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)

COPYRIGHT PROTECTED DOCUMENT

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.

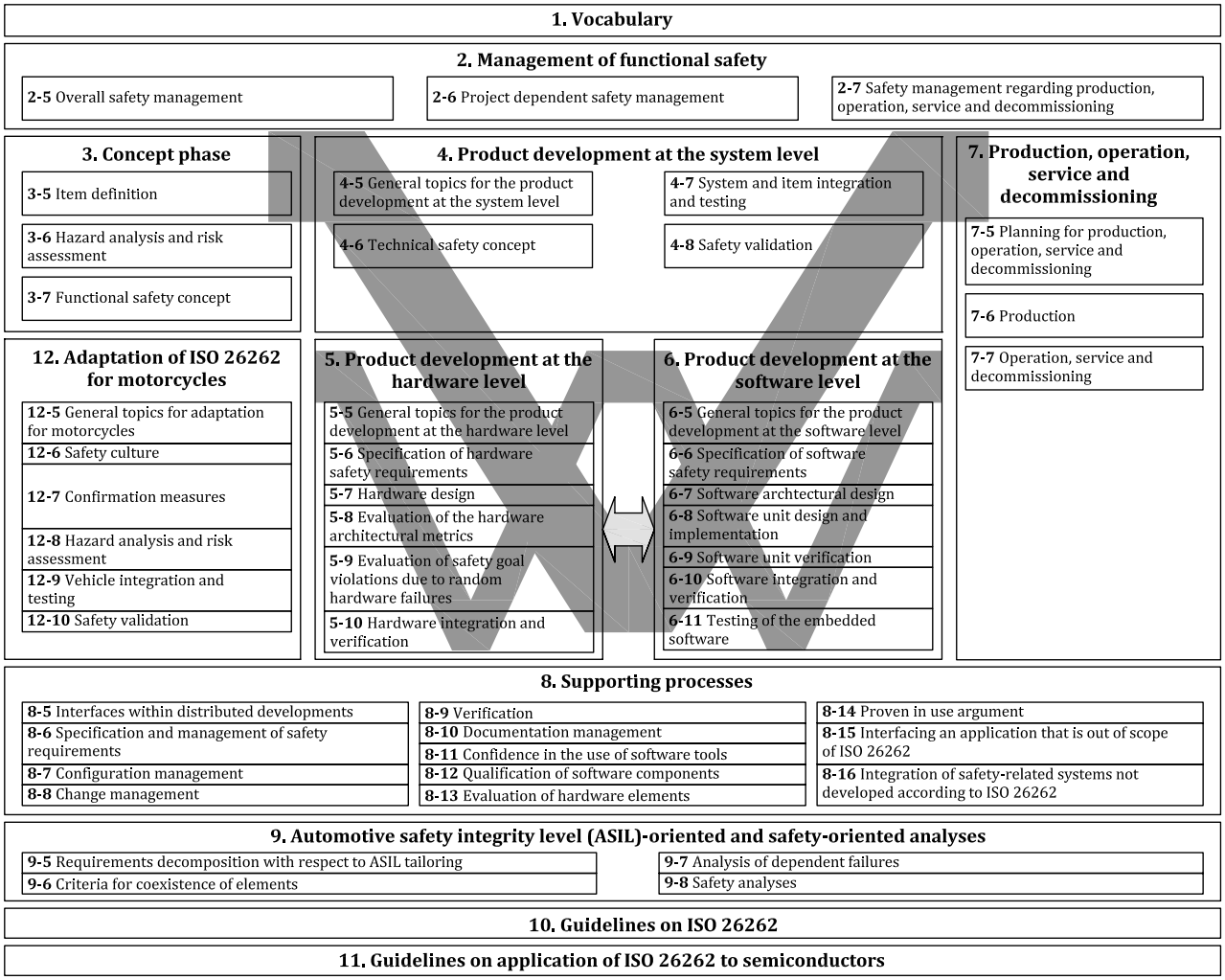


Figure 1 — Overview of the ISO 26262 series of standards

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

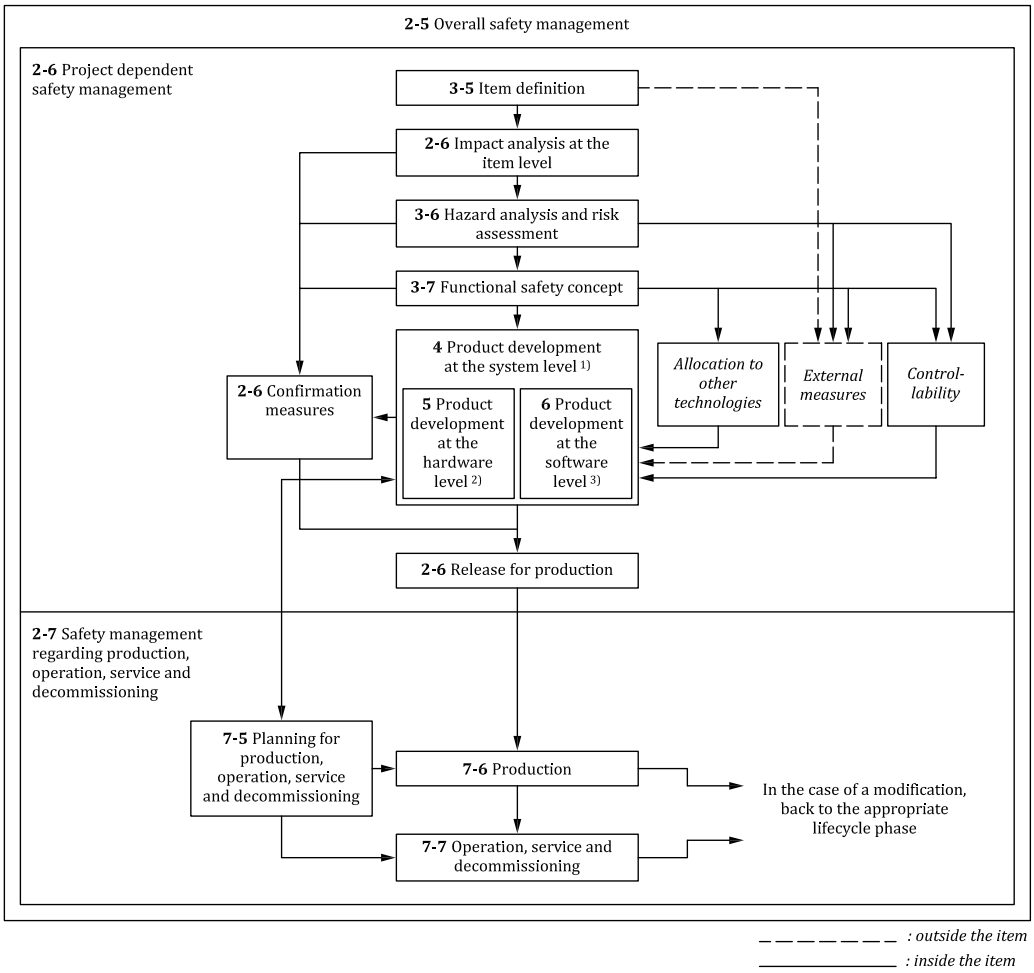
5.2.1 Overview of the safety lifecycle

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

The confirmation measures (see Clause 6) are performed to judge the functional safety achieved by the item, or the contribution to the achievement of functional safety e.g. concerning the development of elements.

b) Controllability

In the hazard analysis and risk assessment (see ISO 26262-3:2018, Clause 6), credit can be taken for the ability of the driver, or the other persons at risk (e.g. pedestrians, cyclists, passengers, drivers of other vehicles) to avoid the specified harm, possibly supported by external measures. The assumptions regarding the controllability in the hazard analysis and risk assessment and the functional and technical safety concept are validated (see ISO 26262-3:2018, Clauses 6 and 7 and ISO 26262-4:2018, Clause 8).

NOTE The exposure and the severity depend on the scenario. The eventual controllability through human intervention is influenced by the design of the item and is therefore evaluated during the safety validation (see ISO 26262-4:2018, Clause 8).

c) External measures

The external measures refer to the measures outside the boundary of the item (see ISO 26262-3:2018, Clause 5) that reduce or mitigate the potential hazards resulting from malfunctioning behaviour of the item. External measures can include additional in-vehicle devices such as dynamic stability controllers or run-flat tyres, but also devices external to the vehicle, such as 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 (see ISO 26262-4:2018, Clause 8).

External measures can be considered in the hazard analysis and risk assessment (see ISO 26262-3:2018, Clause 6). However, if credit is taken from an external measure in the hazard analysis and risk assessment e.g. to reduce the ASIL of a safety goal, that external measure cannot be considered again as a risk reduction in the functional safety concept.

