INTERNATIONAL STANDARD

ISO 26262-8

First edition
2011-11-15

Road vehicles — Functional safety —

Part 8: Supporting processes

Véhicules routiers — Sécurité fonctionnelle —

Partie 8: Processus d'appui

Reference number
ISO 26262-8:2011(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 26262-8 was prepared by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee SC 3, *Electrical and electronic equipment*.

ISO 26262 consists of the following parts, under the general title *Road vehicles — Functional safety*:

— *Part 1: Vocabulary*

— *Part 2: Management of functional safety*

— *Part 3: Concept phase*

— *Part 4: Product development at the system level*

— *Part 5: Product development at the hardware level*

— *Part 6: Product development at the software level*

— *Part 7: Production and operation*

— *Part 8: Supporting processes*

— *Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses*

— *Part 10: Guideline on ISO 26262*

Introduction

ISO 26262 is the adaptation of IEC 61508 to comply with needs specific to the application sector of electrical and/or electronic (E/E) systems within road vehicles.

This adaptation applies to all activities during the safety lifecycle of safety-related systems comprised of electrical, electronic and software components.

Safety is one of the key issues of future automobile development. New functionalities not only in areas such as driver assistance, propulsion, in vehicle dynamics control and active and passive safety systems increasingly touch the domain of system safety engineering. Development and integration of these functionalities will strengthen the need for safe system development processes and the need to provide evidence that all reasonable system safety objectives are satisfied.

With the trend of increasing technological complexity, software content and mechatronic implementation, there are increasing risks from systematic failures and random hardware failures. ISO 26262 includes guidance to avoid these risks by providing appropriate requirements and processes.

System safety is achieved through a number of safety measures, which are implemented in a variety of technologies (e.g. mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic) and applied at the various levels of the development process. Although ISO 26262 is concerned with functional safety of E/E systems, it provides a framework within which safety-related systems based on other technologies can be considered. ISO 26262:

a) provides an automotive safety lifecycle (management, development, production, operation, service, decommissioning) and supports tailoring the necessary activities during these lifecycle phases;

b) provides an automotive-specific risk-based approach to determine integrity levels [Automotive Safety Integrity Levels (ASIL)];

c) uses ASILs to specify applicable requirements of ISO 26262 so as to avoid unreasonable residual risk;

d) provides requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety being achieved;

e) provides requirements for relations with suppliers.

Functional safety is influenced by the development process (including such activities as requirements specification, design, implementation, integration, verification, validation and configuration), the production and service processes and by the management processes.

Safety issues are intertwined with common function-oriented and quality-oriented development activities and work products. ISO 26262 addresses the safety-related aspects of development activities and work products.

Figure 1 shows the overall structure of this edition of ISO 26262. ISO 26262 is based upon a V-model as a reference process model for the different phases of product development. Within the figure:

— the shaded “V”s represent the interconnection between ISO 26262-3, ISO 26262-4, ISO 26262-5, ISO 26262-6 and ISO 26262-7;

— the specific clauses are indicated in the following manner: “m-n”, where “m” represents the number of the particular part and “n” indicates the number of the clause within that part.

EXAMPLE “2-6” represents Clause 6 of ISO 26262-2.

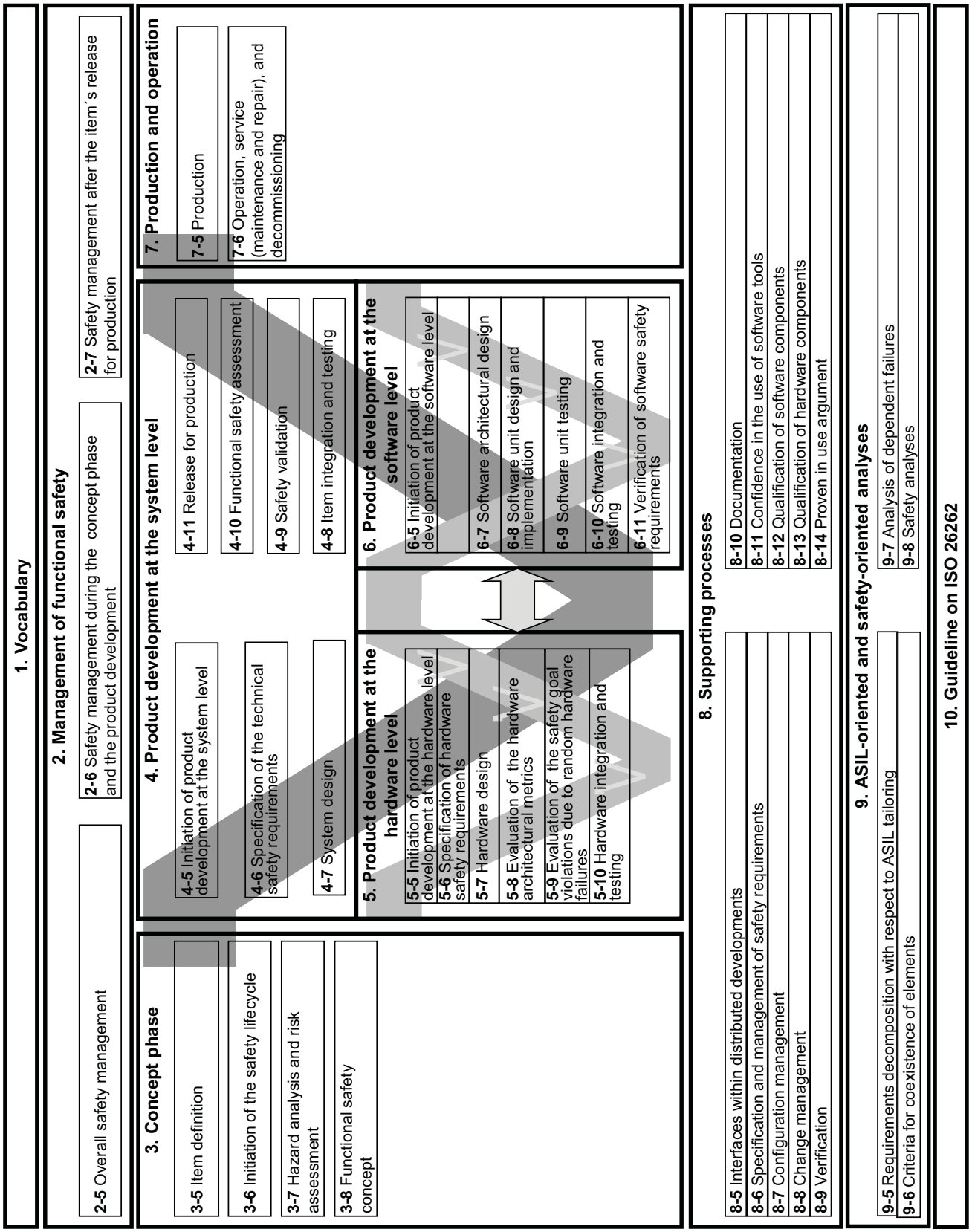


Figure 1 — Overview of ISO 26262

Road vehicles — Functional safety —

Part 8:
Supporting processes

1 Scope

ISO 26262 is intended to be applied to safety-related systems that include one or more electrical and/or electronic (E/E) systems and that are installed in series production passenger cars with a maximum gross vehicle mass up to 3 500 kg. ISO 26262 does not address unique E/E systems in special purpose vehicles such as vehicles designed for drivers with disabilities.

