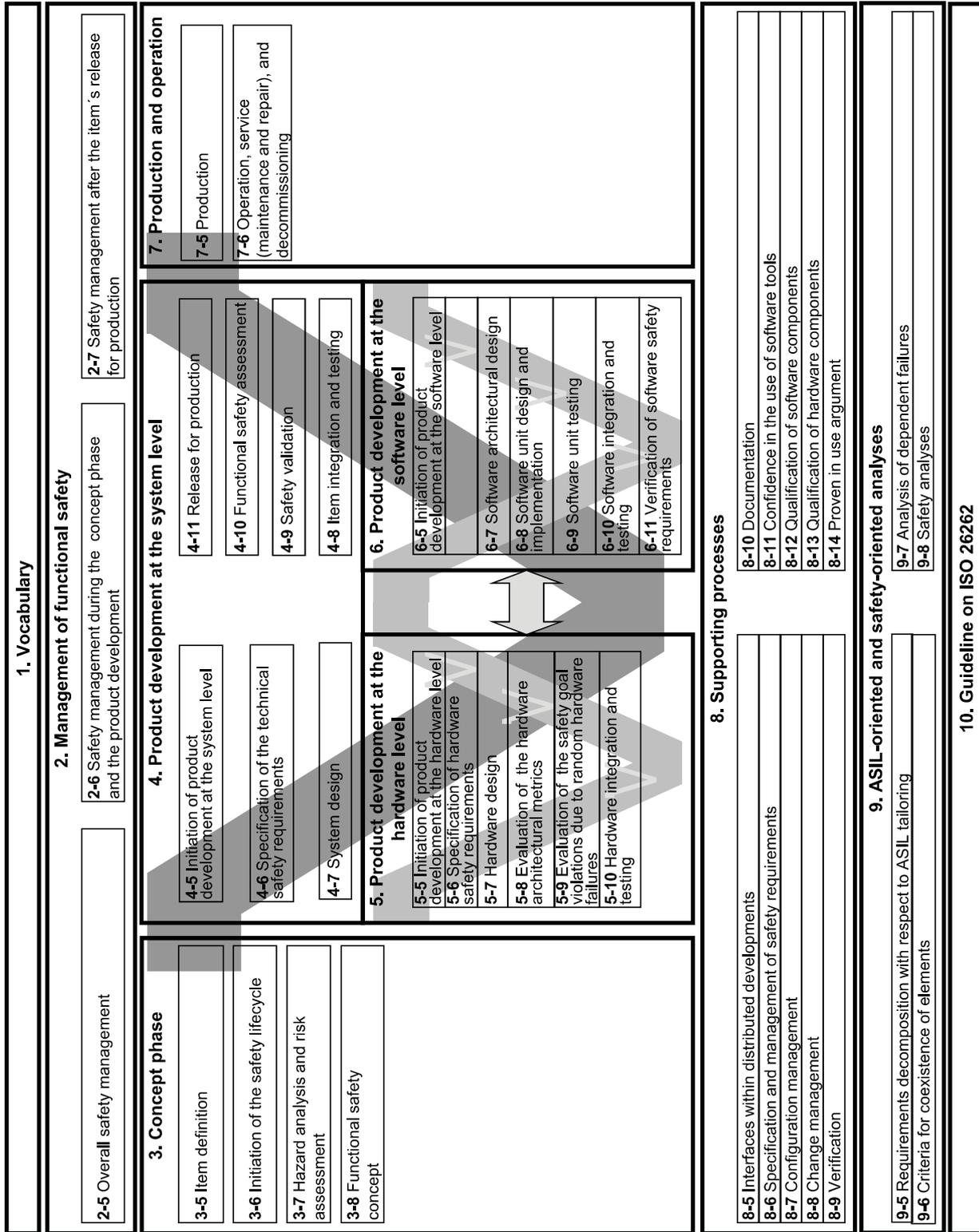


Figure 1 — Overview of ISO 26262

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 26262-2:2011(E)

