INTERNATIONAL STANDARD

ISO 26262-8

Second edition
2018-12

Road vehicles — Functional safety —

Part 8: https://www.kekaoxing.com Supporting processes

Véhicules routiers — Sécurité fonctionnelle —

Partie 8: Processus d'appui

Reference number
ISO 26262-8:2018(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: Foreword - Supplementary information

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.

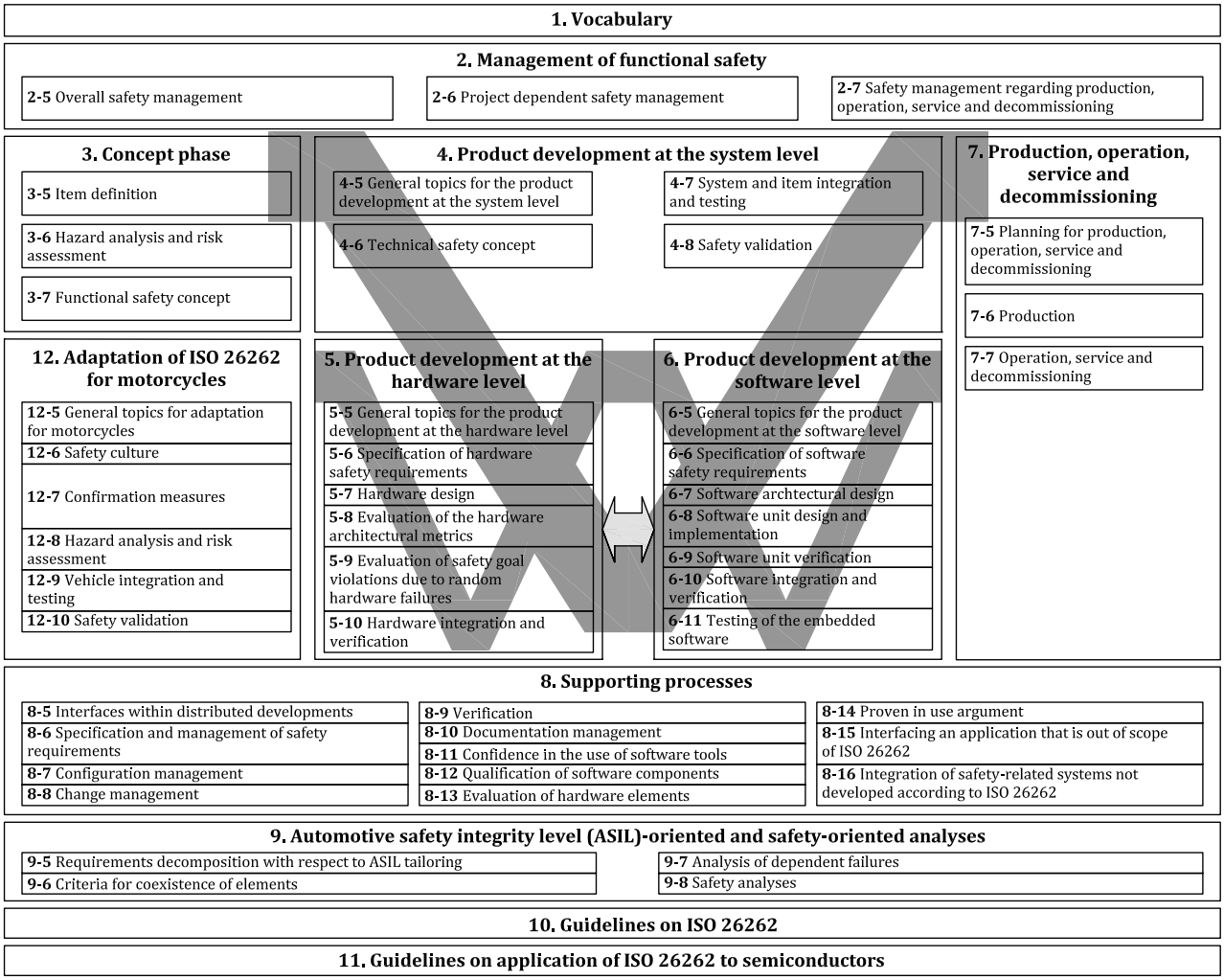


Figure 1 — Overview of ISO 26262

Road vehicles — Functional safety —

Part 8: Supporting processes

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 supporting processes, including the following:

— interfaces within distributed developments;

— overall management of safety requirements;

— configuration management;

— change management;

— verification;

— documentation management;

— confidence in the use of software tools;

— qualification of software components;

— evaluation of hardware elements;

— proven in use argument;

— interfacing an application that is out of scope of ISO 26262; and

— integration of safety-related systems not developed according to ISO 26262.

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 26262-2:2018, *Road vehicles — Functional safety — Part 2: Management of functional safety*

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 26262-9:2018, *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 ISO 26262-2 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 ISO 26262-2.

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 ISO 26262-2 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 Interfaces within distributed developments

5.1 Objectives

The objectives of this clause are:

a) to define the interactions and dependencies between customers and suppliers for development activities;

b) to describe the allocation of responsibilities; and

c) to identify the work products to be exchanged for distributed developments of an item and its elements.

5.2 General

The customer (e.g. vehicle manufacturer) and the suppliers for item or element developments jointly comply with the requirements specified in the ISO 26262 series of standards for distributed developments. Responsibilities are agreed between the customer and the suppliers for the concept, development, production, operation, service and decommissioning phases of the safety lifecycle. Subcontractor relationships are permitted. The customer has safety-related procedures concerning planning, execution and documentation for in-house item developments, therefore comparable procedures apply for co-operation with the supplier on distributed item developments. The same applies for item developments where the supplier has the full responsibility for functional safety.

NOTE 1 The Development Interface Agreement (DIA) aims to describe the roles and responsibilities between the customer and supplier. Consequently the safety planning by the customer and supplier is in line with the DIA.

NOTE 2 This clause is not relevant for the procurement which do not place any responsibility for safety on the supplier, including standard components and parts or development commissions.

NOTE 3 This note applies to T&B: this clause is not relevant for body builder equipment being integrated into base vehicles. Clause 15 applies when integrating body builder equipment developed according to ISO 26262 into a base vehicle which is in scope of another standard. Clause 16 applies when body builder equipment developed according to another standard is integrated into a base vehicle developed according to ISO 26262.

5.3 Inputs to this clause

5.3.1 Prerequisites

See applicable prerequisites of the relevant phases of the safety lifecycle for which a distributed development is planned and carried out.

5.3.2 Further supporting information

The following information can be considered:

— any applicable supporting information of the relevant phases of the safety lifecycle for which a distributed development is planned and carried out; and

— the supplier's tender based on a request for quotation (RFQ) (from an external source).

5.4 Requirements and recommendations

5.4.1 Application of requirements

5.4.1.1 The requirements of this clause shall apply to each item and element developed in accordance with the ISO 26262 series of standards, except for off-the-shelf elements not built-to-order to fulfil specific safety requirements, if one of the following applies:

a) the off-the-shelf hardware element is qualified according to well-established procedures based on quality standards (e.g. AEC standards for electronic components), and is evaluated according to Clause 13,

b) the off-the-shelf software component is qualified according to Clause 12, or

c) the off-the-shelf hardware element or software component is developed as an SEooC.

NOTE 1 Off-the-shelf hardware elements or software components not built-to-order can be a customer-independent SEooC, with project-specific modification covered by the specification of the element.

EXAMPLE Communication stack, operating systems or software libraries are off-the-shelf elements.

NOTE 2 The SEooC assumptions are validated in its target application according to ISO 26262-2:2018, 6.4.5.7.

5.4.1.2 Requirements on the customer-supplier relationship (interfaces and interactions) shall apply to each level of the customer-supplier relationship.

NOTE 1 This includes subcontracts taken out by the supplier or subcontracts taken out by those subcontractors, etc.

NOTE 2 Internal suppliers can be managed in the same way as external suppliers.

5.4.2 Supplier selection criteria

5.4.2.1 The supplier selection criteria shall include an evaluation of the supplier's capability to develop and, if applicable, produce items and elements of comparable complexity and ASIL according to the ISO 26262 series of standards.

NOTE Supplier selection criteria include:

— evidence of the supplier's quality management system,

— the previous performance and quality of the supplier,

— the confirmation of the supplier's capability concerning functional safety as part of the supplier's tender,

— results of previous functional safety assessments according to ISO 26262-2:2018, 6.4.12, or

— recommendations from the development, production, quality and logistics departments of the vehicle manufacturer as far as they impact functional safety.

5.4.2.2 The RFQ from the customer to the supplier candidates shall include:

a) a formal request to comply with ISO 26262;

b) the specification of the scope of supply;

NOTE The specification of the scope of supply defines the functions, properties and boundaries of the items or elements requested from the supplier.

c) the safety goals or the set of relevant safety requirements including their assigned ASIL, if already available, depending on what the supplier is quoting for; and

NOTE If the ASIL is not known at the time of supplier selection, a conservative assumption can be made.

d) the element target values for failure rates and diagnostic coverage according to ISO 26262-4:2018, 6.4.5.3, if already available, depending on what the supplier is quoting for.

5.4.3 Initiation and planning of distributed development

5.4.3.1 The customer and the supplier shall specify a DIA including the following:

a) the appointment of the customer's and the supplier's safety managers;

b) the joint tailoring of the safety activities in accordance with ISO 26262-2:2018, 6.4.5;

c) the activities of the safety lifecycle to be performed by the customer and the activities of the safety lifecycle to be performed by the supplier;

NOTE 1 The joint planning of activities, including responsibilities related to functional safety assessment and functional safety audits according to ISO 26262-2, is considered.

d) the information and the work products to be shared, including distribution and reviews;

NOTE 2 This includes an agreement on the documentation to be provided for the completion of the customer's and supplier's safety cases.

NOTE 3 The information exchanged includes the safety-related special characteristics.

NOTE 4 The relevant parts of the work products necessary for the activities of the development parties involved can be identified and exchanged.

e) the responsibility assigned to each party for each activity;

NOTE 5 This responsibility can be expressed as "Responsible"; "Accountable"; "Support"; "Inform"; "Consult".

f) the communication or confirmation [see 5.4.2.2 d)] of the target values, derived from the system level targets, to each relevant party in order for them to meet the target values for single-point fault metric and latent fault metric in accordance with the evaluation of the hardware architectural metrics and the evaluation of safety goal violations due to random hardware failures (see ISO 26262-5);

g) the interface-related processes, methods and tools needed for the collaboration between customer and supplier;

NOTE 6 Versions and Revisions of processes and tools and tool configuration could be relevant.

h) the agreement on which party (supplier or customer) performs the safety validation in accordance with ISO 26262-4;

NOTE 7 If the supplier performs the vehicle integration and validation, an agreement on the capabilities and resources needed by the supplier is important since safety validation requires the integrated vehicle (see ISO 26262-4).

i) the functional safety assessment activities, in accordance with ISO 26262-2, regarding the elements or work products developed by the supplier;

NOTE 8 These functional safety assessment activities of the elements or work products developed by the supplier can be performed by the supplier itself, by the customer, or by an organization or person designated by the customer or by the supplier.

j) the planning of the supplier's functional safety assessment report; and

NOTE 9 The DIA includes the minimum contents, its version and the milestones of the report(s).

NOTE 10 An example of a DIA is given in Annex B.

k) the agreement between customer and supplier(s) that allows a customer assigned auditor to perform functional safety audits at the supplier's premises.

5.4.3.2 If the supplier conducts the hazard analysis and risk assessment, then the hazard analysis and risk assessment shall be provided to the customer for verification and approval.

5.4.3.3 The party responsible for the concept phase shall create the functional safety concept in accordance with ISO 26262-3.

5.4.4 Execution of distributed development

5.4.4.1 The customer shall ensure that the supplier receives the information and data required for performing the safety activities agreed in the DIA in a timely manner.

5.4.4.2 The supplier shall report to the customer issues that can increase the risk of not complying with the provisions of the DIA.

5.4.4.3 The supplier shall report to the customer safety anomalies which occur during the development activities in their area of responsibility or in that of their subcontractors.

5.4.4.4 The identified safety anomalies that potentially impact the deliverables from the supplier shall be analysed and actions shall be taken to resolve them. An agreement between both parties shall be reached on who performs the actions required.

5.4.4.5 The supplier shall determine whether the safety requirements from the customer are feasible and whether 6.4.1 and 6.4.2 are satisfied. If not, the safety requirements shall be re-examined and, where appropriate, modified by the customer to ensure the correct specification of safety requirements.

5.4.4.6 The supplier shall communicate to the customer the safety requirements of the supplied elements of the item that are outside of its responsibility, but that the supplier deems as necessary to ensure the achievement of functional safety.

5.4.4.7 Both parties should consider previous experience gained in similar developments in accordance with ISO 26262-2:2018, 5.4.2.6, when deriving safety requirements for the current development.

5.4.4.8 The supplier shall report the progress achieved against the tasks and milestones defined in the safety plan to the customer. The contents of the report and the delivery dates shall be agreed between the supplier and the customer.

5.4.5 Functional safety assessment activities in a distributed development

5.4.5.1 For an element which the highest ASIL of the allocated safety requirements is an ASIL (B), C or D, the DIA shall specify which organization performs the functional safety assessment activities, in accordance with ISO 26262-2, regarding the elements or work products developed by the supplier.

NOTE 1 These functional safety assessment activities of the elements or work products developed by the supplier can be performed by the supplier itself, by the customer, or by an organization or person designated by the customer or by the supplier.

NOTE 2 All of these are agreed with the customer during the DIA approval.

5.4.5.2 For an element which the highest ASIL of the allocated safety requirements is an ASIL (B), C or D, the DIA shall specify the planning of the supplier's functional safety assessment activities.

NOTE The planning includes the minimum contents and the milestones of the report(s).

5.4.5.3 For an element which the highest ASIL of the allocated safety requirements is an ASIL (B), C or D, the supplier shall provide functional safety assessment reports to the customer, which includes the supplier's evaluation if the developed elements comply with the safety requirements received from the customer and if the implemented processes meet the criteria to achieve functional safety.

5.4.5.4 For an element which the highest ASIL of the allocated safety requirements is an ASIL (B), C or D, the results of the supplier's functional safety assessment activities shall be made available to the customer and the supplier.

5.4.6 Agreement for production, operation, service and decommissioning

5.4.6.1 The supplier shall provide evidence to the customer that the production process capability is being met and maintained in accordance with ISO 26262-2:2018, Clause 7, and ISO 26262-7:2018, Clause 5 and Clause 6.