An external measure can be outside the scope of the ISO 26262 series of standards (e.g. if the external measure is realized by another technology or is implemented external to the vehicle), or in the scope of the ISO 26262 series of standards (e.g. if the external measure is realized by an E/E system distinct from the item).

d) Impact analysis at the item level

An impact analysis (see 6.4.3) is performed at the item level to determine whether the item is a new development, a modification of an existing item, or an existing item with a modified environment. If there are one or more modifications, the implications of the modifications on functional safety are analysed.

e) Impact analysis at the element level

An impact analysis is performed at the element level when an existing element is reused (see 6.4.4), so as to evaluate whether the reused element is able to comply with the safety requirements allocated to that element, considering the operational context in which the element is reused.

f) Other technologies

Other technologies (e.g. mechanical and hydraulic technologies) are those different from electrical and electronic technologies. These can be considered in the specification and allocation of safety requirements (see ISO 26262-3:2018, Clause 7 and ISO 26262-4), or as an external measure. In other words, an element realized by another technology may be implemented within the item, or may be specified as an external measure.

g) Release for production

The release for production (see 6.4.13) formalizes the decision to release the item, or element, for production, considering the results of the safety lifecycle, including the results of the applicable confirmation measures.

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 compliance with standards that support quality management.

EXAMPLE 1 IATF 16949 in conjunction with ISO 9001 regarding quality management across phases of the safety lifecycle.

EXAMPLE 2 ISO/IEC 33000 series of standards, Capability Maturity Model Integration (“CMMI®”), or Automotive SPICE®[1)] series of standards regarding product development.

5.4 Requirements and recommendations

5.4.1 General

Sub-clauses 5.4.2 to 5.4.6 apply to the organizations involved in the execution of the safety lifecycle.

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.

NOTE Annex B provides more details of what can constitute a safety culture.

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

NOTE Such organization-specific rules and processes can include the creation and maintenance of generic plans (e.g. a generic safety plan) or generic process descriptions.

5.4.2.3 The organization shall institute and maintain effective communication channels between functional safety, cybersecurity, and other disciplines that are related to the achievement of functional safety.

EXAMPLE 1 Communication channels between functional safety and cybersecurity in order to exchange relevant information (e.g. in the case it is identified that a cybersecurity issue might violate a safety goal or a safety requirement, or in the case a cybersecurity requirement might compete with a safety requirement).

EXAMPLE 2 Communication channels between functional safety and non-E/E related safety such as mechanical safety.

EXAMPLE 3 Communication channels between functional safety and quality.

NOTE Guidance on potential interaction of functional safety with cybersecurity is given in Annex E.

1) CMMI® and Automotive SPICE® are examples of suitable products available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of these products.

5.4.2.4 During the execution of the safety lifecycle, the organization shall perform the required safety activities, including the creation and management of the associated documentation in accordance with ISO 26262-8:2018, Clause 10.

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

NOTE Resources include human resources, tools, databases, guidelines and work instructions.

5.4.2.6 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.

5.4.2.7 The organization shall ensure that the persons responsible for achieving or maintaining functional safety, or for performing or supporting the safety activities, are given sufficient authority to fulfil their responsibilities.

5.4.3 Management of safety anomalies regarding functional safety

5.4.3.1 The organization shall institute, execute and maintain processes to ensure that identified safety anomalies are explicitly communicated to the persons responsible for achieving or maintaining functional safety during the safety lifecycle.

NOTE Depending on the safety anomaly, the responsible persons can include the applicable safety manager of the customer, the applicable safety manager of a supplier, the safety manager of the development of a related item, or the persons responsible for achieving and maintaining functional safety during production, operation, service and decommissioning.

5.4.3.2 The organization shall institute, execute and maintain a safety anomaly resolution process to ensure that identified safety anomalies are analysed, evaluated, resolved and managed to closure in a timely and effective manner.

NOTE 1 The safety anomaly resolution process can include a root cause analysis that results in a corrective action for the future.

NOTE 2 If the resolution of a safety anomaly results in a change, this change is entered into the change management process in accordance with ISO 26262-8:2018, Clause 8.

NOTE 3 A safety manager can nominate a person responsible for the resolution of a safety anomaly.

NOTE 4 The safety anomaly resolution process can be integrated in the anomaly resolution processes of the quality management system (see also 5.4.5).

5.4.3.3 A safety anomaly shall only be considered as managed to closure if:

a) an adequate safety measure is implemented that resolves the safety anomaly, based on a rationale; and the effectiveness of the safety measure is verified, or

   NOTE 1 In the case a design change resolves the safety anomaly, the corresponding impact analysis according to ISO 26262-8:2018, Clause 8 can provide the rationale.

   NOTE 2 Safety anomalies might be resolved by measures implemented by other technologies, or by external measures (e.g. measures outside the scope of the ISO 26262 series of standards).

b) the safety anomaly is evaluated as not constituting an unreasonable risk and is closed, based on a rationale.

NOTE 3 If no rationale is available, a safety anomaly is not managed to closure.

5.4.3.4 The rationale for a safety anomaly managed to closure, in accordance with 5.4.3.3, shall be documented; and shall be reviewed.

EXAMPLE The rationale can be reviewed as part of the functional safety assessment (see 6.4.12).

5.4.3.5 Safety anomalies that are not managed to closure shall be escalated to the persons responsible for functional safety, such as the project manager in the case of a safety anomaly regarding product development.

NOTE In the case a safety anomaly is identified during development that is not managed to closure, and a functional safety assessment is performed, one of the persons to whom the safety anomaly is explicitly communicated is the person responsible for the functional safety assessment.

5.4.4 Competence management

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

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

— usual safety practices, concepts and designs;

— the ISO 26262 series of standards and, if applicable, further safety standards;

— organization-specific rules for functional safety;

— organization-specific rules for disciplines that interact with functional safety; and

— functional safety processes instituted in the organization.

NOTE 2 To evaluate the skills, competence and qualification to carry out activities to comply with the ISO 26262 series of standards, the experience from previous professional activities can be considered, such as:

— domain knowledge of the item;

— expertise on the environment of the item;

— management experience; and

— expertise of production, operation, service and decommissioning.

NOTE 3 The organization can define criteria regarding the sufficiency of the corresponding skills, competence and qualification.

EXAMPLE Criteria given in the United Kingdom Health and Safety Executive “Managing competence for safety-related systems”.

5.4.5 Quality management system

5.4.5.1 The organization shall have a quality management system that supports achieving functional safety and complies with a quality management standard, such as IATF 16949 in conjunction with ISO 9001, or equivalent.

5.4.6 Project-independent tailoring of the safety lifecycle

5.4.6.1 The organization may tailor the safety lifecycle for application across items or elements, i.e. apply a project-independent tailoring, but only if such a tailoring is limited to:

a) combining or splitting sub-phases, activities or tasks,

NOTE Sub-phases can be combined if the method used makes it difficult to clearly distinguish between the individual sub-phases (e.g. computer-aided development tools can support activities of several sub-phases within one step).

b) performing an activity or task in a different phase or sub-phase,

c) performing an activity or task in an added phase or sub-phase,

d) iterating phases or sub-phases,

e) performing safety activities concurrently with safety activities of other phases, or sub-phases, provided that 6.4.7.1 is complied with, or

f) omitting a phase or sub-phase that is not applicable to the organization, based on a rationale.

5.5 Work products

5.5.1 Organization-specific rules and processes for functional safety, resulting from 5.4.2 to 5.4.6.

5.5.2 Evidence of competence management, resulting from 5.4.4.

5.5.3 Evidence of a quality management system, resulting from 5.4.5 and 5.4.6.

5.5.4 Identified safety anomaly reports, if applicable, resulting from 5.4.3.

6 Project dependent safety management

6.1 Objectives

The intent of this clause is to ensure that the following objectives are achieved by the organizations involved in the concept phase or the development phases at the system, hardware or software level:

a) to define and assign the roles and responsibilities regarding the safety activities;

b) to perform an impact analysis at the item level to identify whether the item is a new item, a modification of an existing item, or an existing item with a modified environment; and in the case of one or more modifications, to analyse the implications of the identified modifications on functional safety;

c) to perform an impact analysis at the element level in the case an existing element is reused, to evaluate whether the reused element is able to comply with the safety requirements allocated to that element, considering the operational context in which the element is reused;

NOTE An impact analysis at the item or element level can support the planning of the safety activities (see 6.4.6.7).

d) to define the tailored safety activities, to provide the corresponding rationales for tailoring and to review the provided rationales;

e) to plan the safety activities;

f) to coordinate and track the progress of the safety activities in accordance with the safety plan;

g) to plan the distributed developments (see ISO 26262-8:2018, Clause 5);

h) to ensure a correct progression of the safety activities throughout the safety lifecycle;

i) to create a comprehensible safety case in order to provide the argument for the achievement of functional safety;

j) to judge whether the item achieves functional safety (i.e. the functional safety assessment), or to judge the contribution to the achievement of functional safety concerning an element (i.e. the functional safety assessment activities performed by a supplier) or work product (e.g. a confirmation review); and

k) to decide at the end of development whether the item, or element(s), can be released for production based on the evidence that supports confidence in the achieved functional safety.

6.2 General

In a project, the roles and responsibilities regarding the safety activities are defined and assigned.

An impact analysis at the item level is performed to identify whether the item is a new item, a modification of an existing item, or an existing item with a modified environment. In the case of a modification, the implications on functional safety are analysed.

An impact analysis at the element level is performed in the case an existing element is reused, considering the operational context in which the element is reused.

