DRAFT INTERNATIONAL STANDARD ISO/DIS 26262-8

ISO/TC **22**/SC **3** Secretariat: **DIN**

Voting begins on: **2009-07-08** Voting terminates on: **2009-12-08**

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION

Road vehicles — Functional safety —

Part 8: Supporting processes

Véhicules routiers — Sécurité fonctionnelle —

Partie 8: Processus d'appui

ICS 43.040.10

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

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

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

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

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

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

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

PDF disclaimer

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

Adobe is a trademark of Adobe Systems Incorporated.

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

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: system level*

— *Part 5: Product development: hardware level*

— *Part 6: Product development: software level*

— *Part 7: Production and operation*

— *Part 8: Supporting processes*

— *Part 9: ASIL-oriented and safety-oriented analyses*

— *Part 10: Guideline on ISO 26262*

Introduction

ISO 26262 is the adaptation of IEC 61508 to comply with needs specific to the application sector of E/E systems within road vehicles.

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

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

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

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

ISO 26262:

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

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

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

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

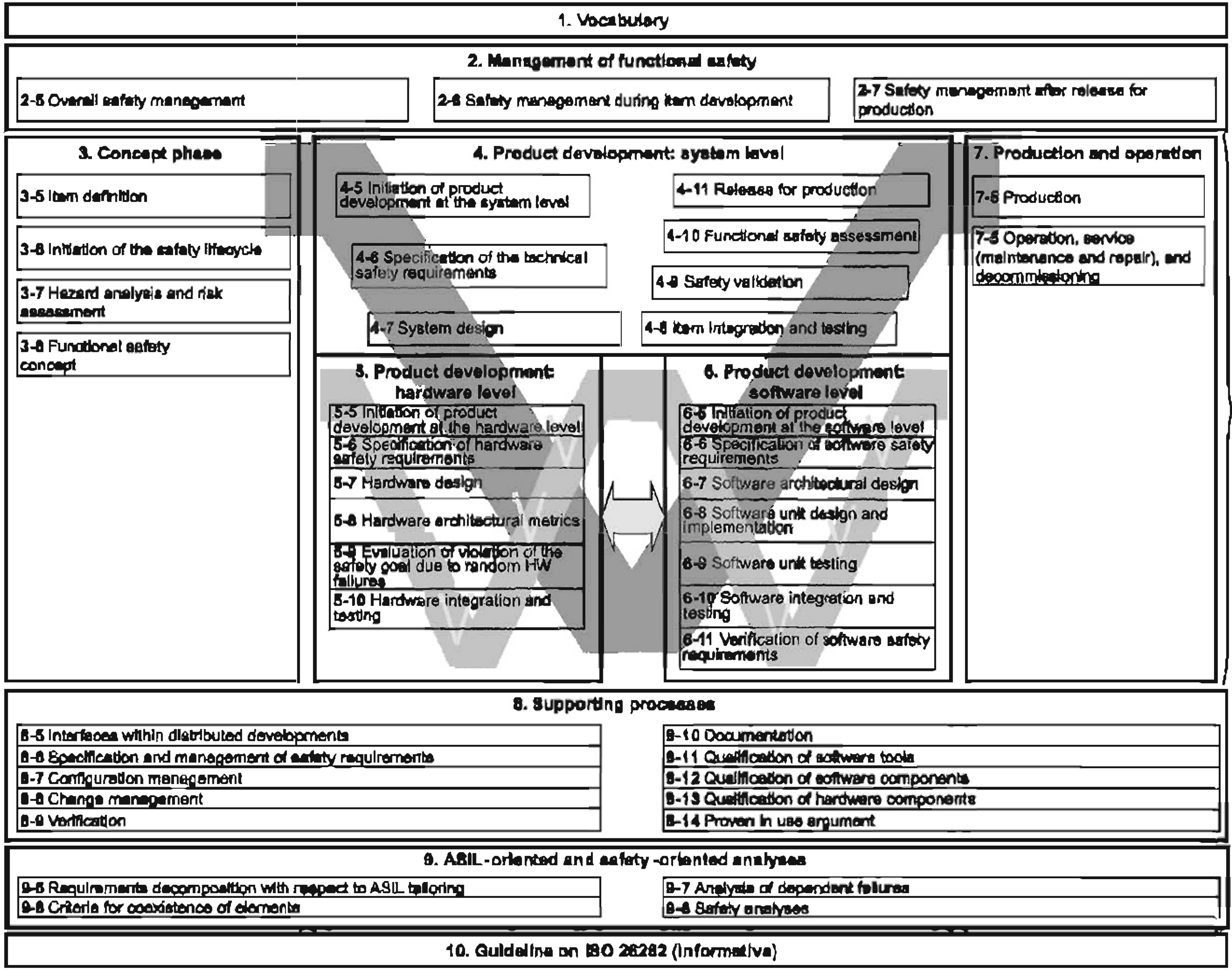
1. Vocabulary
2. Management of functional safety
2-5 Overall safety management
2-6 Safety management during item development
2-7 Safety management after release for production
3. Concept phase
3-5 Item definition
3-6 Initiation of the safety lifecycle
3-7 Hazard analysis and risk assessment
3-8 Functional safety concept
4. Product development: system level
4-5 Initiation of product development at the system level
4-6 Specification of the technical safety requirements
4-7 System design
4-8 Item integration and testing
4-9 Safety validation
4-10 Functional safety assessment
4-11 Release for production
5. Product development: hardware level
5-5 Initiation of product development at the hardware level
5-6 Specification of hardware safety requirements
5-7 Hardware design
5-8 Hardware architectural metrics
5-9 Evaluation of violation of the safety goal due to random HW failures
5-10 Hardware integration and testing
6. Product development: software level
6-5 Initiation of product development at the software level
6-6 Specification of software safety requirements
6-7 Software architectural design
6-8 Software unit design and implementation
6-9 Software unit testing
6-10 Software integration and testing
6-11 Verification of software safety requirements
7. Production and operation
7-5 Production
7-6 Operation, service (maintenance and repair), and decommissioning
Core processes
8. Supporting processes
8-5 Interfaces within distributed developments
8-6 Specification and management of safety requirements
8-7 Configuration management
8-8 Change management
8-9 Verification
8-10 Documentation
8-11 Qualification of software tools
8-12 Qualification of software components
8-13 Qualification of hardware components
8-14 Proven in use argument
9. ASIL-oriented and safety-oriented analyses
9-5 Requirements decomposition with respect to ASIL tailoring
9-6 Criteria for coexistence of elements
9-7 Analysis of dependent failures
9-8 Safety analyses
10. Guideline on ISO 26262 (informative)