NOTE For guidance on production of semiconductors, refer to ISO 26262-11:2018, 4.9.

5.4.6.2 A supply agreement between the customer and the supplier shall address the responsibilities for functional safety in accordance with ISO 26262-2:2018, 7.4.2.1, and define the safety activities for each party.

NOTE For guidance on distributed development of semiconductors, refer to ISO 26262-11:2018, 4.10.

5.4.6.3 The supply agreement shall define the access to, and exchange of, production monitoring records between the parties for the safety-related special characteristics and the results of failure analysis of returned parts from the customer.

NOTE Such topics can already be adequately covered by quality management agreements.

5.4.6.4 The supply agreement shall define the timely communication channels related to the exchange of safety-related events and required analysis. The analysis of these events shall be done, for field issues, according to the established field monitoring process.

NOTE This analysis includes similar items and other parties which are potentially affected by similar events.

5.5 Work products

5.5.1 **Supplier selection report** resulting from requirements 5.4.2.1 and 5.4.2.2.

5.5.2 Development interface agreement (DIA) resulting from requirements 5.4.3, 5.4.5.1 and 5.4.5.2.

5.5.3 Supplier's safety plan resulting from requirements 5.4.3 and 5.4.4.

5.5.4 Functional safety assessment report resulting from requirements 5.4.5.3 and 5.4.5.4.

5.5.5 Supply agreement resulting from requirements 5.4.6.1 to 5.4.6.4.

6 Specification and management of safety requirements

6.1 Objectives

The objectives of this clause are:

a) to ensure the correct specification of safety requirements with respect to their attributes and characteristics; and

b) to ensure consistent management of safety requirements throughout the entire safety lifecycle.

6.2 General

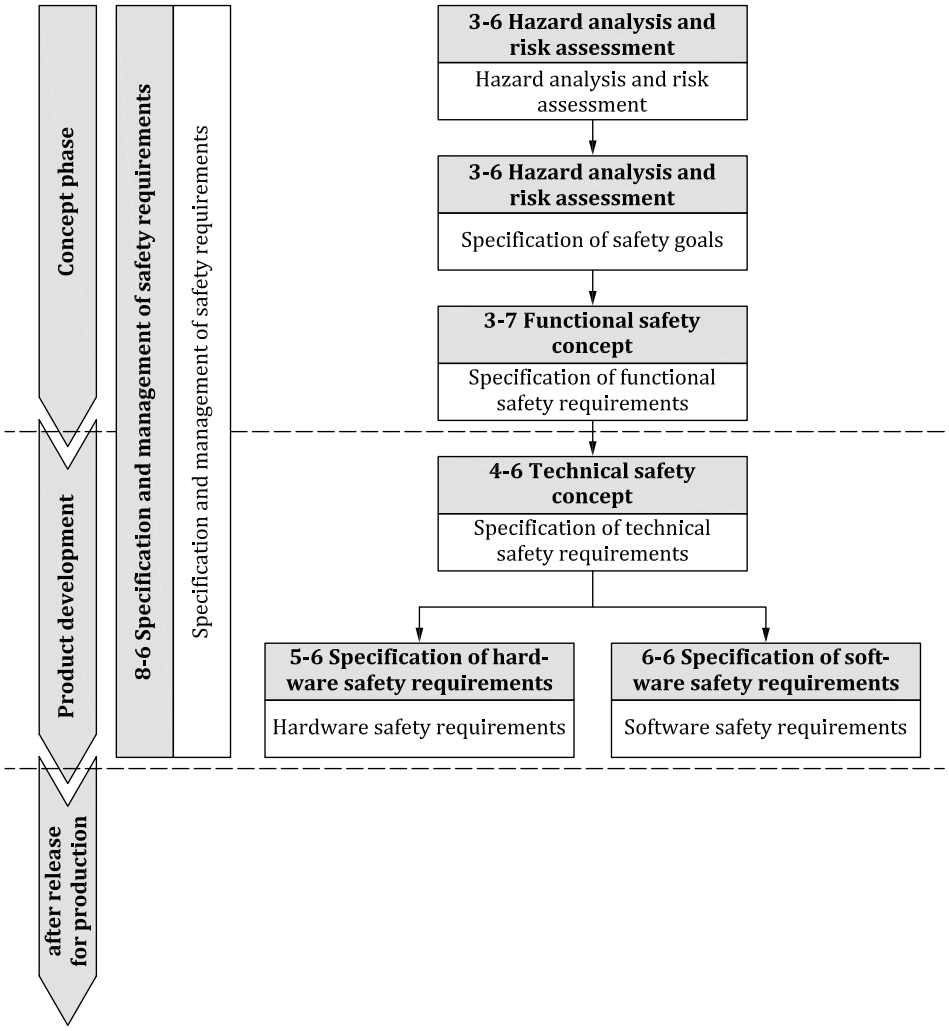
Safety requirements are requirements aimed at achieving and ensuring the required level of functional safety.

During the safety lifecycle, safety requirements are specified and detailed in a hierarchical structure. The structure and dependencies of safety requirements used in the ISO 26262 series of standards are illustrated in Figure 2. The safety requirements are allocated or distributed among the elements.

The management of safety requirements includes obtaining agreement on them, obtaining commitments from those implementing the safety requirements, and maintaining traceability.

In order to support the management of safety requirements, the use of suitable requirements management tools is recommended.

The specific requirements concerning the content of the safety requirements at different hierarchical levels are listed in ISO 26262-3, ISO 26262-4, ISO 26262-5 and ISO 26262-6.



NOTE Within the figure, the specific clauses of each part of ISO 26262 are indicated in the following manner: "m-n", where "m" represents the number of the part and "n" indicates the number of the clause, e.g. "3-7" represents ISO 26262-3:2018, Clause 7.

Figure 2 — Structure of safety requirements

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 ISO 26262-2:2018, 5.5.1; and

— applicable prerequisites of the relevant phases of the safety lifecycle in which safety requirements are specified or managed.

6.3.2 Further supporting information

See applicable further supporting information of the relevant phases of the safety lifecycle in which safety requirements are specified or managed.

6.4 Requirements and recommendations

6.4.1 Specification of safety requirements

To achieve the characteristics of safety requirements listed in 6.4.2.4, safety requirements shall be specified by an appropriate combination of:

a) natural language; and

b) methods listed in Table 1.

Table 1 — Specifying safety requirements

Methods		ASIL			
		A	B	C	D
1a	Informal notations for requirements specification[a, b]	++	++	+	+
1b	Semi-formal notations for requirements specification[a,b,c,d]	+	+	++	++
1c	Formal notations for requirements specification [a]	+	+	+	+

[a] An appropriate selection of methods for the specification of safety requirement considers their adequacy to achieve the characteristics of safety requirement according to 6.4.2 for a specific issue to be specified, its complexity or the knowledge of the persons specifying or managing safety requirements. Examples include the use of state graphs or diagrams for specifying the complex behaviour of software or hardware including many states or/and complex transitions.

[b] For higher level safety requirements (e.g. safety goals, functional and technical safety requirements) natural language and other types of informal notations are the most appropriate forms, though some requirements may be better handled with semi-formal notations.

[c] Semi-formal notation formulates requirements using natural language that is supplemented by mathematical or graphical elements such as equations, graphs, diagrams, flow charts, timing diagrams, and many other forms of representation (e.g. UML® and SysML™). Examples include model-based techniques and applying templates and controlled vocabulary for requirement sentences in natural language.

[d] For lower-level safety requirements where precise hardware and software behaviours and capabilities may be specified, semi-formal notations are more appropriate due to greater clarity. However, even here it may not be possible or necessary to use semi-formal techniques for every requirement.

6.4.2 Attributes and characteristics of safety requirements

6.4.2.1 Safety requirements shall be unambiguously identifiable as safety requirements.

NOTE In order to comply with this requirement, safety requirements can be listed in a separate document. If safety requirements and other requirements are administered in the same document, safety requirements can be identified explicitly by using a special attribute as described in 6.4.2.5.

6.4.2.2 Safety requirements shall inherit the ASIL from the safety requirements from which they are derived, except if ASIL decomposition is applied in accordance with ISO 26262-9.

NOTE As safety goals are the top level safety requirements, the inheritance of ASILs starts at the safety goal level.

6.4.2.3 Safety requirements shall be allocated to the item or element which implements them.

6.4.2.4 Safety requirements shall have the following characteristics:

NOTE 1 The characteristics for safety requirements enable clear communication to the stakeholders. They are the principle means of communicating the safety requirements to those who must implement them. The characteristics cited below are consistent with those referenced by ISO/IEC/IEEE 29148 (see Reference [8]).

a) unambiguous;

NOTE 2 A requirement is unambiguous if there is a common understanding of the meaning of the requirement.

b) comprehensible;

NOTE 3 A requirement is comprehensible if the stakeholders and the consumers of that requirement understand its meaning.

c) atomic (singular);

NOTE 4 Safety requirements at one hierarchical level are atomic when they are formulated in such a way that they cannot be divided into at least two independent safety requirements at the considered level. The achievement of this characteristic could contradict the achievement of the other essential characteristics of safety requirements. In such a case, atomicity can be considered as having less importance.

d) internally consistent;

NOTE 5 A requirement is internally consistent if it contains no contradictions within itself.

e) feasible and achievable;

NOTE 6 A requirement is feasible if it can be implemented within the constraints of the item development (resources, state-of-the-art, etc.).

NOTE 7 A requirement can be accomplished technically, it does not require major technology advances, and fits within item constraints (e.g., cost schedule, technical, legal, regulatory, etc.) acceptably.

f) verifiable;

NOTE 8 A requirement is verifiable if means, at the level where it is specified, are available to check that the requirement is fulfilled.

NOTE 9 Collected evidence pertaining to an item shows the corresponding requirement has been satisfied. Verifiability is enhanced when the requirement is measureable.

g) necessary;

NOTE 10 The requirement defines an essential capability, characteristic, constraint, and/or quality factor. If it is removed or deleted, a deficiency will exist which is not fulfilled by other capabilities of the product or process.

NOTE 11 The requirement is currently applicable and has not been made obsolete by the passage of time. Requirements with planned expiration dates or applicability dates are clearly identified.

h) implementation free;

NOTE 12 The requirement, while addressing what is necessary and sufficient for the item, avoids placing unnecessary constraints on the architectural design. The objective is to be implementation independent. The requirement states what is required, not how the requirement should be met.

i) complete; and

NOTE 13 The stated requirement is clear without further amplification because it is measureable and sufficiently describes the capability and characteristics required to meet the stakeholder's need.

j) conforming.

NOTE 14 The stated requirement conforms to applicable government, automotive industry and product standards, specifications and interfaces for which compliance is required.

6.4.2.5 Safety requirements shall have the following attributes:

a) a unique identification remaining unchanged throughout the safety lifecycle;

EXAMPLE 1 A unique identification of a requirement can be achieved in a variety of ways, such as subscripting each instance of the word "shall", e.g. "The system $shall_{9782}$ check …", or numbering consecutively each sentence containing the word "shall", e.g. "9782 In the case of … the system shall check …".

b) a status; and

EXAMPLE 2 A status of a safety requirement can be "proposed", "assumed", "accepted", "reviewed", "delivered" or "verified".

c) an ASIL.

6.4.3 Management of safety requirements

6.4.3.1 The set of safety requirements for an item, an element, which are derived from one or more safety goals shall have the following properties:

a) hierarchical structure;

NOTE 1 Hierarchical structure means that safety requirements are structured in several successive levels as presented in Figure 2. These levels are always aligned to comply with the corresponding design phases. It is possible that there could be several levels of hierarchy within any of the design phases of Figure 2.

b) organizational structure according to an appropriate grouping scheme;

NOTE 2 Organization of safety requirements means that safety requirements within each level are grouped together, usually corresponding to the architecture.

c) completeness;

NOTE 3 Completeness means that the safety requirements at one level fully implement all safety requirements of the previous level.

d) external consistency;

NOTE 4 Unlike internal consistency, in which an individual safety requirement does not contradict itself, external consistency means that multiple safety requirements do not contradict each other.

e) no duplication of information within any level of the hierarchical structure; and

NOTE 5 No duplication of information means that the content of safety requirements is not repeated in any other safety requirement at one single level of the hierarchical structure and this is true at each hierarchical level.

f) maintainability.

NOTE 6 Maintainability means that the set of requirements can be modified or extended, e.g. by the introduction of new versions of requirements or by adding/removing requirements to the set of requirements.

NOTE 7 Maintainability is facilitated when each requirement meets all of the points of 6.4.2.4, and the set of requirements meets 6.4.3.1.

6.4.3.2 Safety requirements shall be traceable with a reference being made to:

a) each source of a safety requirement at the next upper hierarchical level;

b) each derived safety requirement at the next lower hierarchical level, or to its realisation in the design; and

c) the verification specification in accordance with 9.4.2.

NOTE 1 Various types of traceability records such as requirement management system, electronic materials, etc., can be used.

NOTE 2 Traceability supports:

— the achievement of consistency between a requirement, its realisation and verification,

— the effectiveness of an impact analysis if changes are made to particular safety requirements, and

— the execution of confirmation measures (e.g. functional safety assessment to evaluate the achieved functional safety).

6.4.3.3 An appropriate combination of the verification methods listed in Table 2 shall be applied to verify that the safety requirements comply with the requirements in this clause and that they comply with the specific requirements on the verification of safety requirements within the respective parts of the ISO 26262 series of standards where safety requirements are derived.

Table 2 — Methods for the verification of safety requirements

Methods		ASIL			
		A	B	C	D
1a	Verification by walk-through	++	+	o	o
1b	Verification by inspection	+	++	++	++
1c	Semi-formal verification[a]	+	+	++	++
1d	Formal verification[a]	o	+	+	+
[a] Verification can be supported by executable models.					

6.4.3.4 Safety requirements shall be placed under configuration management in accordance with Clause 7 to maintain consistency throughout the safety lifecycle.

EXAMPLE When the safety requirements at a lower level are consistent with the higher level safety requirements, the configuration management can define a baseline as the basis for subsequent phases of the safety lifecycle.

6.5 Work products

None.

7 Configuration management

7.1 Objectives

The objectives of this clause are:

a) to ensure that the work products, items, elements and the principles and general conditions of their creation can be uniquely identified and reproduced in a controlled manner at any time; and

b) to ensure that the relations and differences between earlier and current versions can be traced.

7.2 General

Configuration management is a well-established practice within the automotive industry and can be applied according to e.g. ISO 10007, Automotive SPICE®[1)], the ISO/IEC 33000 series of standards, ISO/IEC/IEEE 15288 [4], and ISO/IEC/IEEE 12207.