Safety management includes the responsibility to plan and coordinate the safety activities, to track the progress of the safety activities against the corresponding planning and to describe and justify the tailored safety activities.

The safety planning is documented and references the development interface agreements (see ISO 26262-8:2018, Clause 5) that define the interfaces with the safety plans of the other parties in a distributed development.

Safety management also includes the responsibility to ensure that the confirmation measures are performed. Depending on the applicable ASIL, confirmation measures are performed with sufficient independence regarding resources, management and release authority.

Confirmation measures include confirmation reviews, a functional safety audit and a functional safety assessment:

— confirmation reviews are intended to judge whether the key work products (see Table 1) provide sufficient and convincing evidence of their contribution to the achievement of functional safety;

— if applicable, a functional safety audit evaluates the implementation of the processes required for the safety activities; and

— if applicable, a functional safety assessment judges whether the item achieves functional safety, or judges the contribution to the achievement of functional safety e.g. concerning the development of elements.

Table 1 lists the confirmation measures.

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

Finally, the person responsible for the release of the item, or elements of the item, decides whether the item, or element(s), is ready for series-production and operation, based on the evidence that supports confidence in the achieved functional safety.

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 management in accordance with 5.5.2; and

— evidence of a quality management system in accordance with 5.5.3.

6.3.2 Further supporting information

If available, the following information can be considered:

— project plan (from an external source);

— dependencies on other activities, including other safety activities; and

— other existing information useful for conducting an impact analysis (see 6.4.3 and 6.4.4).

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

6.4 Requirements and recommendations

6.4.1 General

Sub-clauses 6.4.2 to 6.4.13 apply to the organizations involved in the concept phase or the product development phases (system, hardware or software) of the item, or of one or more elements of the item.

EXAMPLE A supplier that develops an element, intended to be integrated by the customer (see ISO 26262-8:2018, Clause 5), which implements one or more safety requirements with an ASIL A, B, C or D in accordance with 4.4.

6.4.2 Roles and responsibilities in safety management

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

NOTE In the case of a distributed development (see ISO 26262-8:2018, Clause 5), project managers are appointed at the customer and at the suppliers that develop one or more elements intended to be integrated.

6.4.2.2 The project manager shall be given the responsibility and the authority, in accordance with 5.4.2.7, 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 safety activities, in accordance with 5.4.2.5.

NOTE The estimation, determination and allocation of sufficient resources are included in the planning.

6.4.2.4 The project manager shall ensure that the safety manager is appointed in accordance with 5.4.4.

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 depending on the organization.

NOTE 3 In the case of a distributed development (see ISO 26262-8:2018, Clause 5), safety managers are appointed at the customer and at the suppliers that develop one or more elements intended to be integrated.

6.4.3 Impact analysis at the item level

6.4.3.1 At the beginning of the-safety lifecycle, an impact analysis at the item level shall be performed to determine whether the item is a new development, a modification of an existing item or an existing item with a modified environment.

NOTE A proven in use argument can be applied to a modification (see ISO 26262-8:2018, Clause 14).

6.4.3.2 In the case of a modification of an item or its environment, the impact analysis at the item level in accordance with 6.4.3.1 shall identify and describe the modifications applied to the item, including:

NOTE 1 The impact analysis considered in this clause concerns modifications of the item considered in the planning phase. Design modifications considered during the execution of the development are implemented through a change management process (see ISO 26262-8:2018, Clause 8).

a) modifications to the design;

NOTE 2 A design modification can result from requirement modifications.

NOTE 3 A design modification can impact the behaviour of the item.

EXAMPLE 1 Design modification resulting from a modification of calibration data

EXAMPLE 2 Design modifications resulting from a change in the operating modes of the item

b) modifications of the implementation; and

NOTE 4 Implementation modifications are not intended to affect the specification or performance of the item.

NOTE 5 Implementation modifications to the item might impact the behaviour of the item.

NOTE 6 Implementation modifications can result from corrections of software.

c) modifications related to the environment.

EXAMPLE 3 Temperature, altitude, humidity, vibrations, Electromagnetic Interference (“EMI”) and fuel types

NOTE 7 Modifications include:

— the installation of the item in a new target environment (e.g. another vehicle variant);

— changes to the operational situations; and

— a different location of the item within the vehicle.

6.4.3.3 An impact analysis at the item level in accordance with 6.4.3.2 shall:

a) evaluate the implications of the modifications with regard to functional safety; and

b) identify and describe the safety activities to be performed, based on the impact of the modifications.

6.4.4 Reuse of an existing element

In the case an existing element is reused, an impact analysis at the element level shall be performed, which shall:

a) identify the modifications to the operational context, including resulting modifications of the element;

b) evaluate whether the reused element, with or without modifications, is able to comply with the allocated safety requirements that result from the item, or element, into which the considered element is to be integrated;

NOTE 1 Existing elements can be reused with, or without, modifications being planned for that element. Modifications of the element can be planned, for example, to enable the integration of the existing element.

c) identify the safety activities to be performed based on an evaluation of the implications of the modifications, including implications on the validity of previously made assumptions; and

d) evaluate whether the existing safety-related documentation regarding the reused element is sufficient to support the integration of the element into the item, or element, in which the considered element is to be integrated.

NOTE 2 The impact analysis considered in this clause concerns modifications to the operational context of the element that are considered in the planning phase. Design modifications considered during the execution of the development are implemented through a change management process (see ISO 26262-8:2018, Clause 8).

NOTE 3 An existing element can be reused:

a) based on an evaluation of hardware elements (see ISO 26262-8:2018, Clause 13),

b) based on a qualification of software components (see ISO 26262-8:2018, Clause 12),

c) based on a proven in use argument (see ISO 26262-8:2018, Clause 14), or

d) as a Safety Element out of Context (see ISO 26262-10).

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 than prescribed in the reference ISO 26262 lifecycle. If such a safety activity is tailored, then

a) the tailoring shall be defined in the safety plan (see 6.4.6.5, b); and

b) a rationale as to why the tailoring is appropriate 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 6.4.9) or during the functional safety assessment (see 6.4.12).

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 5.4.6 applies.

6.4.5.2 If a safety activity is tailored in accordance with 6.4.5.1 as a result of an impact analysis in accordance with 6.4.3 or 6.4.4, then the tailoring shall comply with 6.4.6.7.

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 the tailoring shall comply with ISO 26262-8:2018, Clause 14.

6.4.5.4 If a safety activity is tailored in accordance with 6.4.5.1 because of an evaluation of hardware elements, the tailoring shall comply with ISO 26262-8:2018, Clause 13.

6.4.5.5 If a safety activity is tailored in accordance with 6.4.5.1 because of a qualification of software components, the tailoring shall comply with ISO 26262-8:2018, Clause 12.

6.4.5.6 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 the tailoring shall comply with ISO 26262-8:2018, Clause 11.

6.4.5.7 If the safety activities are tailored in accordance with 6.4.5.1 because an element is developed as a Safety Element out of Context ("SEooC"), then

a) the development of the safety element out of context 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 assumptions on the intended use and context of the safety element out of context shall be validated when the element is integrated in its target application.

NOTE 1 The ISO 26262 series of standards as a whole cannot be applied to an element developed as a safety element out of context 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 that can be evaluated by means of a functional safety assessment.

EXAMPLE A microcontroller developed as a safety element out of context

NOTE 2 See ISO 26262-10 for further details of a Safety Element out of Context development.

6.4.5.8 This requirement applies to item developments for T&B: if an application that is out of scope of the ISO 26262 series of standards is being interfaced with a base vehicle or item that has been developed in accordance with those standards, then tailoring of corresponding safety activities shall be performed in accordance with ISO 26262-8:2018, Clause 15.

6.4.5.9 This requirement applies to item developments for T&B: if safety activities are performed to achieve confidence that a system or component not developed according to the ISO 26262 series of standards satisfies the required level of functional safety needed for the integration into an item developed in accordance with those standards, then tailoring of these safety activities shall be performed in accordance with ISO 26262-8:2018, Clause 16.

6.4.6 Planning and coordination of the safety activities

6.4.6.1 The safety manager shall be responsible for the planning and coordination of the safety activities in which the organization is involved, in accordance with 5.4.2.7.

NOTE 1 The safety manager can delegate tasks to persons that possess the required skills, competences and qualifications (see 5.4.4).

NOTE 2 Depending on whether the item is a new development, a modification of an existing item or an existing item with a modified environment (see 6.4.3), or whether the element is new or reused (see 6.4.4), the extent of the safety activities can vary, and the activities are planned accordingly.

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

6.4.6.3 The responsibilities with regard to performing the safety activities shall be clearly assigned and communicated within the organization in accordance with 5.4.2.7 and 5.4.4.

NOTE The safety manager is responsible for planning and coordinating the safety activities. Other persons can be responsible to detail the planning (see also 6.4.6.8) or to perform the safety activities (e.g. to plan or perform integration and verification activities and configuration management).

6.4.6.4 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 26262-8:2018, 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.