Systems and their components released for production, or systems and their components already under development prior to the publication date of ISO 26262, are exempted from the scope. For further development or alterations based on systems and their components released for production prior to the publication of ISO 26262, only the modifications will be developed in accordance with ISO 26262.

ISO 26262 addresses possible hazards caused by malfunctioning behaviour of E/E safety-related systems, including interaction of these systems. It does not address hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy and similar hazards, unless directly caused by malfunctioning behaviour of E/E safety-related systems.

ISO 26262 does not address the nominal performance of E/E systems, even if dedicated functional performance standards exist for these systems (e.g. active and passive safety systems, brake systems, Adaptive Cruise Control).

This part of ISO 26262 specifies the requirements for supporting processes, including the following:

— interfaces within distributed developments,

— overall management of safety requirements,

— configuration management,

— change management,

— verification,

— documentation,

— confidence in the use of software tools,

— qualification of software components,

— qualification of hardware components, and

— proven in use argument.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 26262-1:2011, *Road vehicles — Functional safety — Part 1: Vocabulary*

ISO 26262-2:2011, *Road vehicles — Functional safety — Part 2: Management of functional safety*

ISO 26262-3:2011, *Road vehicles — Functional safety — Part 3: Concept phase*

ISO 26262-4:2011, *Road vehicles — Functional safety — Part 4: Product development at the system level*

ISO 26262-5:2011, *Road vehicles — Functional safety — Part 5: Product development at the hardware level*

ISO 26262-6:2011, *Road vehicles — Functional safety — Part 6: Product development at the software level*

ISO 26262-7:2011, *Road vehicles — Functional safety — Part 7: Production and operation*

ISO 26262-9:2011, *Road vehicles — Functional safety — Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses*

ISO/IEC 12207, *Systems and software engineering — Software life cycle processes*

3 Terms, definitions and abbreviated terms

For the purposes of this document, the terms, definitions and abbreviated terms given in ISO 26262-1:2011 apply.

4 Requirements for compliance

4.1 General requirements

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

a) tailoring of the safety activities in accordance with ISO 26262-2 has been planned and shows that the requirement does not apply, or

b) a rationale is available that the non-compliance is acceptable and the rationale has been assessed in accordance with ISO 26262-2.

Information marked as a “NOTE” or “EXAMPLE” is only for guidance in understanding, or for clarification of the associated requirement, and shall not be interpreted as a requirement itself or as complete or exhaustive.

The results of safety activities are given as work products. “Prerequisites” are information which shall be available as work products of a previous phase. Given that certain requirements of a clause are ASIL-dependent or may be tailored, certain work products may not be needed as prerequisites.

“Further supporting information” is information that can be considered, but which in some cases is not required by ISO 26262 as a work product of a previous phase and which may be made available by external sources that are different from the persons or organizations responsible for the functional safety activities.

4.2 Interpretations of tables

Tables are normative or informative depending on their context. The different methods listed in a table contribute to the level of confidence in achieving compliance with the corresponding requirement. Each method in a table is either

a) a consecutive entry (marked by a sequence number in the leftmost column, e.g. 1, 2, 3), or

b) an alternative entry (marked by a number followed by a letter in the leftmost column, e.g. 2a, 2b, 2c).

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

For alternative entries, an appropriate combination of methods shall be applied in accordance with the ASIL indicated, independent of whether they are listed in the table or not. If methods are listed with different degrees of recommendation for an ASIL, the methods with the higher recommendation should be preferred. A rationale shall be given that the selected combination of methods complies with the corresponding requirement.

NOTE A rationale based on the methods listed in the table is sufficient. However, this does not imply a bias for or against methods not listed in the table.

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

— “++” indicates that the method is highly recommended for the identified ASIL;

— “+” indicates that the method is recommended for the identified ASIL;

— “o” indicates that the method has no recommendation for or against its usage for the identified ASIL.

4.3 ASIL-dependent requirements and recommendations

The requirements or recommendations of each subclause shall be complied with for ASIL A, B, C and D, if not stated otherwise. These requirements and recommendations refer to the ASIL of the safety goal. If ASIL decomposition has been performed at an earlier stage of development, in accordance with ISO 26262-9:2011, Clause 5, the ASIL resulting from the decomposition shall be complied with.

If an ASIL is given in parentheses in ISO 26262, the corresponding subclause shall be considered as a recommendation rather than a requirement for this ASIL. This has no link with the parenthesis notation related to ASIL decomposition.

5 Interfaces within distributed developments

5.1 Objectives

The objective of this clause is to describe the procedures and to allocate associated responsibilities within distributed developments for items and elements.

5.2 General

The customer (e.g. vehicle manufacturer) and the suppliers for item developments jointly comply with the requirements specified in ISO 26262. Responsibilities are agreed between the customer and the suppliers. Subcontractor relationships are permitted. Just as with the customer's safety-related specifications concerning planning, execution and documentation for in-house item developments, comparable procedures are to be

agreed for co-operation with the supplier on distributed item developments, or item developments where the supplier has the full responsibility for safety.

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

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:

— the draft version of development interface agreement (DIA) (from external source);

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

5.4 Requirements and recommendations

5.4.1 Application of requirements

5.4.1.1 The requirements of Clause 5 shall apply to each item and element developed according to ISO 26262, except for off-the-shelf hardware parts, if either of the following applies:

a) there are no specific hardware safety requirements allocated to the hardware parts, or

b) the off-the-shelf hardware parts are qualified according to well-established procedures based on worldwide quality standards (e.g. AEC standards for electronic components), and the qualification of the off-the-shelf hardware parts covers ranges of parameters with regard to the intended application.

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 top level supplier, 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 produce items and elements of comparable complexity and ASIL according to ISO 26262.

NOTE Supplier selection criteria includes:

— evidence of the supplier's quality management system;

— the supplier's past performance and quality;

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

— results of previous safety assessments according to ISO 26262-2:2011, 6.4.9;

— 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 item definition or functional specification of the element, and

c) the safety goals, the functional safety requirements or the technical safety requirements, including their respective ASIL if already available, depending on what the supplier is quoting for.

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

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:

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

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

b) the joint tailoring of the safety lifecycle in accordance with ISO 26262-2:2011, 6.4.5,

c) the activities and processes to be performed by the customer and the activities and processes to be performed by the supplier,

d) the information and the work products to be exchanged,

NOTE 1 This includes an agreement on the documentation to be provided for the completion of the customer's and supplier's safety cases.

NOTE 2 The information exchanged includes the safety-related special characteristics.

NOTE 3 In the case of a distributed development, the relevant parts of the work products necessary for the activities of the development parties involved can be identified and exchanged.

e) the parties or persons responsible for the activities,

f) the communication 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 faults metric and latent faults 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), and

g) the supporting processes and tools, including interfaces, to assure compatibility between customer and supplier.