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

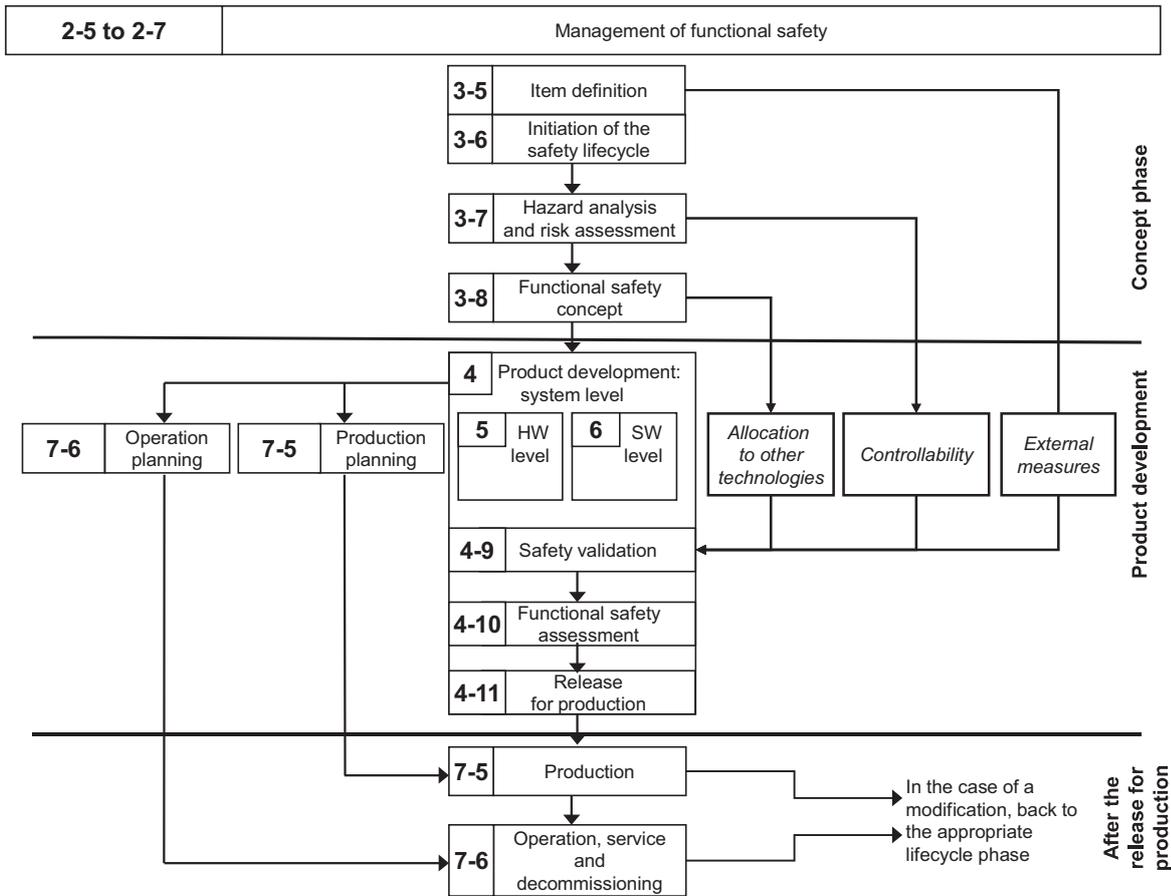
5.2.1 Overview of the safety lifecycle

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;

ISO 26262-2:2011(E)

- 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.

The assumptions regarding the external measures in the item definition, 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).

External measures can be considered in the hazard analysis and risk assessment. However, if credit is taken from an external measure in the hazard analysis and risk assessment, that external measure cannot be considered as a risk reduction in the functional safety concept.

ISO 26262 also applies to those external measures that are in the scope of ISO 26262.

l) Other technologies

Other technologies, e.g. mechanical and hydraulic technologies, are those different from electrical and/or electronic technologies that are in the scope of ISO 26262. These can be considered in the specification of the functional safety concept (see Figure 2 and ISO 26262-3:2011, Clause 8), during the allocation of safety requirements (see ISO 26262-3 and ISO 26262-4), or as an external measure.

NOTE If an implementation in another technology is specified as an external measure, then it can be useful to repeat the hazard analysis and risk assessment to consider the associated risk reduction, which could potentially result in a reduced ASIL of a corresponding safety goal.

5.3 Inputs to this clause

5.3.1 Prerequisites

None.

5.3.2 Further supporting information

The following information can be considered:

- existing evidence of a quality management system complying with a quality management standard, such as ISO/TS 16949, ISO 9001, or equivalent.

5.4 Requirements and recommendations

5.4.1 General

The organizations involved in the execution of the safety lifecycle shall comply with 5.4.2 to 5.4.5.

5.4.2 Safety culture

5.4.2.1 The organization shall create, foster, and sustain a safety culture that supports and encourages the effective achievement of functional safety.

EXAMPLE Examples for evaluating a safety culture are given in Annex B.

5.4.2.2 The organization shall institute, execute and maintain organization-specific rules and processes to comply with the requirements of ISO 26262.

NOTE Such organization-specific rules and processes can include the creation and maintenance of a generic safety plan and process description.

5.4.2.3 The organization shall institute, execute and maintain processes to ensure that identified functional safety anomalies are explicitly communicated to the applicable safety manager(s) and the other responsible persons.

ISO 26262-2:2011(E)

EXAMPLE The safety manager of the customer and the safety manager of a supplier, the safety manager of the development of a related item.

5.4.2.4 The organization shall institute, execute and maintain a safety anomaly resolution process to ensure that the analysis, evaluation, resolution and disposition of functional safety anomalies are performed in a timely and effective manner.

NOTE The anomaly resolution process can include a root cause analysis that results in a corrective action for the future.

5.4.2.5 During the execution of the safety lifecycle, the organization shall perform the required functional safety activities, including the production and management of the associated documentation in accordance with ISO 26262-8:2011, Clause 10.

5.4.2.6 The organization shall provide the resources required for the achievement of functional safety.

NOTE Resources include human resources, tools, databases, and templates.

5.4.2.7 The organization shall institute, execute and maintain a continuous improvement process, based on:

- learning from the experiences gained during the execution of the safety lifecycle of other items, including field experience; and
- derived improvements for application on subsequent items.

5.4.2.8 The organization shall ensure that the persons performing or supporting the safety activities are given sufficient authority to fulfil their responsibilities.

5.4.3 Competence management

5.4.3.1 The organization shall ensure that the persons involved in the execution of the safety lifecycle have a sufficient level of skills, competences and qualifications corresponding to their responsibilities.

NOTE 1 One of the possible means to achieve a sufficient level of skills and competences in development is a training and qualification programme that considers the following knowledge areas:

- usual safety practices, concepts and designs;
- ISO 26262 and, if applicable, further safety standards;
- organization-specific rules for functional safety;
- functional safety processes instituted in the organization.

NOTE 2 To evaluate the skills, competences and qualifications to carry out activities to comply with ISO 26262, the experience from previous professional activities can be considered, e.g.

- domain knowledge of the item;
- expertise on the environment of the item;
- management experience.

5.4.4 Quality management during the safety lifecycle

5.4.4.1 The organizations involved in the execution of the safety lifecycle shall have an operational quality management system complying with a quality management standard, such as ISO/TS 16949, ISO 9001, or equivalent.

5.4.5 Project-independent tailoring of the safety lifecycle

5.4.5.1 The organization may tailor the safety lifecycle for application across item developments, i.e. apply a project-independent tailoring, but only if such a tailoring is limited to applying one or more of the following permissions:

- a) subphases, activities or tasks may be combined or split, or

NOTE Individual subphases can be combined if the method used makes it difficult to clearly distinguish between the individual subphases, e.g. computer-aided development tools can support activities of several subphases within one step.