6.4.6.5 The safety plan shall define the planning of the activities and procedures for achieving functional safety, including:

a) the implementation of project-independent safety activities in accordance with Clause 5 into project-specific safety management;

b) the definition of the tailored safety activities, in accordance with 6.4.5, if applicable;

NOTE 1 For example, tailoring as a result of an impact analysis at the item level (see 6.4.3) or at element level (see 6.4.4). Refer also to 6.4.6.7.

c) the planning of the safety activities to comply with the requirements of ISO 26262-3, ISO 26262-4, ISO 26262-5 and ISO 26262-6;

d) the planning of the supporting processes, in accordance with ISO 26262-8, including if applicable, the reference to the Development Interface Agreements ("DIA"s) that define the interfaces with the safety plans of the other parties in a distributed development, in accordance with ISO 26262-8:2018, Clause 5;

e) the planning of the integration and verification activities to comply with the requirements of ISO 26262-3, ISO 26262-4, ISO 26262-5, ISO 26262-6 and ISO 26262-8:2018, Clause 9; and the planning of the safety validation activities in accordance with ISO 26262-4:2018, Clause 8;

NOTE 2 The work product "safety plan" includes detailed integration, verification, and safety validation planning, however such planning can be in other documents (see ISO 26262-8:2018, Clause 10).

f) the scheduling of the confirmation reviews, the functional safety audit and the functional safety assessment in accordance with 6.4.9 to 6.4.12;

NOTE 3 The level of independence given in 6.4.9 of a person that carries out a confirmation measure is specified in the safety plan.

NOTE 4 The safety manager is responsible for scheduling the confirmation measures. The details of a confirmation measure are planned by the person responsible for that confirmation measure.

g) the planning of the analysis of dependent failures, if applicable, and the safety analyses to comply with the requirements of ISO 26262-3, ISO 26262-4, ISO 26262-5, ISO 26262-6, ISO 26262-9:2018, Clause 7 and ISO 26262-9:2018, Clause 8;

NOTE 5 The objectives and scope of the safety analyses are defined during their planning and depend on the corresponding sub-phase and context.

h) the provision of the proven in use arguments of the candidates in accordance with ISO 26262-8:2018, Clause 14, if applicable; and

i) the provision of the confidence in the usage of software tools in accordance with ISO 26262-8:2018, Clause 11, if applicable.

6.4.6.6 The planning of a safety activity shall include:

a) the objective;

b) the dependencies on other activities or information;

c) the person responsible for performing the activity;

d) the required resources for performing the activity;

e) the starting point, or end point, in time and the duration; and

f) the identification of the corresponding work product.

6.4.6.7 In the case of a modification of the item, a modification of the environment of an existing item, in accordance with 6.4.3, or in the case an element is reused in accordance with 6.4.4:

a) the reference safety lifecycle of the ISO 26262 series of standards shall be tailored based on the results of the corresponding impact analysis;

NOTE 1 The tailored safety activities are defined in the safety plan considering the applicable lifecycle phases and sub-phases (see 6.4.5).

b) the affected work products that need to be created or updated shall be identified, described and reworked accordingly; and

NOTE 2 The affected work products include the safety validation specification (see ISO 26262-4:2018, Clause 8).

c) in the case of safety documentation that does not comply with the ISO 26262 series of standards, the necessary activities to comply with the corresponding requirements of these standards shall be determined.

EXAMPLE 1 An element developed according to a safety standard different from the ISO 26262 series of standards, with the corresponding safety documentation being incomplete to comply with ISO 26262

EXAMPLE 2 A legacy element with missing safety documentation, or safety documentation insufficient to comply with ISO 26262

6.4.6.8 The safety plan shall be updated incrementally, as a minimum at the beginning of each phase.

NOTE At least at the beginning of each phase, the safety plan is updated so as to detail the planning of the safety activities of that phase. The safety plan can be further detailed in a sub-phase.

6.4.6.9 The work products required by the safety plan shall be kept up-to-date during the development phases so as to maintain an adequate representation of the item, or element, until and at the release for production.

6.4.6.10 In the case of a distributed development, both the customer and the supplier shall define a safety plan regarding the respective safety activities.

NOTE The corresponding Development Interface Agreement is defined in accordance with ISO 26262-8:2018, Clause 5.

6.4.7 Progression of the safety lifecycle

6.4.7.1 In the case of a lack of information from the pertinent preceding sub-phases, a subsequent sub-phase shall only start if the lack of information does not cause an unreasonable risk regarding functional safety.

NOTE For cases where the lack of information can jeopardize the project, the issue is escalated.

6.4.7.2 The work products required by the safety plan shall be subject to configuration management, change management and documentation, in accordance with ISO 26262-8:2018, Clause 7, 8 and 10, respectively, no later than the time of entering the phase "product development at the system level" (see ISO 26262-4).

6.4.8 Safety case

6.4.8.1 A safety case shall be developed, in accordance with the safety plan, in order to provide the argument for the achievement of functional safety.

6.4.8.2 The safety case should progressively compile the work products that are generated during the safety lifecycle to support the safety argument.

NOTE 1 In the case of a distributed development, the safety case of the item can be a combination of the safety cases of the customer and of the suppliers, which references evidence from the work products generated by the respective parties. Then the overall argument of the item is supported by arguments from all parties. The interfaces between the customer and a supplier are defined in a Development Interface Agreement (see ISO 26262-8:2018, Clause 5).

NOTE 2 To support safety planning according to 6.4.6, the intended safety arguments can be identified prior to work products becoming available. To support progressive functional safety assessments according to 6.4.12.3 the safety case can be released progressively as work products are generated to provide evidence for the safety arguments.

6.4.9 Confirmation measures

6.4.9.1 The functional safety of the item and its elements shall be confirmed, based on:

a) confirmation reviews to judge whether the key work products, i.e. those included in Table 1, provide sufficient and convincing evidence of their contribution to the achievement of functional safety, considering the corresponding objectives and requirements of the ISO 26262 series of standards, in accordance with Table 1 and 6.4.10;

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

b) a functional safety audit to judge the implementation of the processes required for functional safety, in accordance with Table 1 and 6.4.11; and

   NOTE 2 The reference processes required for functional safety are defined in the ISO 26262 series of standards. The processes pertaining to an item or element are defined through the activities referenced or specified in the safety plan.

c) a functional safety assessment to judge the achieved functional safety of the item, or the contribution to the achievement of functional safety by the developed elements, in accordance with Table 1 and 6.4.12.

   NOTE 3 The aim of the independence defined in Table 1 is to ensure an objective, unbiased viewpoint and to avoid conflict of interest. The use of the term "independence" in this document relates to organizational independence.

   NOTE 4 Guidance for the confirmation measure is given in Annex C.

   NOTE 5 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 26262-8:2018, Clause 10).

   NOTE 6 If the item changes subsequent to the completion of confirmation measures, then the pertinent confirmation measures will be repeated or supplemented (see ISO 26262-8:2018, 8.4.5.2).

   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 independence

Confirmation measures	Level of independence[a] applies to					Scope
	QM	ASIL A	ASIL B	ASIL C	ASIL D	
Confirmation review of the impact analysis at the item level (see 6.5.1) Independence with regard to the author of the impact analysis and project management	I3	I3	I3	I3	I3	Judgement of whether the impact analysis in accordance with 6.4.3 correctly identified the item as being a new item, a modification of an existing item or an existing item with a modified environment. Judgement of whether the impact analysis in accordance with 6.4.3 adequately identified the implications on functional safety caused by the modification(s); and the safety activities to be performed.
Confirmation review of the hazard analysis and risk assessment (see ISO 26262-3:2018, Clause 6) Independence with regard to the developers of the item, project management and the authors of the work product	I3	I3	I3	I3	I3	Judgement of whether the selection of the operational situations pertinent to the hazardous events and the definitions of the hazardous events are appropriate. Judgement of whether the determined ASILs, quality management ("QM") ratings of the identified hazardous events for the item and the parameters resulting in no ASIL e.g. C0/S0/E0 are correct. Judgement of whether the specified safety goals cover the identified hazardous events.
Confirmation review of the safety plan (see 6.5.3) Independence with regard to the developers of the item, project management and the authors of the work product. NOTE 1 A confirmation review of the safety plan includes a review of the impact analyses at element level performed due to the reuse of existing elements (see 6.5.2). NOTE 2 The safety plan includes the proven in use arguments (analysis, data and credit) of the proven in use candidates and the corresponding tailoring, if applicable (see 6.4.6 and ISO 26262-8:2018, Clause 14). NOTE 3 The safety plan includes tailoring due to the use of software tools, if applicable (see 6.4.6 and ISO 26262-8:2018, Clause 11).	—	I1	I1	I2	I3	Applies to the highest ASIL among the safety requirements