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.

5.4.3.3 The party responsible for the item development shall create the functional safety concept in accordance with ISO 26262-3. The functional safety requirements shall be agreed between the customer and the supplier.

5.4.4 Execution of distributed development

5.4.4.1 The supplier shall report to the customer each issue which increases the risk of not conforming to the project plan, the safety plan, integration and testing plan in accordance with ISO 26262-4 or the software verification plan in accordance with ISO 26262-6, or other provisions of the DIA.

5.4.4.2 The supplier shall report to the customer each anomaly which occurs during the development activities in their area of responsibility or in that of their subcontractors.

5.4.4.3 The supplier shall determine whether each safety requirement can be complied with. If not, the safety concept shall be re-examined and, if necessary, modified to yield safety requirements that will be met.

5.4.4.4 Each change potentially affecting the safety of the item or the planned activities to demonstrate compliance with ISO 26262 shall be communicated to the other party to support the impact analysis in accordance with Clause 8.

5.4.4.5 Both parties should consider previous experience gained in similar developments in accordance with ISO 26262-2:2011, 5.4.2.7, when deriving safety requirements for the current development.

5.4.4.6 The supplier shall report to the customer's safety manager the progress achieved against the tasks and milestones defined in the safety plan. The format of the report and the delivery dates shall be agreed between the supplier and the customer.

EXAMPLE At regular intervals, or when the milestones specified in the framework of the schedule have been reached, the customer inspects the released quality management reports compiled by the supplier.

5.4.4.7 An agreement shall be reached on which party (supplier or customer) shall perform the safety validation in accordance with ISO 26262-4.

NOTE If the supplier performs the 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).

5.4.4.8 This requirement applies to ASIL D in accordance with 4.3. The customer shall be allowed to perform additional functional safety audits at the supplier's premises at any appropriate time.

5.4.5 Functional safety assessment at supplier's premises

5.4.5.1 This requirement applies to ASILs (B), C, D in accordance with 4.3. One or more functional safety assessments shall be carried out upon reaching defined milestones, these assessments shall include each phase of the item development. The functional safety assessments shall be at the level of detail appropriate for the complexity of the item and the ASILs of its safety goals. The functional safety assessment shall be performed in accordance with ISO 26262-2:2011, 6.4.9.

5.4.5.2 This requirement applies to ASIL B in accordance with 4.3. A functional safety assessment should be carried out.

NOTE This can be done by the customer, another organization or by the supplier itself.

5.4.5.3 This requirement applies to ASILs C and D in accordance with 4.3. A functional safety assessment in accordance with ISO 26262-2:2011, 6.4.9, shall be carried out at the supplier's premises by the customer, or by an organization or person designated by the customer.

NOTE This can be done by the supplier itself.

5.4.5.4 This requirement applies to ASILs (B), C and D in accordance with 4.3. The functional safety assessment report shall be available at the customer's and at the supplier's premises.

5.4.5.5 This requirement applies to ASILs (B), C and D in accordance with 4.3. Each anomaly identified, that potentially impacts the deliverables from the supplier, shall be analyzed and actions shall be derived to resolve them. An agreement between both parties shall be reached on who performs the actions required.

5.4.6 After release for production

5.4.6.1 The supplier shall provide evidence to the customer that the process capability is being met and maintained in accordance with ISO 26262-2:2011, Clause 7, and ISO 26262-7:2011, Clause 5.

5.4.6.2 A supply agreement between the customer and the supplier shall address the responsibilities for functional safety in accordance with ISO 26262-2:2011, 7.4.2.1, and define the safety activities for each party.

5.4.6.3 The supply agreement shall state the access to, and exchange of, production monitoring records between the parties for the safety-related special characteristics.

5.4.6.4 Each party that becomes aware of a safety-related event shall report this in a timely manner and according to the supply agreement. If a safety-related event occurs, an analysis of that event shall be performed. This analysis should include similar items and related parties which are potentially affected by a similar event.

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 requirement 5.4.3.

5.5.3 **Supplier's project plan** resulting from requirement 5.4.3.

5.5.4 **Supplier's safety plan** resulting from requirement 5.4.3.

5.5.5 **Functional safety assessment report** resulting from requirements 5.4.5.1 to 5.4.5.5.

5.5.6 **Supply agreement** resulting from requirements 5.4.6.2 to 5.4.6.3.

6 Specification and management of safety requirements

6.1 Objectives

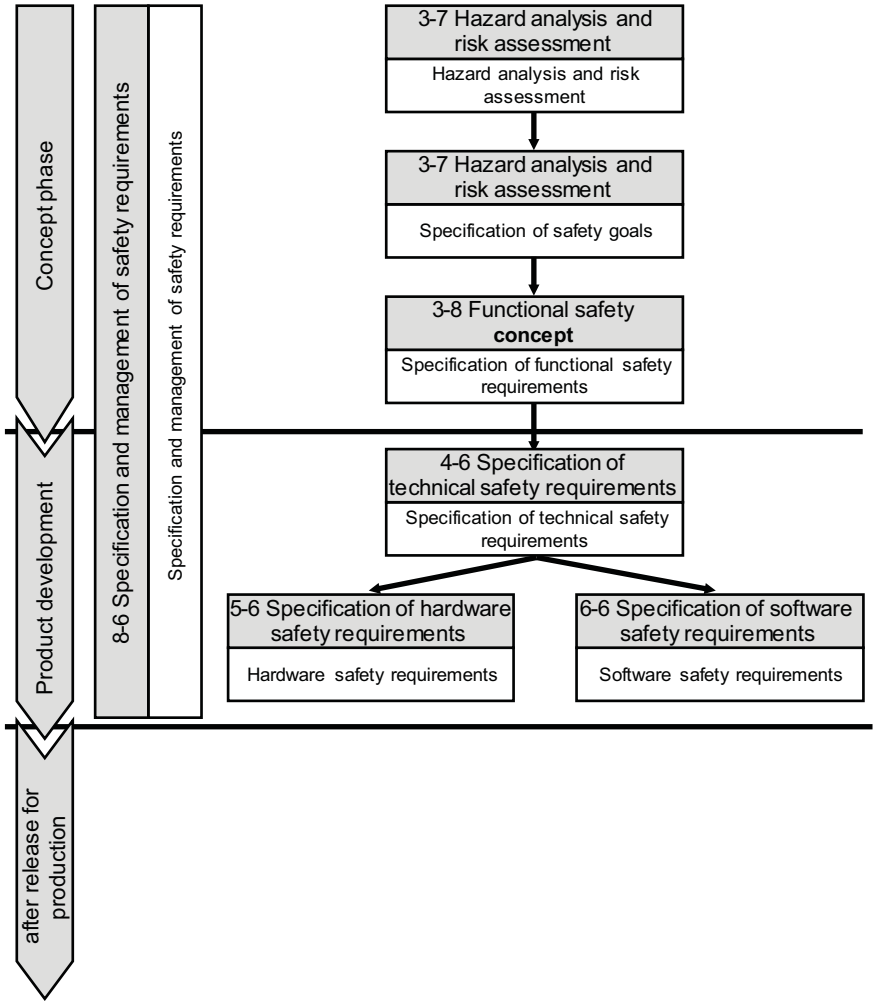
The first objective is to ensure the correct specification of safety requirements with respect to their attributes and characteristics.