- b) an activity or task may be performed in a different phase or subphase, or
- c) an activity or task may be performed in an added phase or subphase, or
- d) phases or subphases may be iterated.

5.5 Work products

5.5.1 Organization-specific rules and processes for functional safety, resulting from 5.4.2 and 5.4.5.

5.5.2 Evidence of competence, resulting from 5.4.3.

5.5.3 Evidence of quality management, resulting from 5.4.4.

6 Safety management during the concept phase and the product development

6.1 Objectives

The first objective of this clause is to define the safety management roles and responsibilities, regarding the concept phase and the development phases in the safety lifecycle (see Figure 1 and Figure 2).

The second objective of this clause is to define the requirements for the safety management during the concept phase and the development phases, including the planning and coordination of the safety activities, the progression of the safety lifecycle, the creation of the safety case, and the execution of the confirmation measures.

6.2 General

Safety management includes the responsibility to ensure that the confirmation measures are performed. Depending on the applicable ASIL, some confirmation measures require independence regarding resources, management and release authority (see 6.4.7).

Confirmation measures include confirmation reviews, functional safety audits and functional safety assessments:

- the confirmation reviews are intended to check the compliance of selected work products to the corresponding requirements of ISO 26262;
- a functional safety audit evaluates the implementation of the processes required for the functional safety activities;
- a functional safety assessment evaluates the functional safety achieved by the item.

In addition to the confirmation measures, verification reviews are performed. These reviews, which are required in other parts of ISO 26262, are intended to verify that the associated work products fulfil the project requirements, and the technical requirements with respect to use cases and failure modes.

ISO 26262-2:2011(E)

Table 1 lists the required confirmation measures. Annex D lists the reviews concerning verification and refers to the applicable parts of ISO 26262.

Safety management includes the responsibility for the description and justification of any tailored safety activity (see 6.4.5).

6.3 Inputs to this clause

6.3.1 Prerequisites

The following information shall be available:

- organization-specific rules and processes for functional safety in accordance with 5.5.1;
- evidence of competence in accordance with 5.5.2;
- evidence of quality management in accordance with 5.5.3.

6.3.2 Further supporting information

If available, the following information can be considered:

- project plan (from external source);
- dependencies on other activities, including other safety activities.

6.4 Requirements and recommendations

6.4.1 General

The organizations involved in the execution of the safety lifecycle shall comply with 6.4.2 to 6.4.9 for items that have at least one safety goal with an ASIL A, B, C, or D, unless stated otherwise.

6.4.2 Roles and responsibilities in safety management

6.4.2.1 A project manager shall be appointed at the initiation of the item development.

6.4.2.2 The project manager shall be given the responsibility and the authority, in accordance with 5.4.2.8, to ensure that:

- a) the safety activities required to achieve functional safety are performed; and
- b) compliance with ISO 26262 is achieved.

6.4.2.3 The project manager shall verify that the organization has provided the required resources for the functional safety activities, in accordance with 5.4.2.6.

NOTE The estimation, determination and allocation of sufficient resources are generally performed in the planning phase.

6.4.2.4 The project manager shall ensure that the safety manager is appointed, in accordance with 5.4.3.

NOTE 1 The role of the safety manager can be fulfilled by the project manager.

NOTE 2 As the term “safety manager” is defined as a role (see ISO 26262-1), its assignment can be split between different persons in a matrix organization.

6.4.3 Planning and coordination of the safety activities

6.4.3.1 The safety manager shall be responsible for the planning and coordination of the functional safety activities in the development phases of the safety lifecycle, in accordance with 5.4.2.8.

NOTE 1 The safety manager can delegate tasks to persons that possess the required skills, competences and qualifications (see 5.4.3).

NOTE 2 The planning of the safety activities is included in the safety plan (see 6.4.3.5). Certain planned safety activities are further detailed in other work products of ISO 26262 (see 6.4.3.3).

NOTE 3 Depending on whether the item is a new development or a modification of an existing item (see ISO 26262-3:2011, Clause 6), the extent of the safety activities can vary, and the activities are planned accordingly.

6.4.3.2 The safety manager shall be responsible for maintaining the safety plan, and for monitoring the progress of the safety activities against the safety plan.

6.4.3.3 The responsibilities with regard to detailing and coordinating the safety activities in the plans listed below shall be assigned and communicated within the organization in accordance with 5.4.2.8 and 5.4.3:

- the item integration and testing plan in accordance with ISO 26262-4;
- the validation plan in accordance with ISO 26262-4;
- the software verification plan in accordance with ISO 26262-6; and
- the functional safety assessment plan in accordance with 6.4.9.

A person assigned with such a responsibility shall also be responsible for maintaining the respective plan and for monitoring the progress of these activities against the respective plan.

6.4.3.4 The safety plan shall either be

- a) referenced in the project plan, or
- b) included in the project plan, such that the safety activities are distinguishable.

NOTE The safety plan can incorporate cross-references to other information under configuration management (see ISO 26262-8:2011, Clause 7). Cross-references are generally preferable to the parallel description of activities in different work products, or in other documents that are under configuration management.

6.4.3.5 The safety plan shall include:

- a) the planning of the activities and procedures for achieving functional safety;
- b) the implementation of project-independent safety activities in accordance with Clause 5 into project-specific safety management;
- c) the definition of the tailored safety activities, in accordance with 6.4.5, if applicable;
- d) the planning of the hazard analysis and risk assessment in accordance with ISO 26262-3:2011, Clause 7;
- e) the planning of the development activities, including the development and implementation of the functional safety concept in accordance with ISO 26262-3:2011, Clause 8, the product development at the system level in accordance with ISO 26262-4, the product development at the hardware level in accordance with ISO 26262-5 and the product development at the software level in accordance with ISO 26262-6;
- f) the planning of the development interface agreement (DIA) in accordance with ISO 26262-8:2011, Clause 5, if applicable;

ISO 26262-2:2011(E)

- g) the planning of the supporting processes, in accordance with ISO 26262-8;
- h) the planning of the verification activities in accordance with ISO 26262-3, ISO 26262-4, ISO 26262-5, ISO 26262-6 and ISO 26262-8:2011, Clause 9; and the planning of the safety validation activities in accordance with ISO 26262-4:2011, Clause 9;

NOTE The verification activities are detailed in the item integration and testing plan (see ISO 26262-4) and the software verification plan (see ISO 26262-6). The validation activities are detailed in the validation plan (see ISO 26262-4). See also 6.4.3.3.