Table 1 *(continued)*

Confirmation measures	Level of independence[a] applies to					Scope
	QM	ASIL A	ASIL B	ASIL C	ASIL D	
Confirmation review of the Functional Safety Concept (see ISO 26262-3:2018, Clause 7), supported by the results of the corresponding safety analyses and dependent failure analyses (see ISO 26262-9:2018, Clause 8 and ISO 26262-9:2018, Clause 7, respectively) Independence with regard to the developers of the item, project management and the authors of the work product	—	I1	I1	I2	I3	Applies to the highest ASIL among the safety goals of the item
Confirmation review of the Technical Safety Concept (see ISO 26262-4:2018, Clause 6), supported by the results of the corresponding safety analyses and dependent failure analyses (see ISO 26262-9:2018, Clause 8 and ISO 26262-9:2018, Clause 7, respectively) Independence with regard to the developers of the item, project management and the authors of the work product	—	I1	I1	I2	I3	Applies to the highest ASIL among the functional safety requirements from which the technical safety requirements are derived. If ASIL decomposition has been applied to the functional safety concept then the resulting ASIL from the decomposition may be considered.
Confirmation review of the integration and test strategy (see ISO 26262-4:2018, Clause 7) 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 requirements
Confirmation review of the safety validation specification (see ISO 26262-4:2018, Clause 8) 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 requirements
Confirmation review of the safety analyses and the dependent failure analyses (see ISO 26262-9:2018, Clause 8 and ISO 26262- 9:2018, Clause 7, respectively) Independence with regard to the developers of the item, project management and the authors of the work product	—	I1	I1	I2	I3	Applies to the highest ASIL among the safety requirements
Confirmation review of the safety case (see 6.5.4) Independence with regard to the authors of the safety case	—	I1	I1	I2	I3	Applies to the highest ASIL among the safety requirements

Table 1 *(continued)*

Confirmation measures	Level of independence[a] applies to					Scope
	QM	ASIL A	ASIL B	ASIL C	ASIL D	
Functional safety audit in accordance with 6.4.11 Independence with regard to the developers of the item and project management	—	—	I0	I2	I3	Applies to the highest ASIL among the safety requirements
Functional safety assessment in accordance with 6.4.12 Independence with regard to the developers of the item and project management	—	—	I0	I2	I3	Applies to the highest ASIL among the safety requirements

[a] The notations are defined as follows:

— —: no requirement and no recommendation for or against regarding this confirmation measure;

— I0: the confirmation measure should be performed; however, if the confirmation measure is performed, it shall be performed by a different person in relation to the person(s) responsible for the creation of the considered work product(s);

— I1: the confirmation measure shall be performed, by a different person in relation to the person(s) responsible for the creation of the considered work product(s);

— I2: the confirmation measure shall be performed, by a person who is independent from the team that is responsible for the creation of the considered work product(s), i.e. by a person not reporting to the same direct superior; and

— I3: the confirmation measure shall be performed by a person who is independent, regarding management, resources and release authority, from the department responsible for the creation of the considered work product(s).

6.4.9.2 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.

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

6.4.10 Confirmation reviews

6.4.10.1 A person responsible to perform the confirmation review shall be appointed, in accordance with 5.4.4 and 5.4.2.7, for each confirmation review that is included in Table 1 and required by the safety plan. This person shall provide a report that contains a judgement of the achieved contribution to functional safety by the work product.

6.4.10.2 The confirmation reviews shall be finalized before the release for production.

6.4.10.3 A confirmation review may be based on performing a judgement of whether the corresponding objectives of the ISO 26262 series of standards are achieved.

NOTE To increase confidence in the achievement of the review objectives, the reviewer checks the correctness, completeness, consistency, adequacy and contents of the work product against the corresponding requirements of the ISO 26262 series of standards.

6.4.10.4 One or more assistants may be appointed to support the performance of a confirmation review in accordance with 6.4.9.2 and 5.4.4. Such persons may lack independence from the developers of the corresponding item, elements or work products, but their independence shall be at least I1, as defined in Table 1, and the reviewer shall appraise their input to ensure an unbiased opinion is given.

NOTE As the confirmation reviews are performed in order to support the functional safety assessment, this appointment and appraisal can also be evaluated in the functional safety assessment, if applicable.

6.4.10.5 A confirmation review and a verification review may be combined, provided the review is performed with sufficient independence in accordance with Table 1.

6.4.11 Functional safety audit

6.4.11.1 For items and elements where the highest ASIL of the safety requirements is ASIL (B), C, or D: a functional safety audit shall be carried out in accordance with 6.4.9; and shall be finalized before the release for production.

6.4.11.2 A person responsible to carry out a functional safety audit shall be appointed in accordance with 5.4.4 and 5.4.2.7.

6.4.11.3 A functional safety audit may be based on a judgement of whether the process related objectives of the ISO 26262 series of standards are achieved.

NOTE The achievement of an objective of the ISO 26262 series of standards is considered against the corresponding requirements of these standards.

EXAMPLE The objectives of the requirements of Clause 6 are specified in 6.1.

6.4.11.4 The person responsible to carry out a functional safety audit shall provide a report that contains a judgement of the implementation of the processes required for functional safety, based on:

a) an evaluation of the implementation of the processes against the definitions of the activities referenced or specified in the safety plan;

b) an evaluation of the safety plan products against the organization-specific rules and processes (see 5.5.1);

c) an evaluation of the arguments, if provided, as to why the process related objectives of the ISO 26262 series of standards are achieved;

NOTE 1 Persons responsible for safety activities can provide an argument as to why the corresponding objectives of the ISO 26262 series of standards are achieved in order to facilitate a functional safety audit, considering 6.4.11.3.

NOTE 2 Compliance with all the corresponding ISO 26262 requirements is a sufficient rationale for having achieved an ISO 26262 objective.

d) an evaluation of whether the work products required by the safety plan are available;

e) an evaluation of whether the work products required by the safety plan comply with ISO 26262-8:2018, 10.4.3 and are consistent between one another; and

f) improvement recommendations in accordance with 5.4.2.6, if applicable, e.g. in the case of non-compliances.

NOTE 3 A functional safety audit can be performed together, or synchronized, with an Automotive Software Process Improvement and Capability determination assessment (see also the ISO/IEC 33000 series of standards). However, an Automotive SPICE®[2)] assessment is not sufficient to perform the functional safety assessment in accordance with 6.4.12.

2) Automotive SPICE® is an example of a suitable product available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of this product.

NOTE 4 An organization's process definitions can address multiple standards at the same time, e.g. the ISO 26262 series of standards and Automotive 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 the ISO 26262 series of standards and to Automotive SPICE can be provided.

NOTE 5 A functional safety audit performed in an early phase in a project is beneficial to identify weaknesses in the processes.

6.4.12 Functional safety assessment

6.4.12.1 For items and elements where the highest ASIL of the safety requirements is ASIL (B), C, or D: a functional safety assessment shall be carried out in accordance with 6.4.9, to judge the achieved functional safety of the item, or the contribution to the achievement of functional safety by the developed elements.

6.4.12.2 A functional safety assessment may be based on a judgement of whether the objectives of the ISO 26262 series of standards are achieved.

NOTE The achievement of an objective of the ISO 26262 series of standards is judged considering the corresponding requirements of these standards, the state-of-the-art regarding technical solutions and the applicable engineering domain knowledge, at the time of the development.

EXAMPLE The objectives of the requirements of Clause 6 are specified in 6.1.

6.4.12.3 A functional safety assessment:

a) shall be planned in accordance with 6.4.6.5 f);

b) should be planned at the latest at the beginning of the product development at the system level;

c) should be progressively performed during the product development; and

d) shall be finalized before the release for production.

EXAMPLE Agenda for a functional safety assessment given in Annex D

6.4.12.4 One or more persons shall be appointed to carry out a functional safety assessment, in accordance with 5.4.2.7 and 5.4.4. The appointed persons shall provide a report that contains a judgement of the achieved functional safety.

6.4.12.5 The persons responsible for performing a functional safety assessment shall be given the authority to perform the functional safety assessment according to their discretion, including:

a) the breadth and depth with which the safety activities and their results, that are within the scope of the functional safety assessment in accordance with 6.4.12.7, are assessed;

b) the information to be made available in accordance with 6.4.9.3; and

c) the support deemed necessary to perform the functional safety assessment in accordance with 6.4.9.2, such as the availability of the persons responsible for a pertinent work product.

6.4.12.6 The functional safety assessor may appoint one or more assistants to support the performance of the functional safety assessment in accordance with 6.4.9.2 and 5.4.4. Such persons may lack independence from the developers of the corresponding item, elements or work products, but their independence shall be at least I1, as defined in Table 1, and the assessor shall appraise their input to ensure an unbiased opinion is given.

NOTE The functional safety assessor remains responsible for the results of the functional safety assessment.

6.4.12.7 The scope of a functional safety assessment shall include:

a) the safety plan and all the work products required by the safety plan;

NOTE 1 The functional safety assessor can tailor the level of detail with which a particular work product is reviewed. However, those work products required by the safety plan which are listed in Table 1 merit particular attention.

NOTE 2 The functional safety assessor considers if requirements management (see ISO 26262-8:2018, Clause 6), including bidirectional traceability, is adequately implemented.