The second objective is to ensure consistent management of safety requirements throughout the entire safety lifecycle.

6.2 General

Safety requirements constitute all requirements aimed at achieving and ensuring the required ASILs.

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



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 Clause 7 of ISO 26262-3.

Figure 2 — Structure of safety requirements

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

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

This clause includes requirements on the specification and management of safety requirements (see Figure 3).

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.

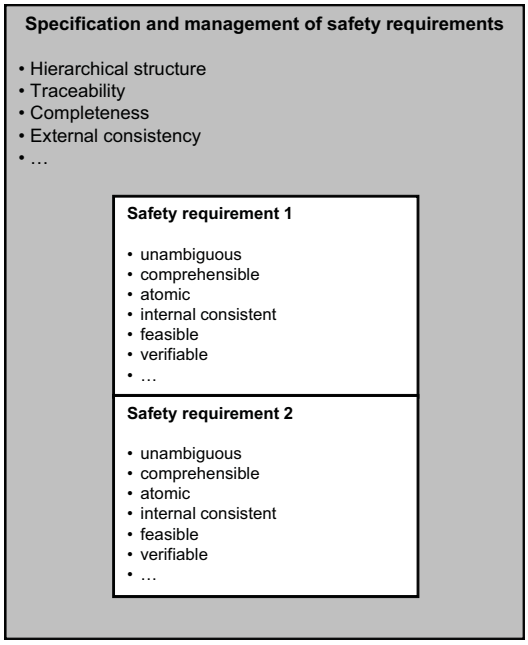


Figure 3 — Relationship between management of safety requirements and particular safety requirements

6.3 Inputs to this clause

6.3.1 Prerequisites

See 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

6.4.1.1 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.

NOTE For higher level safety requirements (e.g. functional and technical safety requirements) natural language is more appropriate while for lower level safety requirements (e.g. software and hardware safety requirements) notations listed in Table 1 are more appropriate.

Table 1 — Specifying safety requirements

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

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 (see ISO 26262-1:2011, definition 1.108).

6.4.2.3 Safety requirements shall be allocated to an item or an element.

6.4.2.4 Safety requirements shall have the following characteristics:

a) unambiguous and comprehensible,

NOTE 1 A requirement is unambiguous if there is common understanding of the meaning of the requirement.

NOTE 2 A requirement is comprehensible if the reader at an adjacent abstraction level (i.e. either the stakeholder or the consumer of that requirement) understands its meaning.

b) atomic,

NOTE Safety requirements at one hierarchical level are atomic when they are formulated in such a way that they can not be divided into more than one safety requirement at the considered level.

c) internally consistent,

NOTE Unlike external consistency, in which multiple safety requirements do not contradict each other, internal consistency means that each individual safety requirement contains no contradictions within itself.

d) feasible, and

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

e) verifiable.

6.4.2.5 Safety requirements shall have the following attributes:

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

EXAMPLE 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 A status of a safety requirement can be “proposed”, “assumed”, “accepted”, or “reviewed”.

c) an ASIL.

6.4.3 Management of safety requirements

6.4.3.1 The set of safety requirements shall have the following properties:

a) hierarchical structure,

NOTE 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.

b) organizational structure according to an appropriate grouping scheme,

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

c) completeness,

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

d) external consistency,

NOTE 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 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 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.

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

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

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

c) the specification of verification in accordance with 9.4.2.

NOTE Additionally, traceability supports:

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

— the functional safety assessment.

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 ISO 26262 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	o	+	+	+

[a] Method 1c can be supported by executable models.

6.4.3.4 Safety requirements shall be placed under configuration management in accordance with Clause 7.

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 first objective is to ensure that the work products, and the principles and general conditions of their creation, can be uniquely identified and reproduced in a controlled manner at any time.

The second objective is 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 ISO/TS 16949, ISO 10007 and ISO/IEC 12207.

Each work product of ISO 26262 is managed by configuration management.

7.3 Inputs to this clause

7.3.1 Prerequisites

The following information shall be available:

— Safety plan in accordance with ISO 26262-2:2011, 6.5.1.

— 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.

7.4.2 The configuration management process shall comply with:

a) the respective requirements of a quality management system (e.g. ISO/TS 16949, or ISO 9001), and

b) the specific requirements for software development according to the clause on configuration management in ISO/IEC 12207.

7.4.3 The work products required by the safety plan in accordance with ISO 26262-2 shall be placed under configuration management and baselined according to the configuration management strategy.

7.4.4 Work products placed under configuration management shall be documented in the configuration management plan**.**

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 in 7.4.1, 7.4.2 and 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 throughout the safety lifecycle.

8.2 General

Change management ensures the systematic planning, control, monitoring, implementation and documentation of changes, while maintaining the consistency of each work product. Potential impacts on functional safety are assessed before changes are made. For this purpose, decision-making processes for change are introduced and established, and responsibilities are assigned to the parties involved.

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

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 26262-2:2011, 6.5.2.

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 initiated at the same time. Interfaces between the two processes are defined and maintained to enable the traceability of changes.

8.4.1.2 The work products to be subject to change management shall be identified and shall include those work products required by ISO 26262 to be placed under configuration management.

8.4.1.3 The schedule for applying the change management process shall be defined for each work product.

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 of the accepted changes in accordance with 8.4.5, and

e) the documentation in accordance with 8.4.5.

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 involved, its interfaces and connected items, shall be carried out for each change request. The following shall be addressed:

a) the type of change request,

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

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

c) the identification and involvement of the parties affected, 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 work products 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 Carrying out and documenting the change

8.4.5.1 The changes shall be carried out and verified as planned.

8.4.5.2 If the change has an impact on safety-related functions, the assessment of functional safety and the applicable confirmation reviews, in accordance with ISO 26262-2:2011, 6.4.7 and 6.4.9, 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 at an appropriate level including configurations and versions, in accordance with Clause 7 (Configuration management),

b) the details of the change carried out, and

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

NOTE 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 8.4.1.1 to 8.4.1.3.

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

8.5.3 **Impact analysis** and **change request plan** resulting from requirements 8.4.3.1, 8.4.4.1 and 8.4.4.2.

8.5.4 **Change report** resulting from requirement 8.4.5.3.

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.

   1) 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 26262-4:2011, Clause 7 (System design), ISO 26262-5:2011, Clause 7 (Hardware design), ISO 26262-6:2011, Clause 7 (Software architectural design) and ISO 26262-6:2011, Clause 8 (Software unit design and implementation).

   2) In the test phases, verification is the evaluation of the work products 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:

   1) the safety requirements are appropriately realised in the production process, user manuals and repair and maintenance instructions; and

   2) 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 26262-4:2011, Clause 9 (Safety validation), for further details.