Each work product of the ISO 26262 series of standards is subject to configuration management.

1) 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 these products.

7.3 Inputs to this clause

7.3.1 Prerequisites

The following information shall be available:

— safety plan in accordance with ISO 26262-2:2018, 6.5.3;

— organization-specific rules and processes for functional safety in accordance with ISO 26262-2:2018, 5.5.1; and

— applicable prerequisites of the relevant phases of the safety lifecycle where configuration management is planned or managed.

7.3.2 Further supporting information

None.

7.4 Requirements and recommendations

7.4.1 Configuration management shall be planned.

NOTE The configuration management plan can include responsibilities and resources, tools and repositories, identification of configuration item and naming convention, access rights, baseline with schedule, procedures for release/approval.

7.4.2 The configuration management process shall comply with:

a) the respective requirements of a quality management system standard; and

b) the specific requirements for software development.

NOTE 1 Specific requirements for software configuration management for software development are given in ISO/IEC/IEEE 12207.

NOTE 2 The configuration management process can be adapted to the corresponding phase of development.

7.4.3 The work products required by the safety plan and those needed to reproduce the items and elements shall be baselined and placed under configuration management according to the configuration management strategy.

7.4.4 The configuration management strategy shall define the conditions or purposes throughout the safety lifecycle for which work products, items and elements need to be uniquely identified and reproduced.

EXAMPLE Conditions or purposes for creating a configuration of work products, items and elements can take place before they are exchanged as part of a safety activity in customer-supplier relationships.

7.4.5 Configuration management shall be maintained throughout the entire safety lifecycle.

7.5 Work products

7.5.1 **Configuration management plan** resulting from requirements 7.4.1 to 7.4.5.

8 Change management

8.1 Objectives

The objective of change management is to analyse and control changes to safety-related work products, items and elements throughout the safety lifecycle.

8.2 General

Change management ensures the systematic planning, control, monitoring, implementation and documentation of changes, while maintaining the relevant functions and properties of the work products, item and elements throughout the safety lifecycle.

NOTE Change is understood as modification due to: anomalies, removals, additions, enhancements, obsolescence of components or parts, etc.

Change management is a well-established practice within the automotive industry and can be applied according to e.g. ISO 10007, Automotive SPICE®[2)], the ISO/IEC 33000 series of standards, ISO/IEC/IEEE 15288 [4], or ISO/IEC/IEEE 12207.

8.3 Inputs to this clause

8.3.1 Prerequisites

The following information shall be available:

— configuration management plan in accordance with 7.5.1;

— safety plan in accordance with ISO 26262-2:2018, 6.5.3;, and

— organization-specific rules and processes for functional safety in accordance with ISO 26262-2:2018, 5.5.1.

8.3.2 Further supporting information

None.

8.4 Requirements and recommendations

8.4.1 Planning and initiating change management

8.4.1.1 The change management process shall be planned and initiated before changes are made to work products.

NOTE Configuration management and change management are interrelated. Interfaces between the two processes are defined and maintained to enable the effectiveness of change management.

8.4.1.2 The work products, items and elements to be subject to change management shall be identified in the change management plan and shall include those work products, items and elements required in 7.4.3.

8.4.1.3 The schedule for applying the change management process shall be defined for the identified work products, items and elements.

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 these products.

8.4.1.4 The change management process shall include:

a) the change requests in accordance with 8.4.2;

b) the analysis of change requests in accordance with 8.4.3;

c) the decision and rationale regarding change requests in accordance with 8.4.4;

d) the implementation and verification of the accepted changes in accordance with 8.4.5; and

e) the documentation in accordance with 8.4.5.

NOTE 1 The change management process can be adapted to the corresponding phase of development.

NOTE 2 Several changes can be handled within one change request.

8.4.2 Change requests

8.4.2.1 A unique identifier shall be assigned to each change request.

8.4.2.2 As a minimum, every change request shall include the following information:

a) the date;

b) the reason for the requested change;

c) the exact description of the requested change; and

d) the configuration on which the requested change is based.

8.4.3 Change request analysis

8.4.3.1 An impact analysis on the item or element involved, its interfaces and connected items or elements, shall be carried out for each change request. The following shall be addressed:

a) the type of change request;

EXAMPLE Possible types of changes include: error resolution, adaptation, elimination, enhancement, prevention.

b) the identification of the work products, items and elements affected and the work products, items and elements to be changed;

c) the identification and responsibilities of the parties involved, in the case of a distributed development;

d) the potential impact of the change on functional safety; and

e) the schedule for the realisation and verification of the change.

8.4.3.2 Each change to a work product shall initiate the return to the applicable phase of the safety lifecycle. Subsequent phases shall be carried out in compliance with ISO 26262.

8.4.4 Change request evaluation

8.4.4.1 The change request shall be evaluated using the results of the impact analysis in compliance with 8.4.3.1 and a decision regarding acceptance, rejection or delay shall be made by the authorized persons.

EXAMPLE Typically, the authorised persons include:

— project manager;

— safety manager;

— person in charge of quality assurance; and

— developers involved.

NOTE The accepted change requests can be prioritised and combined with related accepted change requests.

8.4.4.2 For each accepted change request it shall be decided who shall carry out the change and when the change is due. This decision shall consider the interfaces involved in carrying out the change request.

8.4.5 Implementing and documenting the change

8.4.5.1 The changes shall be implemented and verified as planned.

8.4.5.2 If the change has an impact on safety-related functions or properties, the assessment of functional safety and the applicable confirmation reviews, in accordance with ISO 26262-2:2018, 6.4.9 and ISO 26262-2:2018, 6.4.10, shall be updated before releasing the item.

8.4.5.3 The documentation of the change shall contain the following information:

a) the list of changed work products, items and elements at an appropriate level including configurations and versions, in accordance with Clause 7;

b) the details of the change carried out; and

c) the planned date for the deployment of the change.

NOTE 1 In the case of a change request relating to a change that is expected to be temporary, the rationale for this change request and the period during which the change will persist (if known) are explicitly indicated.

NOTE 2 In the case of a rejected change request, the change request and the rationale for the rejection are also documented.

8.5 Work products

8.5.1 **Change management plan** resulting from requirements 8.4.1.

8.5.2 **Change request** resulting from requirements 8.4.2.

8.5.3 **Impact analysis and change request plan** resulting from requirements 8.4.3 and 8.4.4.

8.5.4 **Change report** resulting from requirement 8.4.5.

9 Verification

9.1 Objectives

The objective of verification is to ensure that the work products comply with their requirements.

9.2 General

Verification is applicable to the following phases of the safety lifecycle:

a) in the concept phase, verification ensures that the concept is correct, complete and consistent with respect to the boundary conditions of the item, and that the defined boundary conditions themselves are correct, complete and consistent, so that the concept can be realised;

b) in the product development phase, verification is conducted in different forms, as described below:

   — In the design phases, verification is the evaluation of the work products, such as requirement specification, architectural design, models, or software code, thus ensuring that they comply with previously established requirements for correctness, completeness and consistency. Evaluation can be performed by review, simulation or analysis techniques. The evaluation is planned, specified, executed and documented in a systematic manner.

     NOTE Design phases are ISO 26262-4:2018, Clause 6, ISO 26262-5:2018, Clause 7, ISO 26262-6:2018, Clause 7 and ISO 26262-6:2018, Clause 8.

   — In the test phases, verification is the evaluation of the work products, items and elements within a test environment to ensure that they comply with their requirements. The tests are planned, specified, executed, evaluated and documented in a systematic manner.

c) In the production and operation phase, verification ensures that:

   — the safety-related special characteristics are appropriately met during production,

   — the safety-related information is appropriately provided in the user manuals and in the repair and maintenance instructions; and

   — the safety-related properties of the item are met by the application of control measures within the production process.

NOTE This is a generic verification process that is instantiated by phases of the safety lifecycle in ISO 26262-3, ISO 26262-4, ISO 26262-5, ISO 26262-6 and ISO 26262-7. Safety validation is not addressed by this process. See ISO 26262-4:2018, Clause 8, for further details.

9.3 Inputs to this clause

9.3.1 Prerequisites

The following information shall be available:

— organization-specific rules and processes for functional safety in accordance with ISO 26262-2:2018, 5.5.1; and

— applicable prerequisites of the relevant phases of the safety lifecycle in which verification is planned or carried out.

9.3.2 Further supporting information

See applicable further supporting information of the relevant phases of the safety lifecycle in which verification is planned or carried out.

9.4 Requirements and recommendations

9.4.1 Verification planning

9.4.1.1 The verification planning shall be carried out for each phase and sub-phase of the safety lifecycle and shall address the following:

a) the content of the work products to be verified;

b) the objective of the verification;

c) the methods used for verification;

d) the pass and fail criteria for the verification;

e) the verification environment, if applicable;

NOTE A verification environment can be a test or simulation environment.

f) the equipment used for verification, if applicable;

EXAMPLE Test tools or measurement equipment.

g) the resources needed for verification, if applicable;

h) the actions to be taken if anomalies are detected; and

i) the regression strategy.

NOTE A regression strategy specifies how verification is repeated after changes have been made to the item or element. Verification can be repeated fully or partially and can include other items or elements that might affect the results of the verification.

9.4.1.2 The planning of verification should consider the following:

a) the adequacy of the verification methods to be applied;

b) the complexity of the work product to be verified;

c) prior experiences related to the verification of the subject material; and

NOTE This includes service history as well as the degree to which a proven in use argument has been achieved.

d) the degree of maturity of the technologies used, or the risks associated with the use of these technologies.

9.4.2 Verification specification

9.4.2.1 The verification specification shall specify the methods to be used for the verification, and shall include:

a) review or analysis checklists, or

b) simulation scenarios, or

c) test cases, test data and test objects.

9.4.2.2 For testing, the specification of each test case shall include the following:

a) a unique identification;

b) the reference to the version of the associated work product to be verified;

c) the preconditions and configurations;

NOTE If a complete verification of the possible configurations of a work product (e.g. variants of a system) is not feasible, a reasonable subset is selected (e.g. minimum or maximum functionality configurations of a system).

d) the environmental conditions, if appropriate;

NOTE Environmental conditions relate to the physical properties (e.g. temperature) of the surroundings in which the test is conducted or is simulated as part of the test.

e) the input data, their time sequence and their values;

f) the expected behaviour which includes output data, acceptable ranges of output values, time behaviour and tolerance behaviour; and

NOTE 1 When specifying the expected behaviour, it can be necessary to specify the initial output data in order to detect changes.

NOTE 2 It can be necessary to use an unambiguous reference to avoid the redundant specification and storage of preconditions, configurations and environmental conditions used for various test cases.

g) the criteria to determine the test case as passed or failed.

9.4.2.3 For testing, test cases shall be grouped according to the test methods to be applied, considering the following aspects:

a) the required test equipment or test environment;

b) the logical and temporal dependencies; and

c) the resources.

EXAMPLE Grouping of test cases for regression testing vs. full testing.

9.4.2.4 For testing, test cases should be reviewed by a different person regarding the author(s) of the work product to be verified.

9.4.3 Verification execution and evaluation

9.4.3.1 The verification shall be executed as planned in accordance with 9.4.1 and specified in accordance with 9.4.2.

9.4.3.2 The verification should be performed by a different person regarding the author(s) of the work product to be verified.

9.4.3.3 The evaluation of the verification results shall contain the following information:

a) the unique identification of the verified work product;

b) the reference to the verification plan and verification specification;

c) the configuration of the verification environment and verification tools used and the calibration data used during the evaluation, if applicable;

d) the level of compliance of the verification results with the expected results;

e) an unambiguous statement of whether the verification passed or failed; if the verification failed the statement shall include the rationale for failure and suggestions for changes in the verified work product; and

NOTE The verification is evaluated according to the criteria for completion and termination of the verification [see 9.4.1.1 d)] and to the expected verification results.

f) the reasons for any verification steps not executed.

9.4.3.4 The test equipment used for verification shall be able to deliver valid and reproducible results and shall be controlled in accordance with the applied quality management system.

9.5 Work products

9.5.1 **Verification plan** resulting from requirements 9.4.1.1 and 9.4.1.2.

9.5.2 **Verification specification** resulting from requirements 9.4.2.1 to 9.4.2.4.

9.5.3 **Verification report** resulting from requirements 9.4.3.1 to 9.4.3.4.

10 Documentation management

10.1 Objectives

The objective is to develop a documentation management strategy for the entire safety lifecycle in order to facilitate an effective and repeatable documentation management process.

10.2 General

Documentation management is a well-established practice within the automotive industry and can be applied in accordance with a quality management system (e.g. IATF 16949 [6] or ISO 9001[3]) or related standard (e.g. ISO/IEC/IEEE 12207 or ISO/IEC/IEEE 15288 [4]).

The documentation requirements in the ISO 26262 series of standards focus mainly on content, and not on layout and appearance.

The information need not be made available in physical documents. The documentation can take various forms and structures and tools can be used to generate documents automatically.

EXAMPLE Possible forms are: paper, electronic media, databases.

What is deemed adequate information depends on a variety of factors, including the complexity, the extent of the safety-related systems/subsystems, and the requirements relating to the special application.

Duplication of information within a document, and between documents, should be avoided to aid maintainability.

NOTE An alternative to duplicating information is the use of a cross-reference within one document, directing the reader to the information source document.

10.3 Inputs to this clause

10.3.1 Prerequisites

The following information shall be available:

— organization-specific rules and processes for functional safety in accordance with ISO 26262-2:2018, 5.5.1; and

— safety plan in accordance with ISO 26262-2:2018, 6.5.3.

10.3.2 Further supporting information

None.

10.4 Requirements and recommendations

10.4.1 The documentation management process shall be planned in order to make documentation available:

a) during each phase of the entire safety lifecycle for the effective completion of the phases and verification activities;

b) for the management of functional safety; and

c) as an input to the confirmation measures.

10.4.2 The identification of a work product in the ISO 26262 series of standards shall be interpreted as a requirement for documentation containing the information concerning the results of the associated requirements.

NOTE The documentation can be in the form of a single document containing the complete information for the work product or a set of documents that together contain the complete information for the work product.

10.4.3 The documents should be:

a) precise and concise;

b) structured in a clear manner;

c) easy to understand by the intended users;

d) verifiable; and

e) maintainable.

10.4.4 The structure of the entire documentation should consider in-house procedures and working practices. It shall be organized to facilitate the search for relevant information.

EXAMPLE Documentation tree.

10.4.5 Each work product or document shall be associated with the following formal elements:

a) the title, referring to the scope of the content;

b) the author and approver;

c) unique identification of each different revision (version) of a document;

d) the change history; and

NOTE The change history contains, per change, the name of the author, the date and a brief description.

e) the status.