- i) the planning of the confirmation reviews, the initiation of the functional safety audit(s) and the initiation of the functional safety assessment in accordance with 6.4.7 to 6.4.9;

NOTE The level of independence given in 6.4.7, and the qualifications given in 5.4.3, of the persons that carry out the confirmation measures are specified in the safety plan.

- j) the planning of the analysis of dependent failures in accordance with ISO 26262-9:2011, Clause 7, if applicable, and the safety analyses in accordance with ISO 26262-9:2011, Clause 8;
- k) the provision of the proven in use arguments of the candidates in accordance with ISO 26262-8:2011, Clause 14, if applicable; and
- l) the provision of the confidence in the usage of software tools in accordance with ISO 26262-8:2011, Clause 11, if applicable.

6.4.3.6 The planning of a safety activity shall include describing:

- a) the objective;
- b) the dependencies on other activities or information;
- c) the resource responsible for performing the activity;
- d) the required resources for performing the activity;
- e) the starting point in time and duration; and
- f) the identification of the corresponding work product.

6.4.3.7 This requirement shall be complied with for items that have at least one safety goal with an ASIL B, C, or D: the safety plan in accordance with 6.4.3.1 to 6.4.3.6 shall be approved by an authorized person, who shall consider the confirmation review of the safety plan in accordance with 6.4.7.

6.4.3.8 Identified safety anomalies shall be reported to the safety manager, and the other responsible persons, in accordance with 5.4.2.3.

NOTE A change that results from the resolution of a safety anomaly is entered into the change management process (see ISO 26262-8:2011, Clause 8).

6.4.4 Progression of the safety lifecycle

6.4.4.1 The safety activities in a subsequent subphase of the safety lifecycle shall be started only when there is sufficient information from the pertinent subphases.

NOTE Information can be considered as sufficient if the lack of information does not cause an unacceptable risk to the achievement of the item's safety goals.

6.4.4.2 The work products required per the safety plan shall be subject to configuration management, change management and documentation, in accordance with ISO 26262-8:2011, Clauses 7, 8 and 10, respectively, no later than the time of entering the phase "product development at system level" (see Figure 1).

6.4.5 Tailoring of the safety activities

6.4.5.1 A safety activity with regard to a specific item development may be tailored i.e. omitted or performed in a different manner. If such a safety activity is tailored, then

- a) the tailoring shall be defined in the safety plan (see 6.4.3.5, c); and
- b) a rationale as to why the tailoring is adequate and sufficient to achieve functional safety shall be available.

NOTE 1 The rationale considers the ASILs of the corresponding requirements.

NOTE 2 The rationale for the tailoring is included in the safety plan and reviewed during the confirmation review of the safety plan (see 6.4.7) or during the functional safety assessment (see 6.4.9).

NOTE 3 This requirement applies to tailoring for application on a specific item. With regard to tailoring of the safety lifecycle for application across item developments within an organization, only 5.4.5 applies.

6.4.5.2 If a safety activity is tailored in accordance with 6.4.5.1 because of a modification of an existing item, then ISO 26262-3:2011, Clause 6 shall be complied with.

6.4.5.3 If a safety activity is tailored in accordance with 6.4.5.1 as a result of a proven in use argument, then ISO 26262-8:2011, Clause 14 shall be complied with.

6.4.5.4 If a safety activity is not applied in accordance with 6.4.5.1 as a result of an ASIL decomposition, then ISO 26262-9:2011, Clause 5 shall be complied with.

6.4.5.5 If a safety activity is tailored in accordance with 6.4.5.1 based on a rationale that considers the confidence in the usage of software tools, then ISO 26262-8:2011, Clause 11 shall be complied with.

6.4.5.6 If the safety activities are tailored in accordance with 6.4.5.1 because an element is developed separately from an item, then

- a) the development of the element developed separately from an item shall be based on a requirement specification that is derived from assumptions on an intended use and context, including its external interfaces; and
- b) the validity of the assumptions on the intended use and context of the element developed separately from an item shall be established.

NOTE ISO 26262 as a whole cannot be applied to an element developed separately from an item, because functional safety is not an element property (however, an element of an item can be identified as safety related). Functional safety is an item property which can be evaluated by means of a functional safety assessment.

EXAMPLE A microcontroller developed separately from an item.

6.4.6 Safety case

6.4.6.1 This requirement shall be complied with for items that have at least one safety goal with an ASIL (A), B, C or D: a safety case shall be developed in accordance with the safety plan.

6.4.6.2 The safety case should progressively compile the work products that are generated during the safety lifecycle.

6.4.7 Confirmation measures: types, independency and authority

6.4.7.1 The confirmation measures specified in Table 1 shall be performed, in accordance with the required level of independency, Table 2, 6.4.3.5 i), 6.4.8 and 6.4.9.

ISO 26262-2:2011(E)

NOTE 1 The confirmation reviews are performed for those work products that are specified in Table 1 and required by the safety plan.

NOTE 2 A confirmation review includes the checking of correctness with respect to formality, contents, adequacy and completeness regarding the requirements of ISO 26262.

NOTE 3 Table 1 includes the confirmation measures. An overview of the verification reviews is given in Annex D.

NOTE 4 A report that is a result of a confirmation measure includes the name and revision number of the work products or process documents analysed (see ISO 26262-8:2011, 10.4.5).