Figure 1 — Overview of ISO 26262

DRAFT INTERNATIONAL STANDARD **ISO/DIS 26262-8**

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

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

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

This Part of the International Standard specifies the requirements for supporting processes. These include interfaces within distributed developments, overall management of safety requirements, configuration management, change management, verification, documentation, qualification 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 10007:2003, Quality management systems – Guidelines for configuration management

ISO 16949, *Quality management systems – Particular requirements for the application of ISO°9001:2000 for automotive production and relevant service part organizations*

ISO 26262-1: —[1] *Road vehicles – Functional Safety — Part 1: Vocabulary*

ISO 26262-2: —[1] *Road vehicles – Functional Safety — Part 2: Management of functional safety*

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

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

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

[1] To be published

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

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

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

3 Terms, definitions, abbreviated terms

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

4 Requirements for compliance

4.1 General requirements

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

1) Tailoring in accordance with ISO 26262-2 has been planned and shows that the requirement does not apply.

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

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

4.2 Interpretations of tables

Tables may be normative or informative depending on their context.

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

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

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

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

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

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

“+“ The method is recommended for this ASIL.

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

4.3 ASIL dependent requirements and recommendations

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

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

5 Interfaces within distributed developments

5.1 Objectives

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

5.2 General

The customer (e.g. vehicle manufacturer) and the suppliers for safety-related projects have to jointly use the procedures specified in ISO 26262. Responsibilities have to be 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 development projects, comparable procedures have to be agreed for co-operation with the supplier on distributed development projects, or development projects where the supplier has the full responsibility for safety.

This Clause is not relevant for 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 prerequisites of the relevant phases of the safety lifecycle for which the distributed development is carried out.

5.3.2 Further supporting information

The following information may be considered:

- Draft version of development interface agreement (from external source)
- Supplier's tender based on a request for quotation (from external source)

5.4 Requirements and recommendations

5.4.1 Application of requirements

5.4.1.1 Requirements of Clause 5 shall apply to each item developed according to ISO 26262, excepted off-the-shelf hardware parts if:

b) there are no specific hardware safety requirements allocated to these hardware parts; or

c) those 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

d) the qualification of 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 customer-supplier relationship.

NOTE 1 This includes subcontracts taken out by the top level supplier, subcontracts taken out by those subcontractors, and so on.