EXAMPLE "Draft", "released", "active", "expired".

10.4.6 It shall be possible to identify the current applicable revision (version) of a document or item of information, in accordance with Clause 7.

10.5 Work products

10.5.1 Documentation management plan resulting from requirement 10.4.1 and 10.4.2.

10.5.2 Documentation guideline requirements resulting from requirements 10.4.3 to 10.4.6.

11 Confidence in the use of software tools

11.1 Objectives

The objectives of this clause are:

a) to provide criteria to determine the required level of confidence in a software tool when applicable; and

b) to provide means for the qualification of the software tool when applicable, in order to create evidence that the software tool is suitable to be used to support the activities or tasks required by the ISO 26262 series of standards (i.e. the user can rely on the correct functioning of a software tool for those activities or tasks required by the ISO 26262 series of standards).

11.2 General

A software tool used in the development of a system or its software or hardware elements can support the activities and tasks required by ISO 26262. In such cases, confidence is needed that the software tool effectively achieves the following goals:

a) the risk of systematic faults in the developed product due to malfunctions of the software tool leading to erroneous outputs is minimized; and

b) the development process is adequate with respect to compliance with the ISO 26262 series of standards, if activities or tasks required by the ISO 26262 series of standards rely on the correct functioning of the software tool used.

NOTE 1 A "software tool" can vary from a stand-alone software package to a suite of software tools integrated into a tool-chain.

EXAMPLE 1 Commercial tools, open source tools, freeware tools, shareware tools or tools developed in-house by the user.

To determine the required level of confidence in a software tool used within development under the conditions mentioned above, the following criteria are evaluated:

— the possibility that the malfunctioning software tool and its corresponding erroneous output can introduce or fail to detect errors in a safety-related item or element being developed; and

— the confidence in preventing or detecting such errors in its corresponding output.

The tool may pre-exist or be developed upon request, based on the tool user requirements.

The confidence in the use of software tools is composed of two groups of activities which are shown in Figure 3:

a) Tool usage aspects

— Evaluation of the software tool usage is based on the tool's required functions and properties. The determination of the corresponding Tool Confidence Level (TCL) is based on analysis classes, Tool Impact (TI), and Tool error Detection (TD). The determination of TI and TD depends on the development process of the element developed and/or verified with the tool.

— Integration of the software tool into the user's environment according to the results of the evaluation and qualification (see 11.4.2 and 11.4.3).

EXAMPLE 2 The tool could need to be integrated with configuration management tools, authoring tools or compilers.

— Verify that the tool is working appropriately in the user environment. Check the validity of the predetermined Tool Confidence Level or qualification (11.4.2) and if required perform qualification procedures in the user environment.

EXAMPLE 3 Test of the tool performed in the user environment for representative use cases.

EXAMPLE 4 Run the tool validation test suite.

— Appropriate usage of the tool: operating the tool in the user environment for performing the development/verification tasks that this tool automates according to the defined procedure (see 11.4.3).

b) Tool qualification aspects

— Tool qualification is carried out based on given or assumed information regarding the tool usage (e.g. use cases, user requirements, TCL, ASIL).

The rigour of requirements placed upon the tool should not be biased by whether the tool pre-exists or is custom-made. Instead, the requirements depend on the role of the tool, the risks related to tool failures and the maximum ASIL of the item or element.

NOTE 2 This approach aims to avoid excessive requirements for tools with low impact developed specifically for E/E systems. It also aims to reduce any bias from the assumption that pre-existing tools do not require appropriate rigour of requirements.

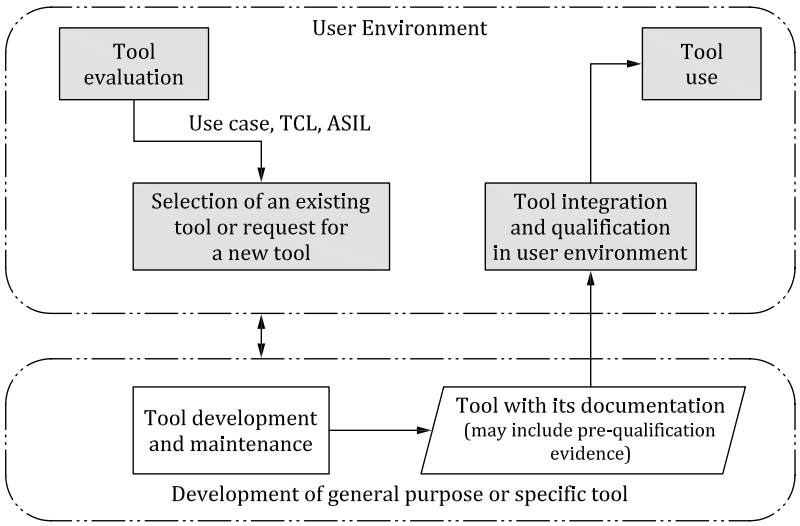


Figure 3 — Overview of Tool Confidence activities

To evaluate the confidence in prevention or detection measures, measures internal to the software tool (e.g. monitoring) as well as measures external to the software tool (e.g. guidelines, tests, reviews) implemented in the development process of the safety-related item or element are considered and can be assessed. The tool evaluation process, determination of its Tool Confidence Level (TCL) and corresponding qualification are shown in Figure 4.

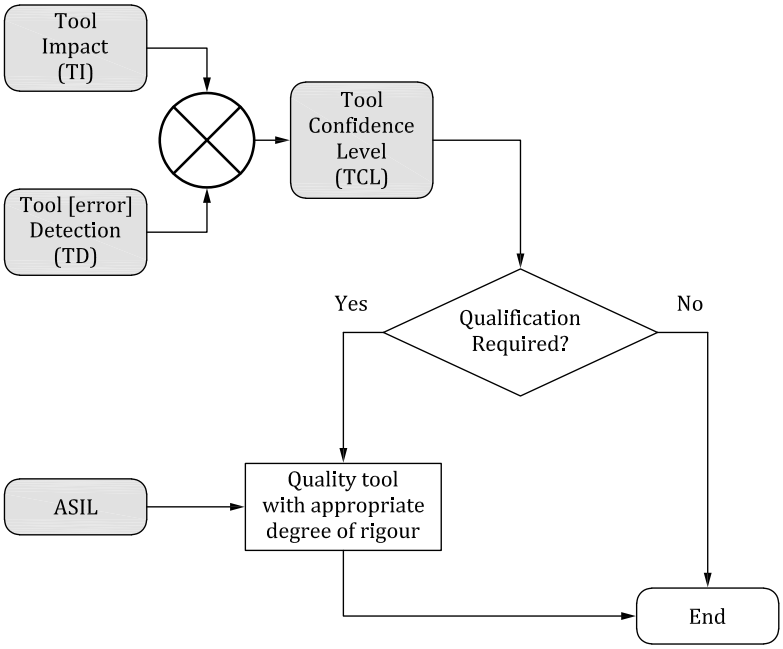


Figure 4 — Tool evaluation and qualification flow

If indicated by the Tool Confidence Level, appropriate qualification methods are applied to comply with both the Tool Confidence Level and the maximum ASIL of the safety requirements allocated to the item or element that are developed using the software tool.

11.3 Inputs to this clause

11.3.1 Prerequisites

The following information shall be available:

— safety plan in accordance with ISO 26262-2:2018, 6.5.3;

— organization-specific rules and processes for functional safety in accordance with ISO 26262-2:2018, 5.5.1; and

— applicable prerequisites of the phases of the safety lifecycle where a software tool is used.

11.3.2 Further supporting information

The following information can be considered:

— pre-determined maximum ASIL;

— user manual for the software tool (from an external source); and

— environment and constraints of the software tool (from an external source).

11.4 Requirements and recommendations

11.4.1 General requirement

If the safety lifecycle incorporates the use of a software tool for the development of a system, or its hardware or software elements, such that activities or tasks required by the ISO 26262 series of standards rely on the correct functioning of a software tool, and where the relevant outputs of that tool are not examined or verified for the applicable process step(s), such software tools shall comply with the requirements of this clause.

11.4.2 Validity of predetermined Tool Confidence Level or qualification

If the confidence level evaluation or qualification of a software tool is performed independently from the development of a particular safety-related item or element, the validity of this predetermined Tool Confidence Level or qualification shall be verified prior to the software tool being used for the development of a particular safety-related item or element.

NOTE The collection of information about the software tools, the confidence level evaluation and the qualification can be a cross-organizational activity, thus facilitating the effort for each development project.

11.4.3 Software tool compliance with its evaluation criteria or its qualification

When using a software tool, it shall be ensured that its usage, its determined environmental and functional constraints and its general operating conditions comply with its evaluation criteria or its qualification.

EXAMPLE Use of identical version and configuration settings for the use cases together with the implemented measures for the prevention or detection of malfunctions and their corresponding erroneous output, as documented in the qualification report for this software tool.

11.4.4 Planning of usage of a software tool

11.4.4.1 The usage of a software tool shall be planned, including the determination of:

a) the identification and version number of the software tool;

b) the configuration of the software tool;

EXAMPLE 1 The configuration of a compiler is defined by setting compiler switches and “#pragma” statements in a C source file.

c) the use cases of the software tool;

NOTE 1 Use cases can describe the user’s interactions with a software tool and the applied subset of the software tool’s functionality when performing activities of the safety lifecycle.

NOTE 2 Use cases can include requirements for the configuration of the software tool and the environment in which the software tool is executed.

d) the environment in which the software tool is executed;

EXAMPLE 2 Resources, infrastructure or runtime environment needed for executing the software tool, process activities preceding the activity that is performed by applying the software tool or subsequent process activities that are related to the verification of the outcomes of the software tool.

e) the maximum ASIL of all the safety requirements allocated to the item or the element that can directly be violated if the software tool is malfunctioning and producing corresponding erroneous output; and

NOTE 3 The maximum ASIL can be determined with regard to a specific development, or an assumption can be made with regard to the generic usage of the software tool. In the case of an assumed pre-determined ASIL, such an assumption is verified.

f) the methods to qualify the software tool, if required, based on the determined level of confidence and ASIL.

11.4.4.2 To ensure the proper evaluation or usage of the software tool, the following information shall be available:

a) a description of the features, functions and technical properties of the software tool;

b) the user manual or other usage guides, if applicable;

c) a description of the environment required for its operation;

d) a description of the expected behaviour of the software tool under anomalous operating conditions, if applicable;

EXAMPLE 1 Anomalous operating conditions can be prohibited combinations of compiler switches, an environment not complying with the user manual or an incorrect installation.

EXAMPLE 2 Expected behaviour under an anomalous operating condition can be a suppression of output generation, a user indication or a user report.

e) a description of known software tool malfunctions and the appropriate safeguards, avoidance or workaround measures, if applicable; and

EXAMPLE 3 Usage guidelines or workarounds addressing known malfunctions, limitation of code optimisation by compilers or the use of a limited set of building blocks for modelling.

EXAMPLE 4 Safeguards include prevention through usage constraints, detection, reporting of all known malfunctions and issues, and provision of safe alternate techniques to perform the corresponding activity.

f) the measures for the prevention or detection of malfunctions and the corresponding erroneous output of the software tool identified during the determination of the required level of confidence for this software tool.

NOTE 1 Measures for the prevention or detection of erroneous corresponding outputs can address both known and potential errors in the output of software tools.

EXAMPLE 5 Comparisons of outputs of redundant software tools, tests performed, static analyses or reviews, analyses of log files of the software tool, avoidance of functionalities with known issues.

11.4.5 Evaluation of a software tool by analysis

11.4.5.1 The description of the usage of a software tool shall contain the following information:

a) the intended purpose;

EXAMPLE 1 Simulation of a function, the generation of source code, or the test of embedded software, the tailoring of the safety-lifecycle or the simplification or automation of activities and tasks required by ISO 26262.

b) the inputs and expected outputs; and

EXAMPLE 2 Data required as input for a subsequent development activity, source code, results of a simulation, results of a test, or other work products of ISO 26262.

c) the usage procedure, environmental and functional constraints, if applicable.

EXAMPLE 3 Embedding the software tool into the development processes, the usage of shared data by different software tools and other usage conditions, process measures to prevent or detect malfunctions placed around the software tool.

11.4.5.2 The intended usage of the software tool shall be analysed and evaluated to determine:

a) the possibility that a malfunction of a particular software tool can introduce or fail to detect errors in a safety-related item or element being developed. This is expressed by the classes of Tool Impact (TI):

   — TI1 shall be selected when there is an argument that there is no such possibility;

   — TI2 shall be selected in all other cases.

b) the confidence in measures that prevent the software tool from malfunctioning and producing corresponding erroneous output, or in measures that detect that the software tool has malfunctioned and has produced corresponding erroneous output. This is expressed by the classes of Tool error Detection (TD):

   — TD1 shall be selected if there is a high degree of confidence that a malfunction and its corresponding erroneous output will be prevented or detected;

   — TD2 shall be selected if there is a medium degree of confidence that a malfunction and its corresponding erroneous output will be prevented or detected;

   — TD3 shall be selected in all other cases.

NOTE 1 Prevention or detection can be accomplished through process steps, redundancy in tasks or software tools or by rationality checks within the software tool itself.

NOTE 2 TD3 typically applies if there are no systematic measures in the development process available, and therefore malfunctions of the software tool and their corresponding erroneous outputs can only be detected randomly.

NOTE 3 If a software tool is used to verify the output from another software tool, the interdependency between those software tools is considered when evaluating the subsequent software tool and an adequate TD is selected for the software tool used subsequently. For instance, interdependency between tools can exist because of common components or shared resources.

NOTE 4 The level of detail for such a usage analysis only needs to permit the proper determination of both of the classes of TI and TD.

EXAMPLE 1 TD1 is selected for a code generator when the generated source code is verified in accordance with ISO 26262. TD3 is selected for a code generator when the generated source code is not verified.

EXAMPLE 2 Usage guidelines prevent malfunctions such as the incorrect or ambiguous interpretation of code constructs by a compiler.

EXAMPLE 3 TD2 is selected for a tool that statically verifies the absence in source code of potential for division by zero if testing is also applied for this purpose. TD3 is selected if absence of division by zero is verified by the tool alone.

11.4.5.3 If the correct selection of TI or TD is unclear or doubtful, TI and TD should be estimated conservatively.

11.4.5.4 Based on the values determined for the classes of TI and TD (in accordance with 11.4.5.2, or 11.4.5.3), the required software Tool Confidence Level shall be determined according to Table 3.