NOTE 5 If the item changes subsequent to the completion of confirmation reviews or functional safety assessments, then these will be repeated or supplemented (see ISO 26262-8:2011, 8.4.5.2).

NOTE 6 The aim of each confirmation measure is given in Annex C.

NOTE 7 Confirmation measures such as confirmation reviews and functional safety audits can be merged and combined with the functional safety assessment to support the handling of comparable variants of an item.

Table 1 — Required confirmation measures, including the required level of independency

Confirmation measures	Degree of independency ^a applies to ASIL				Scope
	A	B	C	D	
Confirmation review of the hazard analysis and risk assessment of the item (see ISO 26262-3:2011, Clauses 5 and 7, and, if applicable, ISO 26262-8:2011, Clause 5) Independence with regard to the developers of the item, project management and the authors of the work product	I3	I3	I3	I3	The scope of this review shall include the correctness of the determined ASILs and quality management (QM) ratings of the identified hazardous events for the item, and a review of the safety goals
Confirmation review of the safety plan (see 6.5.1) Independence with regard to the developers of the item, project management and the authors of the work product	—	I1	I2	I3	Applies to the highest ASIL among the safety goals of the item
Confirmation review of the item integration and testing plan (see ISO 26262-4) Independence with regard to the developers of the item, project management and the authors of the work product	I0	I1	I2	I2	Applies to the highest ASIL among the safety goals of the item
Confirmation review of the validation plan (see ISO 26262-4) Independence with regard to the developers of the item, project management and the authors of the work product	I0	I1	I2	I2	Applies to the highest ASIL among the safety goals of the item
Confirmation review of the safety analyses (see ISO 26262-9:2011, Clause 8) Independence with regard to the developers of the item, project management and the authors of the work products	I1	I1	I2	I3	Applies to the highest ASIL among the safety goals of the item
Confirmation review of the software tool criteria evaluation report and the software tool qualification report ^b (see ISO 26262-8:2011, Clause 11) Independence with regard to the persons performing the qualification of the software tool	—	I0	I1	I1	Applies to the highest ASIL of the requirements that can be violated by the use of the tool

Table 1 (continued)

Confirmation measures	Degree of independency ^a applies to ASIL				Scope
	A	B	C	D	
Confirmation review of the proven in use arguments (analysis, data and credit), of the candidates (see ISO 26262-8:2011, Clause 14) Independence with regard to the author of the argument	10	11	12	13	Applies to the ASIL of the safety goal or requirement related to the considered behaviour, or function, of the candidate
Confirmation review of the completeness of the safety case (see 6.5.3) Independence with regard to the authors of the safety case	10	11	12	13	Applies to the highest ASIL among the safety goals of the item
Functional safety audit in accordance with 6.4.8 Independence with regard to the developers of the item and project management	—	10	12	13	Applies to the highest ASIL among the safety goals of the item
Functional safety assessment in accordance with 6.4.9 Independence with regard to the developers of the item and project management	—	10	12	13	Applies to the highest ASIL among the safety goals of the item
^a The notations are defined as follows: — —: no requirement and no recommendation for or against regarding this confirmation measure; — 10: the confirmation measure should be performed; however, if the confirmation measure is performed, it shall be performed by a different person; — 11: the confirmation measure shall be performed, by a different person; — 12: the confirmation measure shall be performed, by a person from a different team, i.e. not reporting to the same direct superior; — 13: the confirmation measure shall be performed, by a person from a different department or organization, i.e. independent from the department responsible for the considered work product(s) regarding management, resources and release authority. ^b A software tool development is outside the item's safety lifecycle whereas the qualification of such a tool is an activity of the safety lifecycle.					

Table 2 — Procedural requirements for confirmation measures

Topic	Confirmation review	Functional safety audit	Functional safety assessment
Subject for evaluation	Work product	Implementation of the processes required for functional safety	Item as described in the item definition in accordance with ISO 26262-3:2011, Clause 5
Result	Confirmation review report ^a	Functional safety audit report ^a in accordance with 6.4.8	Functional safety assessment report in accordance with 6.4.9
Responsibility of the persons that perform the confirmation measure	Evaluation of the compliance of the work product with the corresponding requirements of ISO 26262	Evaluation of the implementation of the required processes	Evaluation of the achieved functional safety Provision of a recommendation for acceptance, a conditional acceptance or a rejection, in accordance with 6.4.9.6
Timing during the safety lifecycle	After completion of the corresponding safety activity Completion before the release for production	During the implementation of the required processes	Progressively during development, or in a single block Completion before the release for production
Scope and depth	In accordance with the safety plan	Implementation of the processes against the definitions of the activities referenced or specified in the safety plan	The work products required by the safety plan, the implementation of the required processes and a review of the implemented safety measures that can be assessed during the item development
^a This report can be included in a functional safety assessment report.			

ISO 26262-2:2011(E)

6.4.7.2 The persons who carry out a confirmation measure shall have access to, and shall be supported by, the persons and organizational entities that carry out safety activities during the item development.

6.4.7.3 The persons who carry out a confirmation measure shall have access to the relevant information and tools.

6.4.8 Functional safety audit

6.4.8.1 A functional safety audit shall be carried out for items, where the highest ASIL of the item's safety goals is ASIL (B), C, or D, in accordance with 6.4.7, 6.4.3.5 i) and 6.4.8.2.

6.4.8.2 One or more persons shall be appointed to carry out one or more functional safety audits, in accordance with 5.4.3. The appointed persons shall provide a report that contains an evaluation of the implementation of the processes required for functional safety.

NOTE 1 If a functional safety audit is performed by a Software Process Improvement and Capability Determination (SPICE) assessor, then this functional safety audit and a SPICE assessment (see ISO/IEC 15504) can be performed simultaneously. There can be sufficient commonality in content between ISO 26262 and SPICE to allow synchronization of the planning. If synchronized, the SPICE assessor can provide feedback to the functional safety auditor. However, a SPICE assessment can only be synchronized with regard to the examination of some of the supporting process specified in ISO 26262-8 and is not sufficient to perform the functional safety assessment (see 6.4.9).