9.3 Inputs to this clause

9.3.1 Prerequisites

See 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 subphase of the safety lifecycle and shall address the following:

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

b) the methods used for verification,

NOTE Methods for verification include review, walk-through, inspection, model-checking, simulation, engineering analyses, demonstration, and testing. Typically verification applies a combination of these and other methods.

c) the pass and fail criteria for the verification,

d) the verification environment, if applicable,

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

e) the tools used for verification, if applicable,

f) the actions to be taken if anomalies are detected, and

g) 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 select and 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, and

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

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

NOTE 2 To avoid the redundant specification and storage of preconditions, configurations and environmental conditions used for various test cases, the use of an unambiguous reference to such data is recommended.

9.4.2.3 For testing, test cases shall be grouped according to the test methods to be applied. For each test method, in addition to the test cases, the following shall be specified:

a) the test environment,

b) the logical and temporal dependencies, and

c) the resources.

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 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 c)] and to the expected verification results.

f) the reasons for any verification steps not executed.

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 9.4.2.3.

9.5.3 **Verification report** resulting from requirements 9.4.3.1 and 9.4.3.2.

10 Documentation

10.1 Objectives

The primary 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

The documentation requirements in ISO 26262 focus mainly on information, and not on layout and appearance.

The information need not be made available in physical documents, unless explicitly specified by ISO 26262. 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:

— safety plan in accordance with ISO 26262-2:2011, 6.5.1

10.3.2 Further supporting information

None.

10.4 Requirements and recommendations

10.4.1 The documentation 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 functional safety assessment.

10.4.2 The identification of a work product in ISO 26262 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, and

d) 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".

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.

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 first objective of this clause is to provide criteria to determine the required level of confidence in a software tool when applicable.

The second objective of this clause is 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 tailor the activities or tasks required by ISO 26262 (i.e. the user can rely on the correct functioning of a software tool for those activities or tasks required by ISO 26262).

11.2 General

A software tool used in the development of a system or its software or hardware elements, can support or enable a tailoring of the safety-lifecycle, through the tailoring of 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 ISO 26262, if activities or tasks required by ISO 26262 rely on the correct functioning of the software tool used.

NOTE The understanding of “software tool” can vary from a separately used stand-alone software tool to a set of software tools integrated into a tool-chain.

EXAMPLE Such software tools can be 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.

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.

If indicated by the determined tool confidence level, then appropriate qualification methods are applied to comply with both this tool confidence level and the maximum ASIL of all the safety requirements allocated to the item or element that is to be developed using the software tool. Otherwise there is no need to apply such qualification methods.

11.3 Inputs to this clause

11.3.1 Prerequisites

The following information shall be available:

— safety plan in accordance with ISO 26262-4:2011, 5.5.2;

— 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 external source);

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

11.4 Requirements and recommendations

11.4.1 General requirement

11.4.1.1 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 ISO 26262 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

11.4.2.1 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 confirmed, in accordance with ISO 26262-2:2011, Table 1, 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 can be a cross-organizational activity, thus facilitating the classification or qualification effort.

11.4.3 Software tool compliance with its evaluation criteria or its qualification

11.4.3.1 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 same use cases together with the same 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 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 or an applied subset of the software tool’s functionality.

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

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

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

   NOTE 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.

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 work-around measures, if applicable, and

EXAMPLE 1 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 2 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 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 Measures for the detection of erroneous corresponding outputs can address both known and potential errors in the output of software tools.

EXAMPLE Comparisons of outputs of redundant software tools, tests performed, static analyses or reviews, analyses of log files of the software tool.

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 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 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 environmental and functional constraints, if applicable.

EXAMPLE Embedding the software tool into the development processes, the usage of shared data by different software tools and other usage conditions, 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):

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

2) 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):

1) 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;

2) 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;

3) 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 this subsequently-used software tool.

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 can be chosen for a code generator in case the produced source code is verified in accordance with ISO 26262.

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

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 If a software tool is used for the tailoring of the development process in such a way that activities or tasks required by ISO 26262 are omitted, TD2 shall not be selected.

11.4.5.5 Based on the values determined for the classes of TI and TD (in accordance with 11.4.5.2, 11.4.5.3 or 11.4.5.4), 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 or RTCA DO-178.

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 or RTCA DO-178.

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) the pre-determined maximum ASIL, or specific ASIL, of any safety requirement which might 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 requirements of this subclause shall be complied with.

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 subclause.

a) the software tool has been used previously for the same purpose with comparable use cases and 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 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 work-arounds for the known malfunctions, or detection measures for a corresponding erroneous output, if applicable.

EXAMPLE 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 considered 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 requirements of this subclause shall be complied with.

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 provided by an assessment based on an appropriate national or international standard and the proper application of the assessed development process shall be demonstrated.

NOTE This assessment 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, CMMI, ISO 15504.

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 requirements of this subclause shall be complied with.

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

a) the validation measures shall demonstrate that the software tool complies with its specified requirements,

   NOTE Tests designed to evaluate functional and non-functional quality aspects of the software tool can be used for validation.

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

11.4.10 Confirmation review of qualification of a software tool

This subclause applies to ASILs (B), C, D, in accordance with 4.3.

The confidence in the use of the software tool shall be evaluated in accordance with ISO 26262-2:2011 Table 1 to ensure:

a) the correct evaluation of the required level of confidence in the software tool, and

b) the appropriate qualification of the software tool in accordance with its required level of confidence.

11.5 Work products

11.5.1 Software tool criteria evaluation report resulting from requirements 11.4.1, 11.4.2, 11.4.3, 11.4.4, 11.4.5 and 11.4.10.

11.5.2 Software tool qualification report resulting from requirements 11.4.1 to 11.4.10.

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 ISO 26262.

12.2 General

The re-use of qualified software components avoids re-development for software components with similar or identical functionality.

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

EXAMPLE Software components addressed by this clause include:

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

— 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:

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

12.3.2 Further supporting information

The following information can be considered:

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

— 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 12.4.3.1,

b) evidence that the software component complies with its requirements in accordance with 12.4.3.2, 12.4.3.3, and 12.4.3.4,

c) evidence that the software component is suitable for its intended use in accordance with 12.4.4, and

d) evidence that the software development process for the component is based on an appropriate national or international standard.

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

12.4.2 Software component qualification planning

12.4.2.1 The planning of qualification of a software component shall determine:

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, and

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

12.4.3 Qualification of a software component

12.4.3.1 The specification of the software component shall include:

a) the requirements of the software component,

EXAMPLE The following requirements:

— functional 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 many 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).

b) 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.

c) the description of interfaces,

d) the application manual, where appropriate,

e) the description of the software component integration,

NOTE Description might include the development tools required to integrate and use the software component.

f) the reactions of the functions under anomalous operating conditions,

EXAMPLE Re-entrant calling of non-re-entrant software component functions.

g) the dependencies with other software components, and

h) a description of known anomalies with corresponding work-around measures.

12.4.3.2 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 26262-6:2011, Clause 9,

NOTE This verification is primarily based on requirements-based testing. 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) result in no known errors that lead to violation of safety requirements.