Table 3 — Determination of the Tool Confidence Level (TCL)

		Tool error detection		
		TD1	**TD2**	**TD3**
Tool impact	**TI1**	TCL1	TCL1	TCL1
	TI2	TCL1	TCL2	TCL3

11.4.6 Qualification of a software tool

11.4.6.1 For the qualification of software tools classified at TCL3, the methods listed in Table 4 shall be applied. For the qualification of software tools classified at TCL2, the methods listed in Table 5 shall be applied. A software tool classified at TCL1 needs no qualification methods.

Table 4 — Qualification of software tools classified TCL3

Methods		ASIL			
		A	B	C	D
1a	Increased confidence from use in accordance with 11.4.7	++	++	+	+
1b	Evaluation of the tool development process in accordance with 11.4.8	++	++	+	+
1c	Validation of the software tool in accordance with 11.4.9	+	+	++	++
1d	Development in accordance with a safety standard[a]	+	+	++	++
[a] No safety standard is fully applicable to the development of software tools. Instead, a relevant subset of requirements of the safety standard can be selected. EXAMPLE Development of the software tool in accordance with ISO 26262, IEC 61508, EN 50128 or RTCA DO-178C.					

Table 5 — Qualification of software tools classified TCL2

Methods		ASIL			
		A	B	C	D
1a	Increased confidence from use in accordance with 11.4.7	++	++	++	+
1b	Evaluation of the tool development process in accordance with 11.4.8	++	++	++	+
1c	Validation of the software tool in accordance with 11.4.9	+	+	+	++
1d	Development in accordance with a safety standard[a]	+	+	+	+
[a] No safety standard is fully applicable to the development of software tools. Instead, a relevant subset of requirements of the safety standard can be selected. EXAMPLE Development of the software tool in accordance with ISO 26262, IEC 61508, EN 50128 or RTCA DO-178C.					

11.4.6.2 The qualification of the software tool shall be documented including the following:

a) the unique identification and version number of the software tool;

b) the maximum Tool Confidence Level for which the software tool is classified together with a reference to its evaluation analysis;

c) for the considered use cases the pre-determined maximum ASIL, or specific ASIL, of any safety requirement which might directly be violated if the software tool is malfunctioning and produces corresponding erroneous output;

d) the configuration and environment for which the software tool is qualified;

e) the person or organization who carried out the qualification;

f) the methods applied for its qualification in accordance with 11.4.6.1;

g) the results of the measures applied to qualify the software tool; and

h) the usage constraints and malfunctions identified during the qualification, if applicable.

11.4.7 Increased confidence from use

11.4.7.1 If the method "Increased confidence from use" in accordance with Table 4 or Table 5 is applied for the qualification of a software tool, the qualification shall comply with the requirements of this sub-clause.

11.4.7.2 A software tool shall only be argued as having increased confidence from use, if evidence is provided for the following:

NOTE The requirements of the proven in use argument from Clause 14 are not applicable to this sub-clause.

a) the software tool has been used previously for the same purpose with comparable use cases, with a comparable determined operating environment and with similar functional constraints;

b) the justification for increased confidence from use is based on sufficient and adequate data;

NOTE Data can be obtained through accumulated amount of usage (e.g. duration or frequency).

c) the specification of the software tool is unchanged; and

d) the occurrence of malfunctions and corresponding erroneous outputs of the software tool acquired during previous developments are accumulated in a systematic way.

11.4.7.3 The experience from the previous usage of the software tool during given development activities shall be analysed and evaluated by considering the following information:

a) the unique identification and version number of the software tool;

b) the configuration of the software tool;

c) the details of the period of use and relevant data on its use;

EXAMPLE 1 Used features of the software tool and frequency of their use for relevant use cases of the software tool.

d) the documentation of malfunctions and corresponding erroneous outputs of the software tool with details of the conditions leading to them;

e) the list of the previous versions monitored, listing the malfunctions fixed in each relevant version; and

f) the safeguards, avoidance measures or workarounds for the known defects, or detection measures for a corresponding erroneous output, if applicable.

EXAMPLE 2 Sources for the usage report can be a log-book, the version history provided by the supplier of the software tool, published errata sheets.

11.4.7.4 The increased confidence from use argument shall only be valid for the evaluated version of the software tool.

11.4.8 Evaluation of the tool development process

11.4.8.1 If the method “Evaluation of the tool development process” in accordance with Table 4 or Table 5 is applied for the qualification of a software tool, the qualification shall comply with the requirements of this sub-clause.

11.4.8.2 The development process applied for the development of the software tool shall comply with an appropriate standard.

NOTE For open source developments, some of the standards used by those communities can also be appropriate.

11.4.8.3 The evaluation of the development process applied for the development of the software tool shall be based on an appropriate national or international standard and provide evidence that a suitable software development process has been applied.

NOTE This evaluation covers the development of an adequate and relevant subset of the features of the software tool.

EXAMPLE Using an assessment method based on Automotive SPICE®[3)], the ISO/IEC 33000 series of standards or CMMI.

11.4.9 Validation of the software tool

11.4.9.1 If the method "Validation of the software tool" according to Table 4 or Table 5 is applied for the qualification of a software tool, the qualification shall comply with the requirements of this sub-clause.

11.4.9.2 The validation of the software tool shall meet the following criteria:

a) the validation measures shall provide evidence that the software tool complies with specified requirements to its purpose as specified in the classification;

NOTE 1 The validation provides evidence that the assessed tool errors either do not occur or will be detected.

NOTE 2 The validation can be performed either by using a customized test suite developed by the user or by the tool vendor (if the test suite of the vendor includes the tool use cases of the user).

EXAMPLE 1 The standard for a programming language helps to define the requirements for validating the associated compiler.

b) the malfunctions and their corresponding erroneous outputs of the software tool occurring during validation shall be analysed together with information on their possible consequences and with measures to avoid or detect them; and

c) the reaction of the software tool to anomalous operating conditions shall be examined.

EXAMPLE 2 Foreseeable misuse, incomplete input data, incomplete update of the software tool, use of prohibited combinations of configuration settings.

11.5 Work products

11.5.1 Software tool criteria evaluation report resulting from requirements 11.4.1 to 11.4.5.

11.5.2 Software tool qualification report resulting from requirements 11.4.6 to 11.4.9.

12 Qualification of software components

12.1 Objectives

The objective of the qualification of software components is to provide evidence for their suitability for re-use in items developed in compliance with the ISO 26262 series of standards.

12.2 General

The use of qualified software components avoids re-development of existing software components with identical functionalities or properties or enables the use of general purpose commercial off-the-shelf (COTS) software.

NOTE Software components are understood to include source code, models, pre-compiled code, or compiled and linked software.

3) 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 these products.

EXAMPLE Software components addressed by this clause include:

— software libraries from third-party suppliers [commercial off-the-shelf (COTS) software];

— already existing SW components not developed according to ISO 26262;

— in-house components already in use in electronic control units.

12.3 Inputs to this clause

12.3.1 Prerequisites

The following information shall be available:

— organization-specific rules and processes for functional safety in accordance with ISO 26262-2:2018, 5.5.1; and

— requirements of the software component (from an external source).

12.3.2 Further supporting information

The following information can be considered:

— design specification of the software component (from an external source); and

— results of previous verification measures of the software component (from an external source).

12.4 Requirements and recommendations

12.4.1 General

To be able to consider a software component as qualified, the following shall be available:

a) the specification of the software component in accordance with 12.4.2.1;

b) evidence that the software component complies with its requirements in accordance with 12.4.2.2, 12.4.2.3, and 12.4.2.4;

c) evidence that the software component is suitable for its intended use in accordance with 12.4.3;

d) evidence that the software development process for the component is based on an appropriate national or international standard (e.g. ISO/IEC/IEEE 12207); and

e) a plan for the qualification of the software component.

NOTE Some re-engineering activities can be performed in order to comply with this sub-clause in the case of previously developed software components.

12.4.2 Specification of software component qualification

12.4.2.1 The specification of the software component qualification shall include:

a) the unique identification of the software component;

b) the maximum target ASIL of any safety requirement which might be violated if the software component performs incorrectly;

c) the activities that shall be carried out to qualify the software component;

d) the requirements of the software component;

EXAMPLE Requirements can include:

— functional requirements;

— already known safety requirements;

— accuracy of algorithm or numerical accuracy, where accuracy of algorithm considers procedural errors, which only provide approximate solutions and numerical accuracy considers rounding errors, resulting from computational inaccuracy, and truncation errors caused by the approximate representation of functions in the electronic control unit;

— behaviour in the case of failure;

— response time;

— resource usage;

— requirements on the runtime environment; and

— behaviour in an overload situation (robustness).

e) the requirements of the intended use of the software component;

f) the description of the configuration;

NOTE For software components that contain more than one software unit, the description of the configuration includes the unique identification and configuration of each software unit.

g) the description of required and provided interfaces and shared resources, if any;

h) the application manual, where appropriate;

i) the instructions for a correct software component integration;

NOTE This description includes configuration parameters of the development tools required to properly integrate and use the software component.

j) the reactions of the implemented functions under anomalous operating conditions; and

EXAMPLE Reaction to re-entrant calling of a non-re-entrant software function.

k) a description of known anomalies with corresponding workaround measures.

12.4.2.2 To provide evidence that a software component complies with its requirements the verification of this software component shall:

a) show a requirement coverage in accordance with ISO 26262-6:2018, Clause 9;

NOTE This verification is primarily based on requirements-based tests. The results of requirements-based tests of the software component executed during its development or during previous integration tests can be used.

EXAMPLE Application of a dedicated qualification test suite, analysis of all the tests already executed during the implementation and any integration of the software component.

b) cover both normal operating conditions and behaviour in the case of failure; and

c) display no known errors that may lead to a violation of safety requirements allocated to this software component.

12.4.2.3 This requirement applies to ASIL D, in accordance with 4.4: the structural coverage shall be measured in accordance with ISO 26262-6:2018, Clause 9, to evaluate the completeness of the test cases.

12.4.2.4 The verification in accordance with 12.4.2.2, shall only be valid for an unchanged implementation of the software component.

12.4.2.5 The qualification of a software component shall be documented including the following information:

a) the unique identification of the software component;

b) the unique configuration of the software component;

c) the person or organization who carried out the qualification;

d) the environment used for qualification;

e) the results of the verification measures applied to qualify the software component; and

f) the maximum ASIL of the safety requirements allocated to the software component .

12.4.3 Verification of qualification of a software component

The results of qualification of a software component together with the validity of these results regarding the intended use of the software component shall be verified in accordance with Clause 9.

12.5 Work products

12.5.1 Software component documentation resulting from requirement 12.4.2.1.

12.5.2 Software component qualification report resulting from requirements 12.4.2.2 to 12.4.2.5.

12.5.3 Software component qualification verification report resulting from requirement 12.4.3.

13 Evaluation of hardware elements

13.1 Objectives

The objective of this clause is to ensure that the functional behaviour is adequate to meet the allocated safety requirements and therefore the risk of a violation of a safety goal or of a safety requirement, due to a systematic fault of the hardware element, is sufficiently low. Suitability for use based on random fault management is established by the integrator of the evaluated hardware element, at the next highest level of design integration.

NOTE 1 Meeting the requirements of the safety concept includes providing information on failure modes and failure mode distribution of the hardware element, suitable to conduct hardware failure analysis.

NOTE 2 It is not the objective of this clause to ensure the suitability of the hardware element concerning its robustness in its intended environmental conditions or its reliability. This is addressed for every hardware element within ISO 26262-5:2018, Clause 10.

In this clause, the use of the term “hardware element” refers either to COTS hardware components or parts, or to custom hardware components or parts, that:

— are not originally developed or designed according to the ISO 26262 series of standards; and

— are considered to be safety-related within the context of the ISO 26262 compliant item or element into which they are to be integrated.

More precisely, the evaluation of hardware elements is an alternative means of compliance with ISO 26262-5. The hardware elements eligible for evaluation can either be specific to an application

or standard elements. Such elements are often developed for use across many industries either for automotive application or non-automotive application.

13.2 General

The following goals are achieved by the evaluation of hardware elements:

a) provide evidence that the hardware possesses an adequate functional performance and therefore is suitable to provide its intended function as required by the hardware design;

b) identification of new or confirmation of known failure modes and models (including the quantification of their distribution) by using appropriate tests (such as over limit test, accelerated test, etc.) or analyses;

c) identification of new or confirmation of known limits of use for hardware elements; and

d) provide an argument that the risk of a violation of a safety goal or the risk of a violation of a safety requirement due to systematic faults is sufficiently low.

The evaluation of hardware elements is done in the context of a specific application.

Within the evaluation of hardware elements the hardware element under consideration is classified either as class I, class II or class III element depending on its properties. These classes reflect the difficulty of the verification of the safety-related functionality and the role of the hardware element within the safety concept.

Depending on its class, different requirements to evaluate the hardware element are given. As a first step the relevant requirements for the hardware element are specified and its safety related failure modes are identified.

For the evaluation of class I elements it is sufficient to test the hardware element into which the evaluated hardware elements are integrated according to ISO 26262-5:2018, Clause 10.

The evaluation of class II elements can be done with a combination of tests and analyses.

For the evaluation of class III elements, in addition to the evaluation activities necessary for a class II element, an argument is added showing that the risk of a safety goal violation or the risk of a safety requirement violation is sufficiently low.

13.3 Inputs to this clause

13.3.1 Prerequisites

The following information shall be available:

— organization-specific rules and processes for functional safety in accordance with ISO 26262-2:2018, 5.5.1;

— the safety requirements related to the considered hardware element;

— criteria for design verification (analysis and tests) in accordance with ISO 26262-5:2018, Clause 6; and

— the manufacturer's hardware element specification, or, if unavailable, the assumptions on hardware element specification (from an external source).

13.3.2 Further supporting information

The following information can be considered:

— further supporting information for the phases of the safety lifecycle where the evaluation of hardware elements is applied.

13.4 Requirements and recommendations

13.4.1 General

13.4.1.1 Classification of the evaluated hardware element

The hardware element shall be classified as one of the following classes:

a) Class I if:

— the element has at the maximum a few states which can be fully characterized, tested and analysed from a safety perspective;

— safety related failure modes can be identified and evaluated without knowledge about details of the implementation and the production process of the element; and

— the element has no internal safety mechanisms which are relevant for the safety concept to control or detect internal failures.

NOTE This does not include safety mechanisms that monitor properties outside of the element.

EXAMPLE Resistor, capacitor, transistor, diode, quartz, resonator.

b) Class II if:

— the element has e.g. few operating modes, small value ranges, few parameters and can be analysed from safety perspective without knowing implementation details;

— available documentation allows valid assumptions supporting evaluation of systematic faults by testing and analysis without knowledge about details of the implementation and the production process of the element; and

EXAMPLE Datasheets, user manuals, application notes.