NOTE 3 The examination of the corresponding work products supports the judgement of whether an ISO 26262 objective is achieved (see 6.4.12.2).

b) the processes required for functional safety;

NOTE 4 The evaluation of the implemented processes can be based on the results of the functional safety audit and, if any, the resulting corrective actions.

c) the appropriateness and effectiveness of the performed or implemented safety measures that can be assessed during the development of the item or element;

NOTE 5 The functional safety assessment checks the suitability of the requirements related to production, operation, service and decommissioning. Regarding production, the correct implementation of such requirements is checked during the analysis of the production process capability (see ISO 26262-7:2018, 5.4.2.2 and ISO 26262-7:2018, 6.4.1.3).

d) the arguments, if provided, as to why functional safety is achieved considering the achievement of the relevant objectives of the ISO 26262 series of standards;

NOTE 6 The person(s) responsible for the creation of a work product can provide an argument as to why the corresponding objectives of the ISO 26262 series of standards are achieved in order to facilitate a functional safety assessment, considering 6.4.12.2.

NOTE 7 Compliance with all the corresponding ISO 26262 requirements is a sufficient rationale for having achieved an ISO 26262 objective.

e) the argument provided in the safety case; and

f) the rationales for the safety anomalies managed to closure in accordance with 5.4.3.

NOTE 8 In the case of a distributed development, functional safety assessment activities are performed at the customer and at its suppliers (see ISO 26262-8:2018, Clause 5). A functional safety assessment at a supplier judges whether the customer's safety requirements are complied with and judges the contribution to the achievement of functional safety by the developed elements or work products. The supplier provides functional safety assessment reports to the customer at the milestones and in the form defined in the development interface agreement (see ISO 26262-8:2018, 5.4.5). The functional safety assessment at a customer considers the suppliers' safety assessment reports (see 6.4.12.8). Finally, if the customer is a vehicle manufacturer, the functional safety assessment includes a judgement of the achieved functional safety of the item integrated in the target vehicle.

6.4.12.8 A functional safety assessment shall consider:

a) the planning of the other confirmation measures [see 6.4.6.5 f)];

b) the results from the confirmation reviews and functional safety audit;

c) the recommendations resulting from the previous functional safety assessment and the resulting corrective actions, if applicable (see 6.4.12.9 to 6.4.12.13 and ISO 26262-8:2018, 8.4.5.2); and

d) the results of the functional safety assessment activities regarding the elements or work products developed by suppliers, corresponding with the Development Interface Agreements in accordance with ISO 26262-8:2018, Clause 5, if applicable.

6.4.12.9 A functional safety assessment report shall include a recommendation for acceptance, conditional acceptance, or rejection of the functional safety of the item, or of the contribution to the functional safety of the item by the developed elements or work products.

6.4.12.10 A functional safety assessment report in accordance with 6.4.12.9 may include a recommendation for conditional acceptance provided the functional safety of the item, or the required contribution to functional safety by the developed elements or work products, is achieved, subject to the resolution of the identified conditions for acceptance.

NOTE In the case of a distributed development (see ISO 26262-8:2018, Clause 5), the supplier's functional safety assessment report includes such a recommendation for acceptance, conditional acceptance or rejection, regarding the developed elements or work products.

6.4.12.11 In the case of a recommendation for conditional acceptance in accordance with 6.4.12.10, the functional safety assessment report shall include the conditions for acceptance.

6.4.12.12 If the recommendation in a functional safety assessment report in accordance with 6.4.12.10 is a conditional acceptance of the achieved functional safety, the corrective actions needed to address the conditions for acceptance documented in the functional safety assessment report shall be carried out.

6.4.12.13 If the recommendation in a functional safety assessment report in accordance with 6.4.12.9 is a rejection of the achieved functional safety, then:

a) adequate corrective actions shall be performed; and

b) the functional safety assessment shall be repeated.

6.4.13 Release for production

6.4.13.1 The safety case in accordance with 6.4.8 shall be available prior to the release for production.

6.4.13.2 The applicable confirmation measure reports in accordance with 6.4.9 to 6.4.12 shall be available prior to the release for production.

6.4.13.3 The release for production of the item, or elements, shall only be approved if there is sufficient evidence for confidence in the achievement of functional safety.

NOTE Evidence for confidence in the achievement of functional safety can be provided by:

— the results of the confirmation measures, especially the recommendation included in the functional safety assessment report, if applicable, in accordance with 6.4.12.9; and

— the safety case.

6.4.13.4 The documentation of functional safety for release for production shall include the following information:

a) the name and signature of the person responsible for the release;

b) the versions of the released item or elements;

c) the configuration of the released item or elements; and

d) the release date.

6.4.13.5 At the release for production, a baseline for the embedded software, including the calibration data, and a baseline for the hardware shall be available and shall be documented in accordance with ISO 26262-8:2018, Clause 10.

6.5 Work products

6.5.1 **Impact analysis at the item level**, resulting from 6.4.3.

6.5.2 **Impact analyses at element level**, if applicable, resulting from 6.4.4.

6.5.3 **Safety plan**, resulting from 6.4.5 to 6.4.13.

6.5.4 **Safety case**, resulting from 6.4.8.

6.5.5 **Confirmation measure reports**, resulting from 6.4.9 to 6.4.12.

6.5.6 **Release for production report,** resulting from 6.4.13.

7 Safety management regarding production, operation, service and decommissioning

7.1 Objective

The objective of this clause is to define the responsibilities of the organizations and persons responsible for achieving and maintaining functional safety regarding production, operation, service and decommissioning.

7.2 General

See 5.2.

7.3 Inputs to this clause

7.3.1 Prerequisites

The following information shall be available:

— organization-specific rules and processes for functional safety in accordance with 5.5.1;

— evidence of competence management in accordance with 5.5.2;

— evidence of a quality management system in accordance with 5.5.3; and

— release for production report in accordance with 6.5.6.

7.3.2 Further supporting information

None.

7.4 Requirements and recommendations

7.4.1 General

Sub-clause 7.4.2 applies to the organizations involved in the production, operation, service and decommissioning of the item, or elements of the item.

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 5.4.2.7, to achieve and maintain the functional safety of the item regarding production, operation, service and decommissioning.

7.4.2.2 The activities for ensuring the functional safety of the item regarding production, operation, service and decommissioning of the item and its elements:

a) shall be planned in accordance with ISO 26262-7:2018, Clause 5;

b) shall be initiated during the product development at the system level in accordance with ISO 26262-4; and

c) shall be executed in accordance with ISO 26262-7:2018, Clauses 6 and 7.

7.4.2.3 The organization shall institute, execute and maintain processes in order to achieve and maintain the functional safety of the item regarding production, operation, service and decommissioning.

NOTE This includes a field monitoring process with respect to the item's functional safety. Refer to ISO 26262-7.

7.4.2.4 If the item changes during production, operation, service or decommissioning, the release for production in accordance with 6.4.13, shall be updated accordingly.

NOTE These changes are subject to change management (see ISO 26262-8:2018, Clause 8).

7.5 Work products

7.5.1 Evidence of safety management regarding production, operation, service and decommissioning, resulting from 7.4.2.

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	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.	None	5.5.1 Organization-specific rules and processes for functional safety 5.5.2 Evidence of competence management 5.5.3 Evidence of a quality management system 5.5.4 Identified safety anomaly reports, if applicable
6 Project dependent safety management	The intent of this Clause is to ensure that the following objectives are achieved by the organizations involved in the concept phase or the development phases at the system, hardware or software level:	Organization-specific rules and processes for functional safety (see 5.5.1)	6.5.1 Impact analysis at the item level 6.5.2 Impact analyses at element level, if applicable

Table A.1 *(continued)*

Clause	Objectives	Prerequisites	Work products
	a) to define and assign the roles and responsibilities regarding the safety activities; b) to perform an impact analysis at the item level to identify whether the item is a new item, a modification of an existing item, or an existing item with a modified environment; and in the case of one or more modifications, to analyse the implications of the identified modifications on functional safety; c) to perform an impact analysis at the element level in the case an existing element is reused, to evaluate whether the reused element is able to comply with the safety requirements allocated to that element, considering the operational context in which the element is reused; d) to define the tailored safety activities, to provide the corresponding rationales for tailoring and to review the provided rationales; e) to plan the safety activities; f) to coordinate and track the progress of the safety activities in accordance with the safety plan; g) to plan the distributed developments (refer to ISO 26262-8:2018, Clause 5);	Evidence of competence management (see 5.5.2) Evidence of a quality management system (see 5.5.3)	6.5.3 Safety plan 6.5.4 Safety case 6.5.5 Confirmation measure reports 6.5.6 Release for production report
	h) to ensure a correct progression of the safety activities throughout the safety lifecycle; i) to create a comprehensible safety case in order to provide the argument for the achievement of functional safety; j) to judge whether the item achieves functional safety (i.e. the functional safety assessment), or to judge the contribution to the achievement of functional safety concerning an element (i.e. the functional safety assessment activities performed by a supplier) or work product (e.g. a confirmation review); and k) to decide at the end of development whether the item, or element(s), can be released for production based on the evidence that supports confidence in the achieved functional safety.		