12.4.3.3 This subclause applies to ASIL D in accordance with 4.3.

The structural coverage shall be measured in accordance with ISO 26262-6:2011, Clause 9, to evaluate the completeness of the test cases. If necessary, additional test cases shall be specified or a rationale shall be provided.

12.4.3.4 The verification in accordance with 12.4.3.2, shall only be valid for an unchanged implementation of the software component.

12.4.3.5 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 target ASIL of any safety requirement that might be violated if the software component performs incorrectly.

12.4.4 Verification of qualification of a software component

12.4.4.1 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. If necessary, additional measures shall be applied.

NOTE The validity of the qualification can be influenced when the qualification has been performed in the context of another industrial or automotive domain.

EXAMPLE Engine control, body control and chassis control are different automotive domains. Railways and civil avionics are different industrial domains.

12.4.4.2 The specification of the software component shall comply with the requirements of the intended use of this software component.

12.5 Work products

12.5.1 Software component documentation resulting from requirement 12.4.3.1.

12.5.2 Software component qualification report resulting from requirement 12.4.3.5.

12.5.3 Safety plan (refined) resulting from requirement 12.4.2.

13 Qualification of hardware components

13.1 Objectives

The first objective of the qualification of hardware components is to provide evidence of the suitability of intermediate level hardware components and parts for their use as part of items, systems or elements, developed in compliance with ISO 26262, concerning their functional behaviour and their operational limitations for the purposes of the safety concept.

The second objective of the qualification of hardware components is to provide relevant information regarding:

— their failure modes,

— their failure mode distribution, and

— their diagnostic capability with respect to the safety concept for the item.

13.2 General

Every safety-related hardware component and part used within the scope of ISO 26262 is subject to standard qualification to address general functional performance, conformity of production, environmental endurance and robustness.

EXAMPLE 1 Qualification in accordance with ISO 16750, or with AEC-Q100 or AEC-Q200 standards, for electronic parts or equivalent company standards.

For basic parts (passive component, discrete semiconductor), standard qualification is sufficient. These basic parts can then be used in a hardware design in accordance with ISO 26262-5.

The requirements of this clause apply to intermediate level hardware components or parts, which provide dedicated functionality to the system.

EXAMPLE 2 Sensors, actuators, ASICs with dedicated functionality (e.g. protocol adapter).

If the intermediate level hardware component or part is safety-related, depending on its level, it is integrated and tested in accordance with ISO 26262-4 or ISO 26262-5 or both in addition to its qualification in accordance with this clause.

Usually the qualification described in this clause can be applied to components or parts whose failure modes or malfunctions are known and that are adequately testable regarding their possible failures.

EXAMPLE 3 During the development of a fuel pressure sensor the correct function of the sensor was approved within its boundary of operation up to 200 bar fuel pressure and 140 °C temperature. The qualification of this fuel pressure sensor enables the use of this sensor for the realisation of a particular safety-related item with regard to functional performance of the sensor and its malfunctions, provided that the same or lower boundaries of operation apply. In such a situation, the design analysis and the integration and testing of the basic hardware of the sensor according to ISO 26262-5 can be omitted and the integration activities can be carried out directly following ISO 26262-4 with regard to the technical safety requirements allocated to the sensor.

A summary for qualification and integration of basic parts, hardware parts and components is shown in Table 6.

Table 6 — Qualification, integration and test activities to be conducted depending on the level of hardware part or component

Activity	Hardware part or component			
	Safety-related basic hardware part	**Safety-related intermediate hardware part**	**Safety-related intermediate hardware component**	**Safety-related complex hardware component**
	(e.g. resistors, transistors)	(e.g. gray code decoder)	(e.g. fuel pressure sensor)	(e.g. ECU)
Standard qualification	Applicable	Applicable	—	—
Qualification in accordance with Clause 13	—	Applicable	Applicable	—
Integration/test in accordance with ISO 26262-5	—	Applicable[a]	Applicable[a]	Applicable
Integration/test in accordance with ISO 26262-4	—			Applicable

[a] The hardware part or component will be integrated in accordance with ISO 26262-4, or ISO 26262-5, or both ISO 26262-4 and ISO 26262-5, depending on its level.

Qualification of hardware components or parts can be done using two different methods: testing or analysis. These methods can be used individually or in combinations depending on the hardware components or parts.

— When testing, the hardware component or part is exposed to the intended environmental and operational conditions and compliance with its functional requirements is assessed. Reproducing exact environmental conditions is difficult and also any extrapolations are subject to error, therefore the limitations of such test conditions are considered when interpreting the results of tests.

— A qualification through analysis relies on a rationale for the analytical methods and assumptions used. In general, a hardware component is too complex to be qualified by analysis alone. However, the analysis can be used effectively for the extrapolation of testing data and to determine the effects of smaller changes in the already tested hardware component.

Even if different qualification methods are used, the final results are available in a qualification report (which can consist of a set of documents that include reports on findings, notes on interpretation, etc.) that gives evidence of the assumptions, conditions and test cases and results used to qualify the hardware components or parts with associated results. If possible, it is better to formulate the synthesis in such a way that independent checking is possible; it usually includes the performance data, the qualification process, the results and the rationales.

Directions present in ISO 16750 are useful for defining the type and sequence of qualification tests.

13.3 Inputs to this clause

13.3.1 Prerequisites

The following information shall be available:

— related safety requirements,

— qualification criteria (analysis and tests) in accordance with ISO 26262-5:2011, Clause 6, and

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

13.3.2 Further supporting information

The following information can be considered:

— test criteria in accordance with ISO 26262-5:2011, Clause 6;

— see further supporting information for the phases of the safety lifecycle where the qualification of hardware components is applied.

13.4 Requirements and recommendations

13.4.1 General

13.4.1.1 The criteria to apply this clause are:

a) the component or part to be qualified shall have an intermediate complexity excluding complex hardware components and basic hardware parts, and

b) the relevant failure modes of the component or part to be qualified shall be assumed to be verifiable by testing, analysis or both.

13.4.2 Goals of qualification of hardware components or part

13.4.2.1 The following goals shall be achieved by the qualification of hardware component or part:

a) adequate functional performance of components or parts for the purposes of the safety concept,

b) identification of failure modes and models (quantification of their distribution) by using appropriate tests (such as over limit test, accelerated test...) or analyses,

c) sufficient robustness, and

d) identification of limits of use for components or parts.

13.4.3 Methods for qualification of the hardware component or part

13.4.3.1 The qualification of the hardware component or part shall be carried out using an appropriate selection of the following methods:

a) analyses, and

b) testing.

13.4.4 Qualification plan

13.4.4.1 A qualification plan shall be developed and shall describe:

a) precise identification and version of the hardware component or part,

b) specification of the environment in which the hardware component or part is intended to be used,

c) the qualification strategy and the rationale,

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

d) the necessary tools and equipment enabling this strategy,

e) the party responsible for carrying out this strategy, and

f) the criteria used to assess the qualification of a hardware component or part as passed or failed.

13.4.5 Qualification argument

13.4.5.1 A comprehensive argument that the performance of the hardware component or part complies with its specification 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.