— the element has no internal safety mechanisms which are relevant for the safety concept to control or detect internal failures.

NOTE This does not include safety mechanisms that monitor properties outside of the element.

EXAMPLE Fuel pressure sensor, temperature sensor, stand-alone Analog Digital Converter (ADC) without internal safety mechanisms relevant for the safety concept.

c) Class III if:

— the element has e.g. many operating modes, wide value ranges or many parameters which are impossible to analyse without knowing implementation details,

— sources for systematic faults can only be understood and analysed by knowledge about detailed implementation, the development process and/or the production process, or

— the element has internal safety mechanisms which are relevant for the safety concept to control or detect internal failures.

EXAMPLE Microprocessor, microcontroller, Digital Signal Processor (DSP).

13.4.1.2 The requirements for the hardware element resulting from the allocated safety requirements and the safety concept shall be specified.

NOTE For class I elements this usually coincides with the specification of the hardware element, e.g. nominal value and tolerances for a resistor.

13.4.1.3 The failure modes or faults of the hardware element and their distribution concerning random hardware faults shall be identified.

13.4.1.4 The safety related failure modes or faults of the hardware element shall be identified. The analysis shall provide evidence that the requirements resulting from ISO 26262-5:2018, 7.4.3, Clauses 8 and 9 are met.

13.4.2 Evaluation of class I hardware elements

Due to the simplicity of the functionality of a class I element, it does not need to be evaluated by itself; the hardware element into which it is integrated shall be developed in compliance with ISO 26262.

13.4.3 Evaluation of class II hardware elements

13.4.3.1 Methods for evaluation

The evaluation of the class II hardware element shall be carried out using an appropriate selection of analysis and testing.

13.4.3.2 Evaluation plan

An evaluation plan shall be developed and shall describe:

a) a unique identification and version of the hardware element;

b) a specification of the environment in which the hardware element is intended to be used;

c) the evaluation strategy and the rationale;

NOTE The strategy includes: analysis, necessary tests and step by step description.

d) the necessary tools and equipment according to the strategy;

e) the party responsible for carrying out the evaluation; and

f) the pass and fail criteria for the evaluation of a hardware element.

13.4.3.3 Evaluation argument

13.4.3.3.1 A comprehensive argument that the functional performance of the hardware element complies with its specification and it is adequate for its intended use, according to the hardware design, shall be made available.

NOTE The required performances encompass behaviour when it is subjected to the established normal environmental conditions and to the environmental conditions in combination with an assumed failure initiating event.

13.4.3.3.2 The comprehensive argument of 13.4.3.3.1 shall be based on a combination of the following types of information:

a) analytical methods and assumptions used;

b) data from operational experience; and

c) existing testing results.

13.4.3.3.3 A rationale for each assumption, including extrapolations, shall be given.

13.4.3.4 Evaluation by analyses

13.4.3.4.1 The result of the analysis shall be provided in a form that is comprehensive and can be verified by persons who are qualified in the relevant engineering or scientific disciplines.

NOTE Analytical methods that can be used include design verification methods, e.g. extrapolations, mathematical models, damage analysis or similar methods, and process gap analysis in order to show sufficient evidence for systematic failure avoidance will be available.

13.4.3.4.2 The analysis shall consider all the environmental conditions to which the hardware element is exposed, the limits of these conditions and other additional stresses related to operation (e.g. expected switch cycles, charging and discharging, long turn-off times).

13.4.3.5 Evaluation by testing

13.4.3.5.1 A test plan shall be developed which contains the following information:

a) a description of the functions of the hardware element;

b) allocated safety requirements;

c) the specification and sequence of tests to be conducted;

d) the traceability between tests and safety requirements;

e) the requirements for assembly and connections;

f) the operating and environmental conditions to be simulated;

g) number of elements tested;

h) pass and fail criteria;

i) environmental parameters to be measured; and

j) requirements for the testing equipment, including accuracy.

13.4.3.5.2 The test to verify robustness of the hardware element under evaluation against external stresses shall be done in accordance with ISO 26262-5:2018, 10.4.6.

EXAMPLE This specification can be based on the ISO 16750 series of standards or equivalent company standards.

13.4.3.5.3 The test shall be conducted as planned and the resulting test data shall be made available.

13.4.3.5.4 The integration into the ISO 26262 compliant element shall comply with ISO 26262-5:2018, Clause 10 or ISO 26262-4:2018, Clause 7.

13.4.3.6 Evaluation report

13.4.3.6.1 The evaluation report shall state whether the hardware element has passed or failed the evaluation, based on the performed analyses and testing, with respect to the safety requirements specified and allocated to it, including its operating range and conditions.

NOTE The evaluation report can consist of a set of documents that includes reports on findings and notes on interpretation.

13.4.3.6.2 The evaluation report shall be verified in accordance with Clause 9.

13.4.4 Evaluation of class III hardware elements

13.4.4.1 Class III hardware elements should be developed in compliance with ISO 26262.

NOTE This means that the "evaluation of class III elements" is not the preferred approach and therefore the next version of the hardware element is planned to be developed in compliance with ISO 26262.

13.4.4.2 For the evaluation of the class III hardware elements the requirements stated in 13.4.3 shall be met.

13.4.4.3 Additional measures shall be provided to argue that the risk of a safety goal violation or the risk of a safety requirement violation due to systematic faults is sufficiently low.

NOTE 1 Depending on the combination of arguments provided, the result of the hardware evaluation shows that using the class III element in the context of the given application is safe. However the argument is not valid for all applications.

NOTE 2 Measures can include but are not limited to:

a) verifiability of the safety related functionality;

b) field experience/"well-trusted component";

NOTE Field experience can be used as a partial supporting argument for hardware evaluation. For a full proven-in-use argument, ISO 26262-8:2018, Clause 14 is followed instead of this clause.

c) supervision by an independent diverse element with the capability to detect the safety related failure modes; and

NOTE A Dependent Failure Analysis compliant with ISO 26262-9:2018, Clause 7, shows the independence.

d) development compliant with a different safety standard with a comparable integrity level.

13.5 Work products

13.5.1 Hardware element evaluation plan resulting from requirement 13.4.3.2.

13.5.2 Hardware element test plan if applicable, resulting from requirement 13.4.3.5.1.

13.5.3 Hardware element evaluation report for hardware elements resulting from requirements 13.4.1.1, 13.4.3.6 and 13.4.4.3, if applicable.

14 Proven in use argument

14.1 Objectives

The objective of this clause is to provide guidance for a proven in use argument. A proven in use argument is an alternate means of compliance with the ISO 26262 series of standards that may be used in the case of reuse of existing items or elements when field data is available.

14.2 General

A proven in use argument can be applied to any type of product whose definition and conditions of use are identical to or have a very high degree of commonality with a product that is already released and in operation. It can also be applied to any work product related to such products.

NOTE 1 Proven in use argument is not inter-changeability: one product, with alternate design or implementation, that is intended to replace a proven in use product cannot be considered to be proven in use because it fulfils the original functional requirements, unless this product meets the criteria specified in this clause.

An item or an element, such as system, function, hardware or whole software product, can be a candidate for a proven in use argument.

A candidate can also refer to a work product such as a technical safety concept.

The motivation for using the argument for proven in use includes:

a) an automotive application in commercial use intended to be partly or completely carried over to another target, or

b) an Electronic Control Unit (ECU) in operation intended to implement an additional function, or

c) a candidate being in the field prior to the release of the ISO 26262 series of standards, or

d) a candidate being used in other safety-related industries, or

e) a candidate being a widely used COTS product not necessarily intended for automotive applications.

The proven in use argument is substantiated by appropriate documentation on the candidate, configuration management and change management records, and field data regarding safety-related incidents.

Once a candidate has been defined (see 14.4.3) with the expected proven in use credit (see 14.4.2), two important criteria need to be considered when preparing a proven in use argument:

— the relevance of field data during the previous evaluation period of the candidate (see 14.4.5); and

— the changes, if any, that could have impacted the candidate since its previous evaluation period (see 14.4.4).

NOTE 2 With regard to the relevance of field data, the proven in use argument is intended to address systematic and random failures of the candidate; it does not address failures related to ageing of the candidate.

Using proven in use items or elements does not exempt those items or elements from the following project-dependent safety management activities:

— the proven in use credit is described in the safety plan; and

— the data and work products resulting from the proven in use argument are part of the safety case and subject to confirmation measures.

14.3 Inputs to this clause

14.3.1 Prerequisites

The following information shall be available:

— regarding the intended use of a candidate:

  — candidate specification;

  — applicable safety goal(s) or safety requirement(s) with corresponding ASIL(s); and

  - foreseeable operational situation and intended operating modes and interfaces;
- regarding the previous use of a candidate:
  - field data from the service period (from an external source).

14.3.2 Further supporting information

The following information can be considered regarding the previous use of a candidate:

- safety case in accordance with ISO 26262-2:2018, 6.5.4.

NOTE For a candidate not developed in accordance with the ISO 26262 series of standards (e.g. COTS products, candidates developed under a safety standard other than ISO 26262, such as IEC 61508 or RTCA DO-178C), some work products of the safety case may not be available, in which case they are substituted by available data resulting from the development of the candidate.

14.4 Requirements and recommendations

14.4.1 General

The following sub-clauses refer to the ASILs applicable to the future use of the candidate.

14.4.2 Proven in use credit

14.4.2.1 A proven in use credit shall be used only when the candidate complies with 14.4.2 to 14.4.5.

14.4.2.2 The proven in use credit resulting from a proven in use argument shall be planned in accordance with ISO 26262-2:2018, 6.4.5.

14.4.2.3 The proven in use credit shall be limited to the safety lifecycle sub-phases and activities covered by the proven in use argument of the candidate.

14.4.2.4 Integration measures of proven in use elements in an item or element shall be carried out at the appropriate level in accordance with ISO 26262-4:2018, Clause 8.

EXAMPLE The hardware of an ECU has a satisfactory field history and is intended to be 100 % carried over to a new application. The proven in use credit can be applied to the sub-phases and activities of development of this hardware element. Similarly, if the software is a 100 % carryover with a satisfactory service history, then the proven in use credit can also be applied to the software sub-phases and activities.

14.4.2.5 Safety validation of an item which embeds proven in use elements shall be carried out in accordance with ISO 26262-4:2018, Clause 9.

14.4.2.6 The confirmation measures of an item that embeds proven in use elements shall consider the proven in use arguments and related data in accordance with ISO 26262-2:2018, 6.4.9 and 6.4.10.

14.4.2.7 Any modification to a proven in use item or element shall comply with 14.4.4 for the corresponding proven in use credit to be maintained.

NOTE This clause applies to any type of modification including those initiated as a result of a safety-related incident.

14.4.3 Minimum information on candidate

A description of the candidate and its previous use shall be available, and includes:

a) the identification and traceability of the candidate with a catalogue of internal elements or components, if any;

b) the corresponding fit, form and function requirements that describe, if applicable, interface and environmental, physical and dimensional, functional and performance characteristics of the candidate; and

c) the safety requirements of the candidate in the previous use and the corresponding ASILs, if available.

14.4.4 Analysis of modifications to the candidate

14.4.4.1 Proven in use candidates

Modifications to candidates and their environment shall be identified in accordance with 14.4.4.2 to 14.4.4.3.

NOTE 1 Modifications to candidates address design changes and implementation changes. Design changes can result from modification of requirements, functional enhancements or performance enhancement. Implementation changes do not affect specification or performance of the candidate but only its implementation features. Implementation changes can result from software corrections or use of new development or production tools.

NOTE 2 Changes to configuration data or calibration data are considered as modifications to the candidate when they impact its behaviour with regard to the violation of the safety goals.

NOTE 3 Changes to the environment of a candidate can result from use of this candidate in a new type of application with different safety goals or requirements, its installation in a new target environment (e.g. variant of vehicle, range of environmental conditions) or the upgrading of the components interacting with it or located in its vicinity.

14.4.4.2 Modifications to items introduced for a future application

Modifications to items and their environment introduced for the purpose of a future application shall comply with ISO 26262-2:2018, 6.4.3.

14.4.4.3 Modifications to elements introduced for a future application

Modifications to elements and their environment introduced for the purpose of a future application within a different item shall comply with ISO 26262-2:2018, 6.4.4.

14.4.4.4 Modifications to candidate independent of future application

Modifications to a candidate introduced after its evaluation period, independent of future applications, shall provide evidence that the proven in use status remains valid.

14.4.5 Analysis of field data

14.4.5.1 Configuration management and change management

Evidence shall be provided that the candidate has been kept under configuration management and change management during and after its evaluation period so that the current status of the candidate can be established.

14.4.5.2 Target values for proven in use

NOTE When any ASIL is not yet assigned to the candidate, ASIL D target is selected conservatively.

14.4.5.2.1 The rationale for the calculation of the evaluation period of the candidate shall be available.

14.4.5.2.2 The evaluation period of the candidate shall result from the addition of the observation period of all the specimens taken in reference in accordance with 14.4.5.2.3.

14.4.5.2.3 The observation period of each specimen with the same specification and realization as the candidate and running in a vehicle shall exceed the average yearly vehicle operating time before being considered in the analysis of the evaluation period of the candidate.

14.4.5.2.4 For a proven in use status to be obtained by the candidate, its evaluation period shall demonstrate compliance with each safety goal that can be violated by the candidate in accordance with Table 6 with a single-sided lower confidence level of 70 % (using a chi-square distribution).

NOTE 1 For the purpose of the proven in use argument, an observable incident means a failure that is reported to the manufacturer and caused by the candidate with the potential to lead to the violation of a safety goal.

Table 6 — Limits for observable incident rate

ASIL	Observable incident rate
D	$<10^{-9}$/h
C	$<10^{-8}$/h
B	$<10^{-8}$/h
A	$<10^{-7}$/h

NOTE 2 The character and rate of observable incidents are interpreted when analysing the potential violation of the safety goals in the field.

NOTE 3 Table 7 gives an example of the required minimum service period without observable incident which is necessary to achieve 70 % confidence.

Table 7 — Targets for minimum evaluation period of candidate

ASIL	Minimum evaluation period without observable incident
D	$1{,}2 \times 10^9$ h
C	$1{,}2 \times 10^8$ h
B	$1{,}2 \times 10^8$ h
A	$1{,}2 \times 10^7$ h

NOTE 4 If observable incidents are found in the collected data of the specimens, the necessary minimum evaluation period, $t_{service}$, can be adjusted as follows:

$$t_{service} = t_{MTTF} \times \frac{\left(\chi_{CL;2f+2}\right)^2}{2}$$

where

CL is the confidence level as an absolute value (e.g. 0,7 for 70 %);

t_{MTTF} is the mean time to failure (1/failure rate);

f is the number of safety-related incidents;

$\left(\chi_{\alpha,\nu}\right)^2$ is the chi-squared distribution with error probability α and ν degrees of freedom.