NOTE 2 An organization's process definitions can address multiple standards at the same time, e.g. ISO 26262 and SPICE configuration management process requirements. This coordination of processes can help to avoid duplication of work or process inconsistencies. For these coordinated processes, organization-specific process cross-references to the requirements of ISO 26262 and to SPICE can be provided.

6.4.9 Functional safety assessment

6.4.9.1 A functional safety assessment shall be carried out for items, where the highest ASIL of the item's safety goals is ASIL (B), C, or D, in accordance with 6.4.7 and 6.4.9.2 to 6.4.9.8.

6.4.9.2 A functional safety assessment shall be planned in accordance with 6.4.3.3 and 6.4.3.5 i).

EXAMPLE Agenda for a functional safety assessment given in Annex E.

6.4.9.3 One or more persons shall be appointed to carry out a functional safety assessment, in accordance with 5.4.3. The appointed persons shall provide a report that contains a judgement of the achieved functional safety.

6.4.9.4 The scope of a functional safety assessment shall include

- the work products required by the safety plan;
- the processes required for functional safety; and

NOTE 1 The evaluation of the implemented processes can be based on the results of the functional safety audit(s).

- reviewing the appropriateness and effectiveness of the implemented safety measures that can be assessed during the item development.

NOTE 2 The safety measures that are to be implemented during the production subphase, but that cannot be assessed during the item development, are evaluated in conjunction with the production process capability (see ISO 26262-7:2011, 5.4.2.2).

6.4.9.5 A functional safety assessment shall consider:

- a) the planning of the other confirmation measures [see 6.4.3.5 i)];
- b) the results from the confirmation reviews and functional safety audit(s); and

- c) the recommendation(s) resulting from the previous functional safety assessment(s), if applicable (see 6.4.9.7, 6.4.9.8 and ISO 26262-8:2011, 8.4.5.2).

6.4.9.6 A functional safety assessment report, in accordance with 6.4.9.3, shall include a recommendation for acceptance, conditional acceptance, or rejection of the functional safety of the item. In the case of conditional acceptance:

- a) conditional acceptance shall only be given, if the functional safety of the item is considered evident, despite the identified open issues; and
- b) the recommendation for conditional acceptance shall include the deviations from the functional safety assessment criteria and the rationales as to why the specific deviations are considered acceptable.

6.4.9.7 If the recommendation in a functional safety assessment report in accordance with 6.4.9.6 is a conditional acceptance of the achieved functional safety, the corrective actions provided in the functional safety assessment report should be carried out.

6.4.9.8 If the recommendation in a functional safety assessment report in accordance with 6.4.9.6 is a rejection of the achieved functional safety, then:

- a) adequate corrective actions shall be initiated; and
- b) the functional safety assessment shall be repeated.

6.5 Work products

6.5.1 Safety plan, resulting from 6.4.3 to 6.4.5.

6.5.2 Project plan (refined), resulting from 6.4.3.4.

6.5.3 Safety case, resulting from 6.4.6.

6.5.4 Functional safety assessment plan, resulting from 6.4.9.

6.5.5 Confirmation measure reports, resulting from 6.4.7 to 6.4.9.

7 Safety management after the item's release for production

7.1 Objective

The objective of this clause is to define the responsibilities of the organizations and persons responsible for functional safety after the item's release for production. This relates to the general activities for ensuring the required functional safety of the item during the lifecycle subphases after the release for production.

7.2 General

See 5.2.

7.3 Inputs to this clause

7.3.1 Prerequisites

The following information shall be available:

- evidence of quality management in accordance with 5.5.3.

7.3.2 Further supporting information

None.

7.4 Requirements and recommendations

7.4.1 General

The organizations involved in the execution of the safety lifecycle shall comply with 7.4.2 for items that have at least one safety goal with an ASIL A, B, C, or D.

7.4.2 Responsibilities, planning and required processes

7.4.2.1 The organization shall appoint persons with the responsibility and the corresponding authority, in accordance with 5.4.2.8, to maintain the functional safety of the item after its release for production.

7.4.2.2 The activities for ensuring the functional safety of the item after its release for production shall be planned, in accordance with ISO 26262-7, and shall be initiated during the product development at the system level in accordance with ISO 26262-4.

7.4.2.3 The organization shall institute, execute and maintain processes in order to maintain the functional safety of the item in the lifecycle phases after the release for production.

7.4.2.4 The organization shall institute, execute and maintain a field monitoring process with respect to the item's functional safety.

NOTE 1 The field monitoring process for safety incidents includes the reporting of incidents, the measures for correction, e.g. a recall, as well as the corresponding decision-making processes.

NOTE 2 The data collected from field monitoring can be used for proven in use arguments (see ISO 26262-8:2011, Clause 14).

7.4.2.5 If the item changes after its release for production, the release for production in accordance with ISO 26262-4:2011, Clause 11, shall be reissued.

NOTE These changes are subject to change management (see ISO 26262-8:2011, Clause 8).