Table A.1 *(continued)*

Clause	Objectives	Prerequisites	Work products
7 Safety management regarding production, operation, service and decommissioning	The objective of this Clause is to define the responsibilities of the organizations and persons responsible for achieving and maintaining functional safety regarding production, operation, service and decommissioning.	Organization-specific rules and processes for functional safety (see 5.5.1) Evidence of competence management (see 5.5.2) Evidence of a quality management system (see 5.5.3) Release for production report (see 6.5.6)	7.5.1 Evidence of safety management regarding production, operation, service and decommissioning

Annex B
(informative)

Safety culture

Safety culture includes:

a) personal dedication and integrity of the persons responsible for achieving or maintaining functional safety and of the persons performing or supporting safety activities in the organization; and

b) safety thinking throughout the organization that allows for a questioning attitude, that prevents complacency, commits to excellence, fosters the taking of responsibility and corporate self-regulation in safety matters.

NOTE Refer to Safety Series No. 75-INSAG-4, International Atomic Energy Agency, Vienna, 1991.

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 level of independence in the integral processes (safety, quality, verification, safety 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

Table B.1 *(continued)*

Examples indicative of a poor safety culture	Examples indicative of a good safety culture
"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 — safety validation — functional safety audit — functional safety assessment

Annex C
(informative)

Guidance for the confirmation measures

C.1 General

This annex includes guidance for the confirmation measures, which can be used as a basis for judging the expected contribution to functional safety of the corresponding work products.

C.2 Confirmation review of the impact analysis at the item level (see 6.5.1)

The goal is to judge whether the impact analysis correctly and completely identifies the modifications, and assesses their impact on functional safety.

C.3 Confirmation review of the hazard analysis and risk assessment (see ISO 26262-3:2018, Clause 6)

C.3.1 The goal is to judge whether the results of the hazard analysis and risk assessment and the methods used are convincing and are supported by rationales, as well as to judge whether the safety goals cover all identified hazardous events that are classified with an ASIL. This judgement can be based on C.3.2 to C.3.7.

C.3.2 An evaluation of the situation analysis, to ensure that the selection of operational situations is appropriate and complies with ISO 26262-3:2018, 6.4.2.7.

C.3.3 An evaluation of the hazard identification to ensure that the defined hazardous events are appropriate and comply with ISO 26262-3:2018, 6.4.2.

C.3.4 An evaluation of the rationales of the determined E, C, S parameters (including E0, C0 and S0 and those resulting in QM), to ensure that the rationales are sound.

C.3.5 An evaluation of whether the assumptions made in the hazard analysis and risk assessment (e.g. considering the intended use, vehicle context and external measures) are explicitly documented to ensure that no assumption is overlooked or invalid.

NOTE Documenting the assumptions facilitates safety validation.

C.3.6 An evaluation of the consistency of comparable hazardous events among items, including ASILs, regardless of the malfunction, to ensure a consistent risk assessment across items in the organization.

C.3.7 An evaluation of whether the set of safety goals avoids unreasonable risk for all identified hazardous events.

C.4 Confirmation review of the safety plan (see 6.5.3)

C.4.1 The goal is to judge whether the safety activities to be performed are clearly defined, sufficient and adequate to achieve functional safety. This judgement can be based on C.4.2 to C.4.5.

C.4.2 An evaluation of whether the safety planning is consistent with the impact analysis.

C.4.3 An evaluation of the consistency of the safety plan with the project plan and the resource planning to ensure that the necessary safety activities are included in the project.

C.4.4 If applicable, an evaluation of the applied tailoring (i.e. omitting or performing safety activities in a different manner compared to the reference safety lifecycle of ISO 26262) including the corresponding rationales (see 6.4.5), to ensure that the necessary safety activities are properly included in the project.

If tailoring has been applied based on a proven in use argument (see ISO 26262-8:2018, Clause 14):

a) an evaluation of whether the results of the proven in use analyses justify the claimed proven in use credits of the candidates, regarding any associated tailoring of safety activities, to ensure correctness of the proven in use argument;

b) an evaluation of the efficiency of the field monitoring process (see ISO 26262-7), to ensure confidence in the supplied data; and

c) an evaluation of the candidate changes that are considered by the proven in use argument, to ensure that the changes do not affect the candidate's ability to achieve functional safety.

C.4.5 In the case of a distributed development, an evaluation of the distribution of responsibilities, safety activities and deliverables specified in the Development Interface Agreement (see ISO 26262-8:2018, Clause 5), to ensure that the necessary safety activities are properly included in the project.

C.5 Confirmation review of the functional safety concept (see ISO 26262-3:2018, Clause 7)

C.5.1 The goal is to judge whether the functional safety concept provides sufficient and convincing evidence that the functional safety requirements comply with the safety goals, considering the preliminary architecture. The judgement can be based on C.5.2 to C.5.9.

C.5.2 Evaluation of the feasibility of the functional safety concept to ensure the functional safety concept is sound and can be realized.

C.5.3 Evaluation of whether the functional safety concept is appropriate considering the results of the safety analyses (see ISO 26262-9:2018, Clause 8) and the dependent failure analyses (see ISO 26262-9:2018, Clause 7) that correspond with the elements of the preliminary architecture, to ensure confidence in the effectiveness and completeness of the functional safety requirements.

C.5.4 Evaluation of whether the specified safety mechanisms adequately consider malfunctioning behaviour, considering the elements of the preliminary architecture, to ensure the safety mechanisms sufficiently cover faults.

C.5.5 Evaluation of whether the specified safety mechanisms adequately react to faults, to ensure adequate mitigation of failures.

C.5.6 Evaluation of the warning and degradation strategy to initiate appropriate human behaviour of those involved, to ensure appropriate involvement and controllability for the degraded modes.

C.5.7 Evaluation of the validity of the applied ASIL decompositions, to ensure:

— the correctness and redundancy of the decomposed functional safety requirements;

— the feasibility of the required independence; and

— compliance of the resulting ASILs with ISO 26262-9:2018, Clause 5.

C.5.8 An evaluation of whether the assumptions made in the functional safety concept (e.g. considering the vehicle context) are explicitly documented to ensure that no assumption is overlooked, implicit or invalid.

NOTE Documenting the assumptions facilitates safety validation.

C.5.9 The completeness of the allocation of the functional safety requirements to elements of the preliminary architectural assumptions, including elements of other technologies, or to external measures to ensure that no functional safety requirement is overlooked.

C.6 Confirmation review of the technical safety concept (see ISO 26262-4:2018, Clause 6)

C.6.1 The goal is to judge whether the technical safety concept provides sufficient and convincing evidence that the technical safety requirements comply with the functional safety requirements, considering the elements of the system design. The judgement can be based on C.6.2 to C.6.9.

C.6.2 Evaluation of the feasibility of the technical safety concept, to ensure the technical safety concept can be realized in the system design.

C.6.3 Evaluation of whether the technical safety concept is appropriate considering the results of the safety analyses (see ISO 26262-9:2018, Clause 8) and the dependent failure analyses (see ISO 26262-9:2018, Clause 7) that correspond with the elements of the system design, to ensure confidence in the effectiveness and completeness of the technical safety requirements.

C.6.4 Evaluation of whether the specified safety mechanisms adequately consider malfunctioning behaviour, considering the elements of the system design, to ensure the safety mechanisms sufficiently cover faults.

C.6.5 Evaluation of whether the specified safety mechanisms adequately react to faults, to ensure adequate mitigation of failures.

C.6.6 Evaluation of whether the implementation of the warning and degradation strategy is consistent with the functional safety concept.

C.6.7 Evaluation of the validity of the applied ASIL decompositions, to ensure:

— the correctness and redundancy of the decomposed technical safety requirements;

— the feasibility of the required independence; and

— compliance of the resulting ASILs with ISO 26262-9:2018, Clause 5.

C.6.8 An evaluation of whether the assumptions made in the technical safety concept (e.g. considering the vehicle context) are explicitly documented to ensure that no assumption is overlooked, implicit or invalid.

NOTE Documenting the assumptions facilitates safety validation.

C.6.9 The completeness of the allocation of the technical safety requirements to system design elements to ensure that no technical safety requirement is overlooked.

C.7 Confirmation review of the integration and test strategy (see ISO 26262-4:2018, Clause 7)

C.7.1 The goal is to judge whether the integration and testing activities, methods and techniques described in the integration and test strategy are able to provide sufficient evidence that the item or elements comply with system design and corresponding safety requirements. The evaluation can be based on C.7.2 to C.7.4.

C.7.2 Evaluation of the integration and test strategy considering the context of the development project, application specifics, product domains and distributed developments and responsibilities, to ensure a sound plan for the safety relevant aspects of verification.

C.7.3 Evaluation of the integration and test strategy regarding applied methods and existing experience, to ensure a sound selection of verification techniques.

C.7.4 If applicable, an evaluation of the rationales as to why the verification methods and techniques are sufficient to achieve the corresponding objectives or requirements of the ISO 26262 series of standards.

C.8 Confirmation review of the safety validation specification including safety validation environment description (see ISO 26262-4:2018, Clause 8)

C.8.1 The goal is to judge whether the activities described in the safety validation specification are able to provide sufficient and convincing evidence that the safety goals and functional safety concept are appropriate, correct, complete and fully achieved at the vehicle level. The judgement can be based on C.8.2 to C.8.4.

C.8.2 Evaluation of the capability of the defined safety validation activities to validate the assumptions made in the hazard analysis and risk assessment, the functional safety concept and during the system, hardware and software development.