14.4.5.2.5 The application of the proven in use credit may be anticipated provisionally, before a proven in use status is obtained (in accordance with 14.4.5.2.4). In this case, the evaluation period of the candidate shall demonstrate compliance with each safety goal that can be violated by the candidate in accordance with Table 8 with a single sided lower confidence level of 70 % (using a chi-square distribution).

Table 8 — Limits for observable incident rate (interim period)

ASIL	Observable incident rate
D	$<3 \times 10^{-9}$/h
C	$<3 \times 10^{-8}$/h
B	$<3 \times 10^{-8}$/h
A	$<3 \times 10^{-7}$/h

14.4.5.2.6 In the case of any observed incident in the field during the interim period described in 14.4.5.2.5, the following shall be complied with:

— to stop using Table 8 for the observable incident rate and to use Table 6 for the candidate, or alternatively

— to provide evidence that the root cause of the observed incident is fully identified and eliminated in accordance with the ISO 26262 series of standards, and to keep on counting the cumulated hours for the candidate, to reset the counter of cumulated hours for this specific root cause and to record this evidence in the safety case.

14.4.5.2.7 In the case of a candidate with a non-constant failure rate, additional measures shall be applied for the proven in use argument, for instance in the case of damage resulting from fatigue.

NOTE Those measures apply to candidates with failure rates significantly dependent on factors such as wear, ageing or operating hours regarding the lifetime of the item. They can include dedicated endurance tests, or a longer observation period.

14.4.5.3 Field problems

The problem reporting system shall ensure that any observed incident with potential safety impact caused by the candidate in the field, is recorded and retrievable during the period of operation of the candidate (see ISO 26262-2:2018, 7.4.2.3).

14.5 Work products

14.5.1 Description of candidate for proven in use argument resulting from requirement 14.4.3.

14.5.2 Proven in use analysis reports resulting from requirements 14.4.4 to 14.4.5.

15 Interfacing an application that is out of scope of ISO 26262

15.1 Objectives

This clause applies to T&B, where the objective is to achieve confidence that an application that is out of scope of ISO 26262 is not able to violate the safety goals of the base vehicle or item that has been developed in accordance with the ISO 26262 series of standards.

15.2 General

The application of this clause is intended for commercial vehicle business models where a company assembles or integrates a complete vehicle that is not in scope of ISO 26262 but to which another standard applies. The relationship between the application and item according to ISO 26262 is depicted in Figure 5.

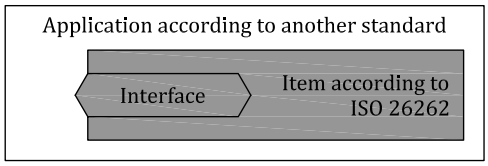


Figure 5 — Item developed according to ISO 26262 used in scope of another standard

EXAMPLE 1 A body builder, as an integrator, assembles a complete vehicle by integrating a base vehicle developed according to the ISO 26262 series of standards with body builder equipment developed according to the Machinery Directive.

EXAMPLE 2 A manufacturer of agricultural equipment integrates a brake system developed according to the ISO 26262 series of standards into agricultural equipment developed according to standards for machinery for agriculture and forestry.

15.3 Inputs to this clause

15.3.1 Prerequisites

The following information shall be available:

— item definition in accordance with ISO 26262-3:2018, 5.5.1

15.3.2 Further supporting information

None.

15.4 Requirements and recommendations

15.4.1 The requirements in 15.4 shall be applied to T&B.

15.4.2 The base vehicle manufacturer or supplier of an item or element shall communicate information to the integrator identifying the modifiable systems and components and the permitted system safety limits/requirements of the modifications.

15.4.3 The base vehicle manufacturer or supplier of an item shall communicate the safety measures required to be applied by the integrator.

NOTE 1 It is assumed that the integrator has the necessary capability to realize the safety measures.

EXAMPLE 1 Criteria for the capability of an integrator can be:

— compliance with other safety standards,

— an appropriate safety culture, and

— an established quality management system.

NOTE 2 The base vehicle manufacturer or supplier of an item or element makes assumptions about intended integrator use cases together with the safety requirements. For exceptions, the integrator contacts the base vehicle manufacturer or supplier of the item or element for safety requirements.

EXAMPLE 2 A body builder contacts a base vehicle manufacturer to request PTO activation during driving. The body builder uses ISO 13849 and both agree on an ASIL to ISO 13849. The base vehicle manufacturer communicates the safety requirements (with ASIL) regarding the PTO request, the body builder complies with these requirements (with agreed Performance Level). The base vehicle manufacturer enables the requested PTO function for the body builder.

15.5 Work products

15.5.1 Base Vehicle Manufacturer or Supplier guideline resulting from requirements 15.4.2 and 15.4.3.

16 Integration of safety-related systems not developed according to ISO 26262

16.1 Objectives

This clause applies to T&B, where the objective is to achieve confidence that a system or component that is not developed according the ISO 26262 series of standards satisfies the required level of functional safety needed for the integration into an item developed according to the ISO 26262 series of standards.

16.2 General

The application of this clause is intended for commercial vehicle business models where a company which follows ISO 26262 integrates a system or component which is not developed according to the ISO 26262 series of standards, but which has been developed according to another standard. The relationship between the application and item according to the ISO 26262 series of standards is depicted in Figure 6.

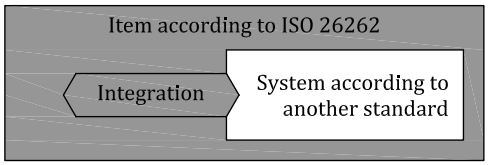


Figure 6 — Integration of a system developed according to another standard

NOTE 1 Since this business model can demand higher effort and development costs for the integrator due to additional safety activities, a conventional ISO 26262 development is favoured.

NOTE 2 A business model for commercial vehicles could be series production with low quantities.

NOTE 3 Another standard could be the Machinery Directive including IEC 61508, ISO 13849 and ISO 25119. Company specific processes could also be used for the integration.

16.3 Inputs to this clause

16.3.1 Prerequisites

The following information shall be available:

— item definition in accordance with ISO 26262-3:2018, 5.5.1.

NOTE 1 The Item definition relates to the system or array of systems on the integrator side, that includes the system or component not developed according to ISO 26262.

NOTE 2 An integrator of such systems or components can be the base vehicle manufacturer.

16.3.2 Further supporting information

None.

16.4 Requirements and recommendations

16.4.1 The requirements in 16.4 shall be applied to T&B.

16.4.2 A rationale shall be given in the integrator safety case that justifies the application of this clause.

EXAMPLE The supplier follows the safety standard ISO 13849.

16.4.3 The integrator shall define the criteria to argue that the safety-related system that has been developed to another safety standard meets the required level of functional safety.

EXAMPLE 1 A mapping between ASIL and PL (Performance Level as used in ISO 13849).

NOTE The criteria address the design process, the product design, qualification measures and approval process.

EXAMPLE 2 Comparison of requirements regarding applied methods and requested failure rates of different safety standards.

16.4.4 The integrator and supplier shall agree on the relevant set of measures to verify that the criteria are met.

EXAMPLE A set of measures can be:

— availability of the specification for the system to be integrated;

— evidence that the system to be integrated complies with its requirements by test report;

— structured design analysis for systematic design faults by FMEA, FTA, application of established design pattern/configurations;

— evidence that the system to be integrated is suitable for its intended use;

— evidence that the product release for the component is based on an adequate approval process by PPAP (Production Part Approval Process);

— design verification/validation testing by highly accelerated life testing, environmental testing, testing beyond specification limits, robustness testing; and

— analysis of field data.

16.5 Work products

16.5.1 Safety rationale resulting from requirements 16.4.2 to 16.4.4.

Annex A
(informative)

Overview of and workflow of supporting processes

Table A.1 provides an overview on objectives, prerequisites and work products of the supporting processes.

Table A.1 — Overview of supporting processes

Clause	Objectives	Prerequisites	Work products
5 Interfaces within distributed developments	The objectives of this Clause are: a) to define the interactions and dependencies between customers and suppliers for development activities; b) to describe the allocation of responsibilities; and c) to identify the work products to be exchanged for distributed developments of an item and its elements.	See applicable prerequisites of the relevant phases of the safety lifecycle for which the distributed development is planned and carried out.	5.5.1 Supplier selection report resulting from requirements 5.4.2.1 and 5.4.2.2. 5.5.2 Development interface agreement (DIA) resulting from requirements 5.4.3, 5.4.5.1 and 5.4.5.2. 5.5.3 Supplier's safety plan resulting from requirements 5.4.3 and 5.4.4. 5.5.4 Functional safety assessment report resulting from requirements 5.4.5.3 and 5.4.5.4. 5.5.5 Supply agreement resulting from requirements 5.4.6.1 to 5.4.6.4.
6 Specification and management of safety requirements	The objectives of this Clause are: a) to ensure the correct specification of safety requirements with respect to their attributes and characteristics; and b) to ensure consistent management of safety requirements throughout the entire safety lifecycle.	Organization-specific rules and processes for functional safety in accordance with ISO 26262-2:2018, 5.5.1. Applicable prerequisites of the relevant phases of the safety lifecycle in which safety requirements are specified or managed.	None
7 Configuration management	The objectives of this Clause are: a) to ensure that the work products, items, elements and the principles and general conditions of their creation, can be uniquely identified and reproduced in a controlled manner at any time; and b) to ensure that the relations and differences between earlier and current versions can be traced.	Safety plan in accordance with ISO 26262-2:2018, 6.5.3. Organization-specific rules and processes for functional safety in accordance with ISO 26262-2:2018, 5.5.1 Applicable prerequisites of the relevant phases of the safety lifecycle where configuration management is planned or managed.	7.5.1 Configuration management plan resulting from requirements 7.4.1 to 7.4.5.

Table A.1 *(continued)*

Clause	Objectives	Prerequisites	Work products
8 Change management	The objective of change management is to analyse and control changes to safety-related work products, items and elements throughout the safety lifecycle.	Configuration management plan in accordance with 7.5.1. Safety plan in accordance with ISO 26262-2:2018, 6.5.3. Organization-specific rules and processes for functional safety in accordance with ISO 26262-2:2018, 5.5.1.	8.5.1 Change management plan resulting from requirements 8.4.1. 8.5.2 Change request resulting from requirements 8.4.2. 8.5.3 Impact analysis and change request plan resulting from requirements 8.4.3 and 8.4.4. 8.5.4 Change report resulting from requirement 8.4.5.
9 Verification	The objective of verification is to ensure that the work products comply with their requirements.	Organization-specific rules and processes for functional safety in accordance with ISO 26262-2:2018, 5.5.1. Applicable prerequisites of the relevant phases of the safety lifecycle in which verification is planned or carried out. 	9.5.1 Verification plan resulting from requirements 9.4.1.1 and 9.4.1.2. 9.5.2 Verification specification resulting from requirements 9.4.2.1 to 9.4.2.4. 9.5.3 Verification report resulting from requirements 9.4.3.1 to 9.4.3.4.
10 Documentation management	The objective is to develop a documentation management strategy for the entire safety lifecycle in order to facilitate an effective and repeatable documentation management process.	Organization-specific rules and processes for functional safety in accordance with ISO 26262-2:2018, 5.5.1. Safety plan in accordance with ISO 26262-2:2018, 6.5.3.	10.5.1 Documentation management plan resulting from requirement 10.4.1 and 10.4.2. 10.5.2 Documentation guideline requirements resulting from requirements 10.4.3 to 10.4.6.
11 Confidence in the use of software tools	The objectives of this Clause are: a) to provide criteria to determine the required level of confidence in a software tool when applicable; and b) to provide means for the qualification of the software tool when applicable, in order to create evidence that the software tool is suitable to be used to support the activities or tasks required by the ISO 26262 series of standards (i.e. the user can rely on the correct functioning of a software tool for those activities or tasks required by the ISO 26262 series of standards).	Safety plan in accordance with ISO 26262-2:2018, 6.5.3. Organization-specific rules and processes for functional safety in accordance with ISO 26262-2:2018, 5.5.1. Applicable prerequisites of the phases of the safety lifecycle where a software tool is used.	11.5.1 Software tool criteria evaluation report resulting from requirements 11.4.1 to 11.4.5. 11.5.2 Software tool qualification report resulting from requirements 11.4.6 to 11.4.9.

Table A.1 *(continued)*

Clause	Objectives	Prerequisites	Work products
12 Qualification of software components	The objective of the qualification of software components is to provide evidence for their suitability for re-use in items developed in compliance with the ISO 26262 series of standards.	Organization-specific rules and processes for functional safety in accordance with ISO 26262-2:2018, 5.5.1 Requirements of the software component.	12.5.1 Software component documentation resulting from requirement 12.4.2.1. 12.5.2 Software component qualification report resulting from requirement 12.4.2.2 to 12.4.2.5. 12.5.3 Software component qualification verification report resulting from requirement 12.4.3.
13 Evaluation of hardware elements	The objective of this Clause is to ensure that the functional behaviour is adequate to meet the allocated safety requirements and therefore the risk of a violation of a safety goal or of a safety requirement due to a systematic fault of the hardware element is sufficiently low. Suitability for use based on random fault management is established by the integrator of the evaluated hardware element, at the next highest level of design integration. In this Clause, the use of the term "hardware element" refers either to COTS hardware components or parts, or to custom hardware components or parts, that are not originally developed or designed according to the ISO 26262 series of standard and are considered to be safety-related within the context of the ISO 26262 compliant item or element in which they are to be integrated. More precisely the evaluation of hardware elements is an alternative means of compliance with ISO 26262-5. The hardware elements eligible for evaluation can either be specific to an application or standard elements. Such elements are often developed for use across many industries either for automotive application or non-automotive application.	Organization-specific rules and processes for functional safety in accordance with ISO 26262-2:2018, 5.5.1 The safety requirements related to the considered hardware element. Criteria for design verification (analysis and tests) in accordance with ISO 26262-5:2018, Clause 6. The manufacturer's hardware element specification, or, if unavailable, the assumptions on hardware element specification.	13.5.1 Hardware element evaluation plan resulting from requirement 13.4.3.2. 13.5.2 Hardware element test plan if applicable, resulting from requirement 13.4.3.5.1. 13.5.3 Hardware element evaluation report for hardware elements resulting from requirement 13.4.1.1, 13.4.3.6 and 13.4.4.3, if applicable.