13.4.5.2 The comprehensive argument of 13.4.5.1 shall be based on a combination of the following types of information:

a) analytical methods and assumptions used; or

b) data from operational experience; or

c) existing testing results.

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

13.4.6 Qualification by analyses

13.4.6.1 The analysis shall be expressed in a form that can be easily understood and checked by persons who are qualified in the relevant engineering or scientific disciplines.

NOTE Analytical methods that can be used include extrapolations, mathematical models, damage analysis or similar methods.

13.4.6.2 The analyses shall consider all the environmental conditions to which the hardware component or part is exposed, the limits of these conditions and, other additional strains related to operation (e.g. expected switch cycles, charging and discharging, long turn-off times).

13.4.7 Qualification by Testing

13.4.7.1 A test plan shall be developed and shall contain the following information:

a) description of the functions of the hardware component or part,

b) number and sequence of tests to be conducted,

c) requirements for assembly and connections,

d) procedure for accelerated ageing, considering the operating conditions of the hardware component or part,

e) operating and environmental conditions to be simulated,

f) pass/fail criteria to be established,

g) environmental parameters to be measured,

h) requirements for the testing equipment, including accuracy, and

i) maintenance and replacement processes permitted during the testing.

13.4.7.2 A standardized test specification shall be used.

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

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

13.4.8 Qualification report

13.4.8.1 The qualification report shall state whether the hardware component or part has passed or failed the qualification with respect to the operating envelope.

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

13.4.8.2 The qualification report shall be verified in accordance with Clause 9.

13.5 Work products

13.5.1 Qualification plan resulting from requirement 13.4.4.

13.5.2 Hardware component test plan if applicable, resulting from requirement 13.4.7.1.

13.5.3 Qualification report resulting from requirement 13.4.8.1.

14 Proven in use argument

14.1 Objectives

This clause provides guidance for a proven in use argument. A proven in use argument is an alternate means of compliance with ISO 26262 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 software product, can be a candidate for a proven in use argument.

A candidate can also refer to system, hardware or software work products such as a technical safety concept, algorithms, models, source code, object code, software components, a set of configurations or calibration data.

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 ECU in operation intended to implement an additional function; or

c) a candidate being in the field prior to the release of ISO 26262; 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 service period of the candidate (see 14.4.5), and

— the changes, if any, that could have impacted the candidate since its service 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 26262-2:2011, 6.5.3.

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

14.4 Requirements and recommendations

14.4.1 General

14.4.1.1 The following subclauses 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 26262-2:2011, 6.4.3.5.

14.4.2.3 The proven in use credit shall be limited to the safety lifecycle subphases 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 26262-4:2011, Clause 8.

EXAMPLE The hardware of an ECU has a satisfactory service history and is intended to be 100 % carried over to a new application. The proven in use credit can be applied to the subphases 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 subphases 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 26262-4:2011, 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 26262-2:2011, 6.4.7.

14.4.2.7 Any change 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

14.4.3.1 A description of the candidate and its previous use shall be available, that 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 changes to the candidate

14.4.4.1 Proven in use candidates

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

NOTE 1 Changes 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 performances 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 changes 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 Changes to items introduced for a future application

Changes to items and their environment introduced for the purpose of a future application shall comply with ISO 26262-3:2011, 6.4.2.

14.4.4.3 Changes to elements introduced for a future application

Changes to elements and their environment introduced for the purpose of a future application within a different item shall comply with Clause 8.

14.4.4.4 Changes to candidate independent of future application

Changes to a candidate introduced after its service 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 service 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 service period of the candidate shall be available.

14.4.5.2.2 The service 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 service period of the candidate.

14.4.5.2.4 For a proven in use status to be obtained by the candidate, its service period shall demonstrate compliance with each safety goal that can be violated by the candidate in accordance with Table 7 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 7 — 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 8 gives an example of the required minimum service period without observable incident which is necessary to achieve 70 % confidence:

Table 8 — Targets for minimum service period of candidate

ASIL	Minimum service 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 service period, t_{service}, can be adjusted as follows:

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

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 service period of the candidate shall demonstrate compliance with each safety goal that can be violated by the candidate in accordance with Table 9 with a single sided lower confidence level of 70 % (using a chi-square distribution).

Table 9 — 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 9 to the observable incident rate and to use Table 7 for the candidate; or alternatively

— to provide evidence that the root cause of the observed incident is fully identified and eliminated in accordance with ISO 26262, 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 26262-7:2011, 6.4.2.1).

14.5 Work products

14.5.1 Safety plan (refined) resulting from requirements 14.4.2.1 to 14.4.2.7.

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

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

Annex A
(informative)

Overview on and document flow 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 objective of this clause is to describe the procedures and to allocate associated responsibilities within distributed developments for items and elements.	See prerequisites of the relevant phases of the safety lifecycle for which the distributed development is carried out.	5.5.1 Supplier selection report 5.5.2 Development interface agreement (DIA) 5.5.3 Supplier's project plan 5.5.4 Supplier's safety plan 5.5.5 Safety assessment report 5.5.6 Supply agreement
6 Specification and management of safety requirements	The first objective is to ensure the correct specification of safety requirements with respect to their attributes and characteristics. The second objective is to ensure consistent management of safety requirements throughout the entire safety lifecycle	See applicable prerequisites of the relevant phases of the safety lifecycle in which safety requirements are specified or managed.	None
7 Configuration management	The first objective is to ensure that the work products, and the principles and general conditions of their creation, can be uniquely identified and reproduced at any time. The second objective is to ensure that the relations and differences between earlier and current versions can be traced.	Safety plan in accordance with ISO 26262-2:2011, 6.5.1. Applicable prerequisites of the relevant phases of the safety lifecycle where configuration management is planned or managed.	7.5.1 Configuration management plan
8 Change management	The objective of change management is to analyse and control changes to safety-related work products occurring throughout the safety lifecycle.	Configuration management plan (see 7.5.1). Project plan in accordance with ISO 26262-2:2011, 6.5.2.	8.5.1 Change management plan 8.5.2 Change request 8.5.3 Impact analysis and change request plan 8.5.4 Change report
9 Verification	The objective of verification is to ensure that the work products comply with their requirements.	See applicable prerequisites of the relevant phases of the safety lifecycle in which verification is planned or carried out.	9.5.1 Verification plan 9.5.2 Verification specification 9.5.3 Verification report
10 Documentation	The primary objective is to develop a documentation management strategy for the entire safety lifecycle in order to facilitate an effective and repeatable documentation management process.	Safety plan in accordance with ISO 26262-2:2011, 6.5.1.	10.5.1 Document management plan 10.5.2 Documentation guideline requirements

Table A.1 (*continued*)