7.5 Work products

7.5.1 Evidence of field monitoring, resulting from 7.4.2.4.

Annex A (informative)

Overview of and workflow of functional safety management

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

Table A.1 — Functional safety management: overview

Clause	Objectives	Prerequisites	Work products
5 Overall safety management	<p>The objective of Clause 5 is to define the requirements for the organizations that are responsible for the safety lifecycle, or that perform safety activities in the safety lifecycle.</p> <p>Clause 5 serves as a prerequisite to the activities in the ISO 26262 safety lifecycle.</p>	None	<p>5.5.1 Organization-specific rules and processes for functional safety.</p> <p>5.5.2 Evidence of competence.</p> <p>5.5.3 Evidence of quality management.</p>
6 Safety management during the concept phase and the product development	<p>The first objective of Clause 6 is to define the safety management roles and responsibilities, regarding the concept phase and the development phases in the safety lifecycle.</p> <p>The second objective of Clause 6 is to define the requirements for the safety management during the concept phase and the development phases, including the planning and coordination of the safety activities, the progression of the safety lifecycle, the creation of the safety case, and the execution of the confirmation measures.</p>	<p>Organization-specific rules and processes for functional safety (see 5.5.1)</p> <p>Evidence of competence (see 5.5.2)</p> <p>Evidence of quality management (see 5.5.3)</p>	<p>6.5.1 Safety plan.</p> <p>6.5.2 Project plan (refined).</p> <p>6.5.3 Safety case.</p> <p>6.5.4 Functional safety assessment plan.</p> <p>6.5.5 Confirmation measure reports.</p>
7 Safety management after the item's release for production	<p>The objective of Clause 7 is to define the responsibilities of the organizations and persons responsible for functional safety after the item's release for production. This relates to the general activities for ensuring the required functional safety of the item during the lifecycle subphases after the release for production.</p>	Evidence of quality management (see 5.5.3).	7.5 Evidence of field monitoring.

Annex B
(informative)

Examples for evaluating a safety culture

Table B.1 — Examples for evaluating a safety culture

Examples indicative of a poor safety culture	Examples indicative of a good safety culture
Accountability is not traceable	The process assures that accountability for decisions related to functional safety is traceable
Cost and schedule always take precedence over safety and quality	Safety is the highest priority
The reward system favours cost and schedule over safety and quality	The reward system supports and motivates the effective achievement of functional safety The reward system penalizes those who take shortcuts that jeopardize safety or quality
Personnel assessing safety, quality and their governing processes are influenced unduly by those responsible for executing the processes	The process provides adequate checks and balances, e.g. the appropriate degree of independence in the integral processes (safety, quality, verification, validation and configuration management)
Passive attitude towards safety, e.g. — heavy dependence on testing at the end of the product development cycle, — management reacts only when there is a problem in the field	Proactive attitude towards safety, e.g. — safety and quality issues are discovered and resolved from the earliest stage in the product lifecycle
The required resources are not planned or allocated in a timely manner	The required resources are allocated Skilled resources have the competence commensurate with the activity assigned
“Groupthink” “Stacking the deck” when forming review groups Dissenter is ostracised or labelled as “not a team player” Dissent reflects negatively on performance reviews “Minority dissenter” is labelled or treated as a “troublemaker”, “not a team player” or a “whistleblower” Concerned employees fear repercussion	The process uses diversity to advantage: — intellectual diversity is sought, valued and integrated in all processes — behaviour which counters the use of diversity is discouraged and penalised Supporting communication and decision-making channels exist and the management encourages their usage: — self-disclosure is encouraged — disclosure of discovery by anyone else is encouraged — the discovery and resolution process continues in the field
No systematised continuous improvement processes, learning cycles or other forms of “lessons learned”	Continuous improvement is integral to all processes
Processes are “ad hoc” or implicit	A defined, traceable and controlled process is followed at all levels, including: — management — engineering — development interfaces — verification — validation — functional safety audit — functional safety assessment

Annex C

(informative)

Aim of the confirmation measures

C.1 Review of the safety plan (see 6.5.1)

C.1.1 Evaluation of the compliance of the safety plan with the ISO 26262 safety lifecycle. If applicable, evaluation of the tailoring of the safety activities, i.e. concerning the safety activities that are omitted or performed in a different manner compared to the reference safety lifecycle, including the corresponding rationales (see 6.4.5).

C.1.2 Evaluation of the compliance of the safety plan with the ISO 26262 requirements on the planning of the safety activities (see 6.4.3 to 6.4.5).

C.2 Review of the completeness of the safety case (see 6.5.3)

C.2.1 Confirmation that the work products referenced in the safety case are available and sufficiently complete, so that the item's achievement of functional safety can be adequately evaluated.

NOTE The referenced work products can be the work products that are identified as relevant to support the safety case.

C.2.2 Confirmation that the work products referenced in the safety case:

- are traceable from one to another,
- have no contradictions within or between work products, and
- either have no open issues that can lead to the violation of a safety goal, or have only open issues that are controlled and have a plan for closure.

C.3 Functional safety audit (see 6.4.8 and 6.5.5)

Evaluation of the implementation of the functional safety processes, during the execution of these processes, against the definitions of the activities referenced or specified in the safety plan.

C.4 Functional safety assessment (see 6.4.9 and 6.5.5)

C.4.1 Evaluation of the compliance of the work products required by the safety plan with the corresponding requirements of ISO 26262, including but not limited to the work products that require a confirmation review. For the latter work products, the results of the confirmation reviews are also considered.

C.4.2 Evaluation of the implementation of the functional safety processes, considering the results of the performed functional safety audit(s) (see 6.4.8).

C.4.3 A review of the appropriateness and effectiveness of the implemented safety measures that can be assessed during the item development.

ISO 26262-2:2011(E)

C.4.4 Follow-up of the recommendations resulting from the previous functional safety assessments, including any performed corrective actions, if applicable (see 6.4.9.7 and 6.4.9.8).

C.5 Review of the hazard analysis and risk assessment (see ISO 26262-3:2011, Clause 7, and, if applicable, ISO 26262-8:2011, Clause 5)

Evaluation of the completeness of the hazard analysis and risk assessment, and of the correctness of the determined ASILs (including QM) and the safety goals, considering the ISO 26262 hazard analysis and risk assessment procedure.

C.6 Review of the item integration and testing plan (see ISO 26262-4)

Evaluation of the compliance of the item integration and testing plan with the ISO 26262 requirements on the integration and testing activities.

C.7 Review of the validation plan (see ISO 26262-4)

Evaluation of the compliance of the validation plan with the ISO 26262 requirements on the safety validation activities.