C.8.3 Evaluation of the capability of the defined safety validation activities to provide evidence of adequate failure mitigation, considering the effectiveness of the implemented safety measures, relevant external measures and relevant elements of other technologies.

C.8.4 Evaluation of the capability of the defined safety validation activities to provide evidence of the expected avoidance of harm by the driver or the other persons potentially at risk (i.e. controllability).

C.9 Confirmation review of the safety analyses and dependent failure analyses (see ISO 26262-9:2018, Clauses 7 and 8)

The goal is to judge whether the safety analyses and dependent failure analyses are correctly executed, to ensure that relevant identified faults and safety measures are sufficiently addressed.

C.10 Confirmation review of the safety case (see 6.5.4)

C.10.1 The goal is to judge whether the argument provided in the safety case is convincing. This judgement can be based on C.10.2 to C.10.4.

C.10.2 Evaluation of whether the argument provided in the safety case is plausible and sufficient to argue functional safety is achieved.

C.10.3 Evaluation of whether the referenced work products are available and sufficiently complete so that the achievement of functional safety can be adequately argued.

C.10.4 Evaluation of whether 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 (see also 5.4.3).

C.11 Functional safety audit (see 6.4.11)

The goal is to judge whether the implementation of the processes required for functional safety, considering the definitions of the activities referenced or specified in the safety plan, achieve the process related objectives of the ISO 26262 series of standards.

C.12 Functional safety assessment (see 6.4.12)

C.12.1 The goal is to judge whether functional safety of the item, or the expected contribution to functional safety of the developed elements, is achieved and to provide a recommendation for acceptance, conditional acceptance or rejection of the achieved functional safety. This judgement and recommendation can be based on C.12.2 to C.12.8.

C.12.2 Evaluation of the safety plan, and all the work products required by the safety plan, against the objectives of the ISO 26262 series of standards, considering the corresponding requirements of these standards, to judge whether the work products provide sufficient and convincing evidence of their contribution to the achievement of functional safety. For the work products that require a confirmation review (see Table 1), the results of the confirmation reviews are considered.

C.12.3 Evaluation of the implementation of the functional safety processes, considering the results of the performed functional safety audit(s) (see 6.4.11), to judge whether the process related aspects of the objectives of the ISO 26262 series of standards are achieved.

C.12.4 Evaluation of the implemented safety measures that can be assessed during the item development to judge whether these measures are appropriate and effective.

C.12.5 If arguments are provided as to why functional safety is achieved considering the achievement of objectives of the ISO 26262 series of standards, a judgement of whether these arguments are convincing considering the corresponding requirements of these standards.

C.12.6 Evaluation of the argument provided in the safety case to judge whether the argument is sufficiently convincing, considering the confirmation review of the safety case.

C.12.7 Evaluation of the rationales for the safety anomalies managed to closure in accordance with 5.4.3, to judge whether these rationales are convincing.

C.12.8 Follow-up of the recommendations resulting from the previous functional safety assessments, including any performed corrective actions, if applicable (see 6.4.12.9 to 6.4.12.13).

Annex D
(informative)

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

D.1 Safety management

D.1.1 Application of the organization's safety culture and supporting processes in the assessed project.

D.1.2 Application of the competence management and the continuous improvement practice in the assessed project.

D.1.3 Roles and responsibilities in the assessed project.

D.1.4 Safety plan of the assessed project and planning of the distributed development.

D.1.5 Tailoring of the safety lifecycle, including the proven in use arguments of the candidates, of the assessed project.

D.1.6 Functional safety audits, the safety case and available documents.

D.2 Safety activities during the concept phase

D.2.1 Development of the item definition.

D.2.2 Hazard analysis and risk assessment.

D.2.3 Functional safety concept.

D.2.4 Dependencies of the item and its safety concept with other systems/functions.

D.2.5 Allocation of functional safety requirements to:

— E/E elements;

— elements implemented by other technologies; and

— interfaces with external measures.

D.2.6 Verification of the functional safety concept.

D.3 Safety activities during the system development

D.3.1 Planning of the system development, integration and validation.

D.3.2 Technical safety concept and its verification.

D.3.3 System design and avoidance of systematic failures.

D.3.4 Allocation of the technical safety requirements to hardware and software elements and a review of the hardware-software interface.

D.3.5 Verification of the system design.

D.4 Hardware development

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

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

D.4.3 Hardware architectural constraints.

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

D.4.5 Hardware integration and testing.

D.5 Software development

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

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

D.5.3 Software unit testing.

D.5.4 Software integration and testing.

D.5.5 Verification of the software safety requirements.

D.6 Item integration

D.6.1 Planning of the integration tests.

D.6.2 Hardware-software integration and testing.

D.6.3 System/item integration and testing.

D.6.4 Vehicle integration and testing.

D.7 Safety validation

D.7.1 Safety validation activities.

D.7.2 Safety validation documentation.

D.8 Supplier(s) functional safety assessments.

D.8.1 Consideration of the supplier(s) functional safety assessment reports.

D.9 Safety-related special characteristics

D.9.1 Safety-related special characteristics for production.

D.9.2 Safety-related special characteristics for operation, service and decommissioning.

D.10 Summary

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

Annex E
(informative)

Guidance on potential interaction of functional safety with cybersecurity

E.1 Objectives

To address potential adverse effects of cybersecurity on the achievement of functional safety, this annex provides guidance on the possible interactions between the activities of functional safety and cybersecurity where both contribute to the overall achievement of safe E/E systems.

The aim is to provide guidance from the perspective of functional safety and not to provide guidance on the achievement of cybersecurity. The relationship between development processes of functional safety and cybersecurity depends on the organization and the scope of the project, therefore the methods or the technical content of the interaction is not described. Organizations can determine the most appropriate approach for this interaction.

E.2 General

While functional safety addresses systematic and random faults resulting in malfunctioning behaviour of E/E systems, cybersecurity addresses issues resulting from malicious intent external to the E/E system.

To achieve functional safety it can be advantageous to know relevant information from cybersecurity that can negatively impact functional safety or that can support the achievement of functional safety.

NOTE Refer also to SAE J3061, ISO/IEC 27001 and ISO/IEC 15408.

E.3 Potential interaction between functional safety and cybersecurity

E.3.1 Functional safety management

Functional safety management interaction with the management of cybersecurity can include:

— plans and milestones for cybersecurity activities in order to consider dependencies that can influence the planning of the safety activities, for example, for the development of software, the selection of tools, programming languages and guidelines;

— coordination of the management of field monitoring activities for cybersecurity and functional safety including incident reporting, tracking and resolution in order to enable the communication of safety-related cybersecurity field incidents to functional safety.

E.3.2 Concept phase

In the concept phase, the interaction can include:

— cybersecurity threats to be analysed as a hazard from a functional safety perspective in order to support the completeness of the hazard analyses and risk assessment and the safety goals;

— functional safety can provide information such as hazards and associated risks to support the cybersecurity identification of threats;

— cybersecurity strategies or countermeasures related to the behaviour of the E/E-system in case of a detected attack in order to determine potential impacts on safety goals or safety concepts.

E.3.3 Product development

In product development, the interaction can include:

— technical information related to the design and implementation of the cybersecurity strategies or countermeasures for the E/E-system in order to determine potential impacts on the technical safety concept and the system design;

— cybersecurity software and hardware design considerations in order to determine potential impacts on the achievement of the software and hardware safety requirements and design constraints such as independence;

— functional safety can provide information related to design and implementation of safety measures in order to communicate functional safety constraints that can be relevant to cybersecurity;

— safety and cybersecurity analysis activities can be harmonized in order to uncover potential cybersecurity impacts on functional safety. Safety analyses can also consider the impact of cybersecurity strategies and countermeasures; and

— cybersecurity countermeasures identified to address systematic failures in order to determine the potential impacts on functional safety, for example, methods required for the development of safety measures that are shared with cybersecurity.

E.3.4 Production and operation

During production and operation the interaction can include:

— cybersecurity incident resolution strategies in order to consider potential impacts on functional safety due to design changes resulting from cybersecurity incident response.

Bibliography

[1] ISO 26262-10, *Guidelines on ISO 26262*

[2] ISO 26262-12, *Adaptation of ISO 26262 for motorcycles*

[3] ISO 9001, *Quality management systems — Requirements*

[4] IATF 16949, *Quality management system requirements for automotive production and relevant service parts organizations*

[5] ISO/IEC 33000 (all parts), *Information technology — Process assessment*

[6] IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

[7] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[8] ISO/IEC 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

[9] SAE J3061, *Cybersecurity Guidebook for Cyber-Physical vehicle Systems*

[10] No S.S. 75-INSAG-4, *International Atomic Energy Agency, Vienna*, 1991

[11] United Kingdom Health and Safety Executive. *Managing competence for safety-related systems,* 2007

[12] Automotive SPICE [viewed 2017-10-11]. Available at: http://www.automotivespice.com

[13] CMMI for Development [viewed 2017-10-11]. Available at: http://www.cmmiinstitute.com/resources

This page is intentionally blank.

This page is intentionally blank.

ICS 43.040.10

Price based on 45 pages