Clause	Objectives	Prerequisites	Work products
11 Confidence in the use of software tools	The first objective of this clause is to provide criteria to determine the required level of confidence in a software tool when applicable. The second objective of this clause is 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 tailor the activities or tasks required by ISO 26262 (i.e. the user can rely on the correct functioning of a software tool for those activities or tasks required by ISO 26262).	Safety plan (see ISO 26262-4, 5.5.2). Applicable prerequisites of the phases of the safety lifecycle where a software tool is used.	11.5.1 Software tool criteria evaluation report 11.5.2 Software tool qualification report
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 ISO 26262.	Requirements of the software component.	12.5.1 Software component documentation 12.5.2 Software component qualification report 12.5.3 Safety plan (refined)
13 Qualification of hardware components	The first objective of the qualification of hardware components is to provide evidence of the suitability of intermediate level hardware components and parts for their use as part of items, systems or elements, developed in compliance with ISO 26262, concerning their functional behaviour and their operational limitations for the purposes of the safety concept. The second objective of the qualification of hardware components is to provide relevant information regarding their failure modes, their failure mode distribution, and their diagnostic capability with respect to the safety concept for the item.	Related safety requirements. Qualification criteria (analysis and tests) in accordance with ISO 26262-5:2011, Clause 6); and manufacturer's hardware component specification, or, if unavailable, the assumptions on hardware component specification.	13.5.1 Qualification plan 13.5.2 Hardware component test plan 13.5.3 Qualification report
14 Proven in use argument	This clause provides guidance for a proven in use argument. A proven in use argument is an alternate means of compliance with ISO 26262 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 (from external source).	14.5.1 Safety Plan (refined) 14.5.2 Definition of a candidate for proven in use argument 14.5.3 Proven in use analysis reports

Annex B
(informative)

DIA example

B.1 Purpose

This annex provides an illustrative example of a development interface agreement (DIA), in accordance with the requirements of Clause 5 [especially 5.4.3.1 c) to g)], with organization-specific adaptation under the requirements and recommendations of ISO 26262-2, 5.4.5 and 5.5.1, if any. Project specific tailoring, in accordance with ISO 26262-2, 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.

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

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

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

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

    5) 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 26262-2:2011, 5.4.2); — evidence of competence (ISO 26262-2:2011, 5.4.3; — evidence of quality management (ISO 26262-2:2011, 5.4.4); — ISO 26262 Consent, e.g.: — independent assessment (5.4.5); — DIA template	—
A.2		—	Acceptance of conditions[a]
A.3		—	Capability assessment[a] (ISO 26262-2:2011, 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 26262-2:2011, 5.4.5 incl. methods, languages, tools & usage constraints/guidelines.	—
		—	1st 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	Invite proposal 5.4.2.2	RFP/RFQ, including project-specific tailored process [5.4.3.1 b)], product concept i.e. item definition (ISO 26262-3:2011, 5.5) and safety goals (ISO 26262-3:2011, 7.5.2).	—
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.9		—	Selected project resources and their capability assessment, e.g. safety team members' skills, competencies and qualification (ISO 26262-2:2011, 5.5.2); Organization-specific rules and processes (ISO 26262-2:2011, 5.5.1), incl. tools, libraries; Preliminary plans, e.g. safety plan (ISO 26262-2:2011, 6.5.1)
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 26262-4:2011, Clause 5) 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 26262-3:2011, Clauses 5 to 8)	System level plans Item definition (ISO 26262-3:2011, 5.5) and its lifecycle (Figure 1, ISO 26262-2:2011, 5.2.2; ISO 26262-2:2011, Figure 2 and ISO 26262-2:2011, 6.4.5) Functional safety concept (ISO 26262-3:2011, Clause 8)	—
B.2	—	—	Project plan (5.5.3) Safety plan (5.5.4) H&R analysis (5.4.3.2), hardware component behaviour models, incl. fault metrics [5.4.3.1 f), ISO 26262-5:2011, Annex B, and ISO 26262-5:2011, 9.4.3.1]. 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 c) e), g), 5.4.5]
B.3	—	Acceptance	—
B.4	Consideration of experience gained from proven in use components, tools, libraries used in similar projects (5.4.4.5), as well as proven in use data and analyses of possible candidates (ISO 26262-8:2011, Clause 14)	Initial safety plan (ISO 26262-2:2011, Clause 5), incl. system safety case structure	—
B.5	—	—	Proven in use elements offered (Clause 14), with independent assessment of fitness for the project (5.4.5 and ISO 26262-2:2011, Table 1)
B.6	—	Acceptance	—
B.7	System development lifecycle [5.4.3 b)]	Technical safety concept (ISO 26262-4:2011, 7.5.1), relevant parts of system design specs, hardware specs, design & implementation (D&I) constraints, hardware-software Interface (HSI) specifications (ISO 26262-4:2011, 7.5.3).	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 26262-4:2011, 7.5.2, ISO 26262-4:2011, 7.5.5), hardware specifications (ISO 26262-5:2011, 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 (5.5.4 and ISO 26262-5:2011, 5.5.1), Project plan (5.5.3 and ISO 26262-5:2011, 5.5.2), item integration and testing plan (see ISO 26262-4:2011, 5.5.3), planning of DIA (5.4.3) etc. Independent reviews of conformance to planning (5.4.4.8 and 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 26262-5:2011, 7.5.1). Extension to Verification Plan[a] HSI change requests, if any (ISO 26262-5:2011, 10.5). Independent safety audit (5.4.4.8) Independent confirmation (5.4.5 and 5.5.5).
C.5	—	Acceptance. Authorisation to commence design.	—
C.6	Design (5.4.5, and ISO 26262-5)	—	Design specs (ISO 26262-5:2011, 7.5.1); implementation constraints, incl. architectural (ISO 26262-5:2011, Clause 8). Extension or modification to H&R analysis (ISO 26262-3:2011, Clause 7), if any. Extension to item integration and testing plan (ISO 26262-5:2011, 10.5). HSI change requests, if any (ISO 26262-5:2011, 10.5). Independent safety audit (5.4.4.8, 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 5.5.5).
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 5.5.5).
C.9	—	Acceptance	—
C.10	—	—	Prototype part Integrated verification (ISO 26262-5:2011, 10.5) Independent assessment (5.4.5).
C.11	—	Integrated evaluation (ISO 26262-4:2011, Clause 8). Change requests, if any.	—
C.12	—	—	Reviews & audits of processed changes Independent assessment (5.4.5, 5.5.5).
C.13	—	Acceptance	—
C.14	—	—	Sample for series production Independent assessment (5.4.5, 5.5.5).
C.15	—	Integrated evaluation (ISO 26262-4:2011, Clause 8) Change requests, if any.	—
C.16	—	—	Reviews & audits of processed changes Independent assessment (5.4.4, 5.4.5 and 5.5.5).
C.17	—	Authorisation for commencing production phase	—
C.18	—	—	Post-SOP reports (5.4.6 and 5.5.6 and ISO 26262-2:2011, 7.5).

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

Bibliography

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

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

[3] ISO/TS 16949, *Quality management systems — Particular requirements for the application of ISO 9001:2008 for automotive production and relevant service part organizations*

[4] ISO/IEC 15504 (all parts), *Information technology — Process assessment*

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

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

[7] CMMI, http://www.sei.cmu.edu/cmmi/

[8] German V-Model, http://www.v-modell-xt.de/

[9] AEC-Q100, *Stress Qualification For Integrated Circuits*

[10] AEC-Q200, *Stress Test Qualification For Passive Components*

ICS 43.040.10

Price based on 48 pages