C.8 Review of the proven in use arguments of the candidates (see ISO 26262-8:2011, Clause 14), if applicable

C.8.1 Evaluation to determine whether the results of the proven in use analyses justify the claimed proven in use credits of the candidates (with regard to any associated tailoring of safety activities).

C.8.2 Evaluation of the efficiency of the field monitoring process.

C.8.3 Evaluation of the candidate changes that are considered by the proven in use argument.

C.9 Review of the software tool criteria evaluation report and the software tool qualification report (see ISO 26262-8:2011, Clause 11)

C.8.1 Confirmation of the correct evaluation of the required level of confidence in the software tool(s) used in the development of an item or a safety-related element.

C.8.2 Evaluation of the qualification of the software tool(s), considering the required level of confidence of the respective software tools.

C.10 Review of the safety analyses (see ISO 26262-9:2011, Clause 8)

Evaluation of the correct execution of the safety analyses that can identify faults or inadequate safety mechanisms that can lead to the violation of a safety goal.

Annex D (informative)

Overview of the verification reviews

Table D.1 provides an overview of verification reviews which are required in other parts of ISO 26262 (see also ISO 26262-8:2011, Clause 9).

Table D.1 — Overview of verification reviews

Verification review subject	Highest ASIL among the safety goals of the item				Clause in which required or recommended
	A	B	C	D	
Hazard analysis and risk assessment of the item (see ISO 26262-3:2011, Clauses 5 and 7, and, if applicable, ISO 26262-8:2011, Clause 5)	required ^a				ISO 26262-3:2011, Clause 7
Safety goals	required				ISO 26262-3:2011, Clause 7
Functional safety concept	required				ISO 26262-3:2011, Clause 8
Technical safety requirements specification	required				ISO 26262-4:2011, Clause 6
System design	required				ISO 26262-4:2011, Clause 7
Hardware safety requirements	required				ISO 26262-5:2011, Clause 6
Hardware design	required				ISO 26262-5:2011, Clause 7
Results of the applied methods with regard to the evaluation of the hardware architectural metrics	b	recommended	required	required	ISO 26262-5:2011, Clause 8
Analysis of the potential safety goal violations due to random hardware failures, considering the applied evaluation method	b	recommended	required	required	ISO 26262-5:2011, Clause 9
Software safety requirements and the refined hardware-software interface requirements	required				ISO 26262-6:2011, Clauses 6 and 11
Software architectural design	required				ISO 26262-6:2011, Clause 7
Software unit design and implementation	required				ISO 26262-6:2011, Clause 8
Software component qualification report	required for the qualified software components				ISO 26262-8:2011, Clause 12
Hardware component qualification report	required for the qualified hardware components				ISO 26262-8:2011, Clause 13
Safety analyses	required				ISO 26262-9:2011, Clause 8
^a The scope of this review also includes hazardous events rated as QM.					
^b No requirement and no recommendation for or against.					

Annex E (informative)

Example of a functional safety assessment agenda (for items that have an ASIL D safety goal)

E.1 Safety management

- E.1.1** Application of the organization's safety culture and supporting processes in the assessed project.
- E.1.2** Application of the competence management and the continuous improvement practice in the assessed project.
- E.1.3** Roles and responsibilities in the assessed project.
- E.1.4** Safety plan of the assessed project and planning of the distributed development.
- E.1.5** Tailoring of the safety lifecycle, including the proven in use arguments of the candidates, of the assessed project.
- E.1.6** Functional safety audits, the safety case and available documents.

E.2 Safety activities during the concept phase

- E.2.1** Item definition.
- E.2.2** Hazard analysis and risk assessment.
- E.2.3** Functional safety concept.
- E.2.4** Dependencies of the item and its safety concept with other systems/functions.
- E.2.5** Allocation of functional safety requirements to:
 - E/E elements;
 - elements implemented by other technologies;
 - interfaces with external measures.
- E.2.6** Verification of the functional safety concept.

E.3 Safety activities during the system development

- E.3.1** Planning of the system development, integration and validation.
- E.3.2** Technical safety concept and its verification.
- E.3.3** System design and avoidance of systematic failures.
- E.3.4** Allocation of the technical safety requirements to hardware and software elements and a review of the hardware-software interface.

E.3.5 Verification of the system design.

E.4 Hardware development

E.4.1 Planning of the hardware development, qualification and integration.

E.4.2 Hardware safety requirements, hardware design and verification.

E.4.3 Hardware architectural constraints.

E.4.4 Evaluation of the probability of violation of the safety goals by random hardware failures.

E.4.5 Hardware integration and testing.

E.5 Software development

E.5.1 Planning of the software development, qualification and integration.

E.5.2 Software safety requirements, software architectural design, software unit design and implementation.

E.5.3 Software unit testing.

E.5.4 Software integration and testing.

E.5.5 Verification of the software safety requirements.

E.6 Item integration

E.6.1 Planning of the integration tests.

E.6.2 Hardware-software integration and testing.

E.6.3 System/item integration.

E.6.4 Vehicle integration.

E.7 Safety validation and the release for production

E.7.1 Validation activities.

E.7.2 Validation documentation and the release for production.

E.8 Planning of production and maintenance

E.8.1 Safety-related special characteristics for production.

E.8.2 Safety-related special characteristics for operation, service and decommissioning.

E.9 Summary

Functional safety assessment documentation, the recommendations and actions to be taken after the functional safety assessment.

Bibliography

- [1] ISO 9001, *Quality management systems — Requirements*
- [2] ISO/TS 16949, *Quality management systems — Particular requirements for the application of ISO 9001:2008 for automotive production and relevant service part organizations*
- [3] ISO/IEC 15504 (all parts), *Information technology — Process assessment*
- [4] IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

This page is intentionally blank.

This page is intentionally blank.

ISO 26262-2:2011(E)

ICS 43.040.10

Price based on 26 pages

© ISO 2011 – All rights reserved