Table A.1 *(continued)*

Clause	Objectives	Prerequisites	Work products
14 Proven in use argument	The objective of this Clause is to provide guidance for a proven in use argument. A proven in use argument is an alternate means of compliance with the ISO 26262 series of standards that may be used in the case of reuse of existing items or elements when field data is available.	Regarding the intended use of a candidate: — candidate specification; — applicable safety goal(s) or safety requirement(s) with corresponding ASIL(s); — foreseeable operational situation and intended operating modes and interfaces. Regarding the previous use of a candidate: — field data from service period.	14.5.1 Description of candidate for proven in use argument resulting from requirement 14.4.3. 14.5.2 Proven in use analysis reports resulting from requirements 14.4.4 to 14.4.5
15 Interfacing an application that is out of scope of ISO 26262	This Clause applies to T&B, where the objective is to achieve confidence that an application that is out of scope of ISO 26262 is not able to violate the safety goals of the base vehicle or item that has been developed in accordance with the ISO 26262 series of standards.	Item definition in accordance with ISO 26262-3:2018, 5.5.1	15.5.1 Base Vehicle Manufacturer or Supplier guideline resulting from requirements 15.4.2 and 15.4.3.
16 Integration of safety-related systems not developed according to ISO 26262	This Clause applies to T&B, where the objective is to achieve confidence that a system or component that is not developed according ISO 26262 satisfies the required level of functional safety needed for the integration into an item developed according to ISO 26262.	Item definition in accordance with ISO 26262-3:2018, 5.5.1	16.5.1 Safety rationale resulting from requirements 16.4.2 to 16.4.4.

Annex B
(informative)

Development Interface Agreement (DIA) example

B.1 Purpose

This annex provides an illustrative example of a DIA, in accordance with the requirements of Clause 5 [especially 5.4.3.1 c) to k)], with organization-specific adaptation under the requirements and recommendations of ISO 26262-2:2018, 5.4.6 and ISO 26262-2:2018, 5.5.1, if any. Project specific tailoring, in accordance with ISO 26262-2:2018, 6.4.5, can also be applied.

B.2 General

Many factors will affect the type and amount of customer-supplier interactions; the example is simplified, based on an application scenario described in B.3 and a set of premises listed in B.4.

Tables B.1 to B.3 constitute an example of a DIA as follows:

— Table B.1 approximately corresponds to the requirements of 5.4.2, with some organization-specific additions, intended to avoid or eliminate risk from a supplier with inadequate capability.

— Table B.2 approximately corresponds to the requirements of 5.4.3, with some organization-specific additions, intended to avoid or eliminate risk from improper understanding or definition of the boundary of Component C and its interactions with its environment.

— Table B.3 approximately corresponds to the requirements of 5.4.4, as applied to hardware Component C.

NOTE In each table, the corresponding ISO 26262 clause is indicated in parentheses.

B.3 Application scenario

The DIA example shown in Tables B.1 to B.3 is based on the following application scenario:

a) The customer is responsible for engineering and manufacturing the vehicle.

b) The customer is responsible for engineering the system comprised of many hardware and software components of which one hardware component, C, is to be sourced from some supplier.

c) Component C will be allocated requirements with assigned ASIL D.

d) Component C has not been developed previously, i.e., it is not a commercial off-the-shelf (COTS) product. It involves new technology for which there is an inadequate pool of proven suppliers.

e) Multiple suppliers are interested in the supply of Component C, but adequate capability to support the project is not evident.

f) A model-based development process is used.

B.4 Premises

This example is developed on the following premises:

a) Resources required for project management and engineering are available when needed.

b) Assessment teams that qualify as “independent” are available to each participating organization, and are used where needed.

c) The same process and architectural framework is in use in all the participating organizations, independently assessed to qualify for the highest integrity level.

   — Reusable assets conform to the process and architectural framework, and are independently assessed to qualify for the required integrity level.

   — Other resources, e.g., tools, conform to the process and architectural framework, and are independently assessed to qualify for the required integrity level.

   — The participating organizations choose specific processes and tools that are compatible, and commit to the same architecture.

   — Explicit meta-models or specifications define unambiguously the semantics of the tools, modelling languages, programming languages, and the produced models.

   — Models of externally-visible behaviour, performance (including worst-case), and failure modes and effects are available for hardware components, including I/O devices. The models are in a form that can be correctly integrated to create (sub-)system models.

d) There is high quality execution of other customer-supplier interactions, not unique to high integrity engineering, not included in this example, e.g., interactions for business processes, project management, and quality management.

In case the premises above do not hold, additional customer-supplier interactions and effort will be required — not identified in this example.

Table B.1 — Customer-supplier data exchanges to qualify and select supplier

ID	Activity	Data from customer to supplier	Data from supplier to customer
A.1	Pre-qualify[a] suppliers; Project independent criteria; Feeds into 5.4.2	Capability assessment questionnaire[a]: — safety culture (ISO 26262-2:2018, 5.4.2); — evidence of competence (ISO 26262-2:2018, 5.4.4); — evidence of quality management (ISO 26262-2:2018, 5.4.5); — ISO 26262 Consent, e.g.: — independent assessment (5.4.5); — DIA template	—
A.2		—	Acceptance of conditions[a]
A.3		—	Capability assessment[a] (ISO 26262-2:2018, Clause 5) Disclosure[a] Corrective action proposed[a]
A.4		Evaluation: ASILs for which not qualified[a]	—
A.5	Qualify suppliers (short-list)[a] 5.4.2	Customer-organization-specific process adaptation of ISO 26262-2:2018, 5.4.6 incl. methods, languages, tools & usage constraints/guidelines.	—
		—	First party assessment of compliance. Disclosure[a] Track record (5.4.2.1). Corrective action proposed[a] Alternative approach or proposal to meet objectives[a]
		Iterative evaluation & enquiries about gaps and alternatives[a]	Iterative revisions to plans and alternatives[a]
		Evaluation: ASILs for which not qualified[a]	—
A.6	Send proposal 5.4.2.2	RFP/RFQ, including project-specific tailored process [5.4.3.1 b)], product concept i.e. item definition (ISO 26262-3:2018, 5.5.1) and safety goals (extracted from ISO 26262-3:2018, 6.5.1).	—
A.7	—	—	Offer; Statement of compliance; Updates to previously submitted information[a]
A.8	Select supplier 5.4.2	Proposed DIA (project-specific) 5.4.3	—

[a] Activity or data which is organization-specific and is not required in ISO 26262.

Table B.1 *(continued)*

ID	Activity	Data from customer to supplier	Data from supplier to customer
A.9		—	Selected project resources and their capability assessment, e.g. safety team members' skills, competencies and qualification (ISO 26262-2:2018, 5.5.2); Organization-specific rules and processes (ISO 26262-2:2018, 5.5.1), incl. tools, libraries; Preliminary plans, e.g. safety plan (ISO 26262-2:2018, 6.5.3)
A.10		Iterative evaluation and enquiries, e.g. regarding skill gaps[a]	Iterative revisions addressing customer concerns[a]
A.11		Acceptance of DIA. (5.5.2) Selection report (5.5.1)	Acceptance of DIA (5.5.2)
A.12		Contract for concept (ISO 26262-3; ISO 26262-4) and planning phase (ISO 26262-2) incl. statement of development work.	Acceptance.

[a] Activity or data which is organization-specific and is not required in ISO 26262.

Table B.2 — Customer-supplier data exchanges in project initiation and system concept

ID	Activity	Data from customer to supplier	Data from supplier to customer
B.1	Initiate project (5.4.3) Create functional safety concept (ISO 26262-3:2018, Clauses 5 to 7)	System level plans Item definition (ISO 26262-3:2018, 5.5.1) and its lifecycle (Figure 1, ISO 26262-2:2018, 5.2.2; ISO 26262-2:2018, Figure 2 and ISO 26262-2:2018, 6.4.5) Functional safety concept (ISO 26262-3:2018, Clause 7)	—
B.2	—	—	Safety plan (5.5.3) HARA (5.4.3.2), Hardware component behaviour models, incl. fault metrics [5.4.3.1 f), ISO 26262-5:2018, Annex B, and ISO 26262-5:2018, Clause 9]. Independent assessment of plans, incl. assurance that processes and resources are configured and allocated to match the required work products, incl. skill-sets. [5.4.3.1 c) e), g), j), 5.4.5]
B.3	—	Acceptance	—
B.4	Consideration of experience gained from proven in use components, tools, libraries used in similar projects, as well as proven in use data and analyses of possible candidates (Clause 14)	Initial safety plan (ISO 26262-2:2018, Clause 5), incl. system safety case structure	—

Table B.2 *(continued)*

ID	Activity	Data from customer to supplier	Data from supplier to customer
B.5	—	—	Proven in use elements offered (Clause 14), with independent assessment of fitness for the project (5.4.5)
B.6	—	Acceptance	—
B.7	System development lifecycle [5.4.3.1 c)]	Technical safety concept (ISO 26262-4:2018, 6.5.2), relevant parts of system design specs, hardware specs, design & implementation (D&I) constraints, hardware-software Interface (HSI) specifications (ISO 26262-4:2018, 6.5.4).	Iterative evaluation, clarification-queries, and feedback about conflicts, completeness, consistency, etc.; technological limitations, if any; change requests, if any (5.4.4). Updated behaviour models, incl. fault models.
B.8		Iterative clarifications, responses, and revisions, including updates to system architecture design & verification specifications (ISO 26262-4:2018, 6.5.3, ISO 26262-4:2018, 6.5.6), hardware specifications (ISO 26262-5:2018, 7.5.1) relevant to Component C, HSI, allocation, etc.	Feedback about boundary between Component C & its environment.
B.9	—	—	Acceptance

Table B.3 — Customer-supplier data exchanges in hardware development lifecycle

ID	Activity	Data from customer to supplier	Data from supplier to customer
C.1	Plan (5.4.3)	Authorisation for hardware development	—
C.2		—	Plans: Safety plan (5.5.3 and ISO 26262-2:2018, 6.5.3), planning of DIA (5.4.3) etc. Independent reviews of conformance to planning (5.4.5).
C.3		Acceptance. Authorisation to commence requirements specification.	—
C.4	Requirements (5.4.5 and ISO 26262-5)	—	Hardware specifications - derived; refined; D&I constraints (ISO 26262-5:2018, 6.5.1). Extension to Verification Plan[a] HSI change requests, if any (ISO 26262-5:2018, 6.5.2). Independent safety audit (5.4.3.1) Independent confirmation (5.4.5 and 5.5.4).
C.5	—	Acceptance. Authorisation to commence design.	—

[a] Activity or data which is organization-specific and is not required in ISO 26262.

Table B.3 *(continued)*

ID	Activity	Data from customer to supplier	Data from supplier to customer
C.6	Design (5.4.5, and ISO 26262-5)	—	Design specs (ISO 26262-5:2018, 7.5.1); implementation constraints, incl. architectural (ISO 26262-5:2018, Clause 8). Extension or modification to HARA (ISO 26262-3:2018, Clause 6), if any. Extension to item integration and testing plan (ISO 26262-5:2018, 10.5). HSI change requests, if any (ISO 26262-5:2018, 6.5.2). Independent safety audit (5.4.3.1, 5.4.5)
C.7	5.4.4 and 5.4.5	Iterative evaluation and feedback concerning conflicts discovered at system level.	Iterative clarifications, revisions, and other responses addressing customer feedback and enquiries. Independent assessment (5.4.5 and 5.5.4).
C.8	5.4.4 and 5.4.5	Acceptance of component design. Authorisation to implement.	Implementation. Requirements from the environment. Independent assessment (5.4.5 and 5.5.4).
C.9	—	Acceptance	—
C.10	—	—	Prototype part Integrated verification (ISO 26262-5:2018, 10.5) Independent assessment (5.4.5).
C.11	—	Integrated evaluation (ISO 26262-4:2018, Clause 7). Change requests, if any.	—
C.12	—	—	Reviews & audits of processed changes Independent assessment (5.4.5, 5.5.4).
C.13	—	Acceptance	—
C.14	—	—	Sample for series production Independent assessment (5.4.5, 5.5.4).
C.15	—	Integrated evaluation (ISO 26262-4:2018, Clause 7) Change requests, if any.	—

[a] Activity or data which is organization-specific and is not required in ISO 26262.

Table B.3 *(continued)*

ID	Activity	Data from customer to supplier	Data from supplier to customer
C.16	—	—	Reviews & audits of processed changes Independent assessment (5.4.4, 5.4.5 and 5.5.4).
C.17	—	Authorisation for commencing production phase	—
C.18	—	—	Post-SOP reports (5.4.6 and 5.5.5 and ISO 26262-2:2018, 7.5.1).
[a] Activity or data which is organization-specific and is not required in ISO 26262.			

Bibliography

[1] ISO 26262-11:2018, *Road vehicles — Functional safety — Part 11: Guideline on application of ISO 26262 to semiconductors*

[2] ISO 26262-12:2018, *Road vehicles — Functional safety — Part 12: Adaptation of ISO 26262 for motorcycles*

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

[4] ISO/IEC/IEEE 15288, *Systems and software engineering — System life cycle processes*

[5] ISO 16750 (all parts), *Road vehicles — Environmental conditions and testing for electrical and electronic equipment*

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

[7] ISO 25119 (all parts), *Tractors and machinery for agriculture and forestry — Safety-related parts of control systems*

[8] ISO/IEC/IEEE 29148, *Systems and software engineering — Life cycle processes — Requirements engineering*

[9] ISO 13849 (all parts), *Safety of machinery — Safety-related parts of control systems*

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

[11] RTCA DO-178C, *Software Considerations in Airborne Systems and Equipment Certification*

[12] CMMI for Development, CMMI-DEV, Carnegie Mellon University Software Engineering Institute.

[13] German V-Model - Available at: http://www.v-modell-xt.de/[viewed 2018-09-27]

[14] AEC Q100. *Failure Mechanism Based Stress Test Qualification For Integrated Circuits*

[15] AEC Q101. *Failure Mechanism Based Stress Test Qualification For Discrete Semiconductors*

[16] AEC Q200. *Stress Test Qualification For Passive Components*

[17] Automotive SPICE®[4] - Available at: http://www.automotivespice.com [viewed 2018-09-27]

[18] ISO 10007, *Quality management — Guidelines for configuration management*

[19] ISO/IEC/IEEE 12207, *Systems and software engineering — Software life cycle processes*

[20] ISO/IEC 33000 (series), *Information Technology — Process Assessment*

4) 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 these products.

ICS 43.040.10

Price based on 60 pages