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

5.4.2 Supplier selection criteria

5.4.2.1 Supplier selection criteria shall include an evaluation of the supplier's capability to develop and produce items of comparable complexity and ASIL according to ISO 26262.

NOTE This includes:

- 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, 6.4.6.7
- 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 item; and

c) the safety goals and functional or technical safety requirements including their respective ASIL, if already available.

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

The customer and the supplier shall specify a development interface agreement (DIA) including:

a) the appointment of a safety manager at the customer's and the supplier's side;

b) the joint tailoring of the safety lifecycle according to ISO 26262-2, 6.4.3.4;

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 required and the work products of these activities 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. Documentation is compliant with Clause 10.

e) the parties or persons responsible for these activities;

f) the communication of the target values derived from the targets specified at the system level to each relevant party in order to fulfil the target values for single point faults metric and latent faults metric (see ISO 26262-5, Clause 8) and evaluation of violation of the safety goal due to random hardware failures (see ISO 26262-5, Clause 9);and

g) the supporting processes and tools including interfaces assuring compatibility between customer and supplier.

NOTE 2 An example DIA is given in Annex B.

5.4.3.1 In the case that the supplier conducts the hazard analysis and risk assessment, then the customer shall be able to review it.

5.4.3.2 The party responsible for the item shall derive 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 disclose, and report findings, concerning increasing risk of not conforming to the project plan, the safety plan, the verification plan, or other provisions of the DIA, to the customer.

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

5.4.4.2 The supplier shall report to the customer each safety-related event, occurring during the project activities in its area of responsibility or in that of its subcontractors.

5.4.4.3 The supplier shall determine if any safety requirement that cannot be complied with. In this case, the safety concept shall be checked and, if needed, modified to yield safety requirements that will be met.

5.4.4.4 Any change that could affect the safety of the item or planned measures to demonstrate compliance with ISO 26262 shall be communicated to the other party to support the impact analysis.

5.4.4.5 While developing the safety requirements for the current project, both parties should consider experience gained in similar projects.

5.4.4.6 The supplier shall report to the customer's safety manager the progress achieved according to the safety plan. The form of the report shall be agreed between the supplier and the customer.

5.4.4.7 Agreement shall be reached on which party (supplier or customer) shall perform the safety validation in accordance with ISO 26262-4, Clause 9 .

NOTE If the supplier performs the integration and validation, an agreement on the capabilities and resources needed by the supplier is important as validation requires the integrated vehicle (see ISO 26262-4, 9.4.2).

5.4.5 Safety assessment at supplier's premises

5.4.5.1 Safety assessments shall be carried out within each phase on reaching defined milestones. The level of detail of safety assessments shall depend on the complexity and the ASIL of the item and shall be performed according to ISO 26262-2, 6.4.6.

5.4.5.2 This subclause applies to ASILs A and B in accordance with 4.3.

A safety assessment of the work products should be carried out.

Note This can be done by the customer, another organisation or by the supplier itself.

5.4.5.3 This subclause applies to ASILs C and D in accordance with 4.3.

A safety assessment as defined in ISO 26262-2, 6.4.6.7 shall be carried out at the supplier's premises by the customer, or by an organisation or person designated by the customer.

Note This can be done by the customer, another organisation or by the supplier itself.

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

The assessment report shall be available at the customer's and at the supplier's premises.

5.4.5.5 This subclause applies to ASILs C and D in accordance with 4.3.

The supplier shall analyse the identified anomalies and derive actions to resolve them. An agreement between both parties shall be reached on who performs the actions required.

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

The customer may perform additional audits at the supplier's premises at any time if adequate.

5.4.6 After SOP

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

5.4.6.2 A supply agreement shall address the safety responsibilities in accordance with ISO 26262-2, 7.4.4 and safety-related actions between the customer and the supplier.

5.4.6.3 The supplier shall make available to the customer, on demand, the production monitoring records of the safety-related special characteristics.

5.4.6.4 Each party that acquires knowledge of a safety-related event shall report this in a timely manner. If safety-related event occurs, an analysis of that event and of similar items shall be performed. This should include each party 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 5.4.4.1.

5.5.4 **Supplier's safety plan** resulting from requirement 5.4.4.1.

5.5.5 **Safety assessment report** resulting from requirements 5.4.5.1, 5.3.5.2, 5.4.5.3, 5.4.5.4, 5.4.5.5 and 5.4.5.6.

5.5.6 **Supply agreement** resulting from requirement 5.4.6.2.

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 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 functional safety level.

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 components

The management of safety requirements includes managing requirements, obtaining agreement on the requirements, obtaining commitments with 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.

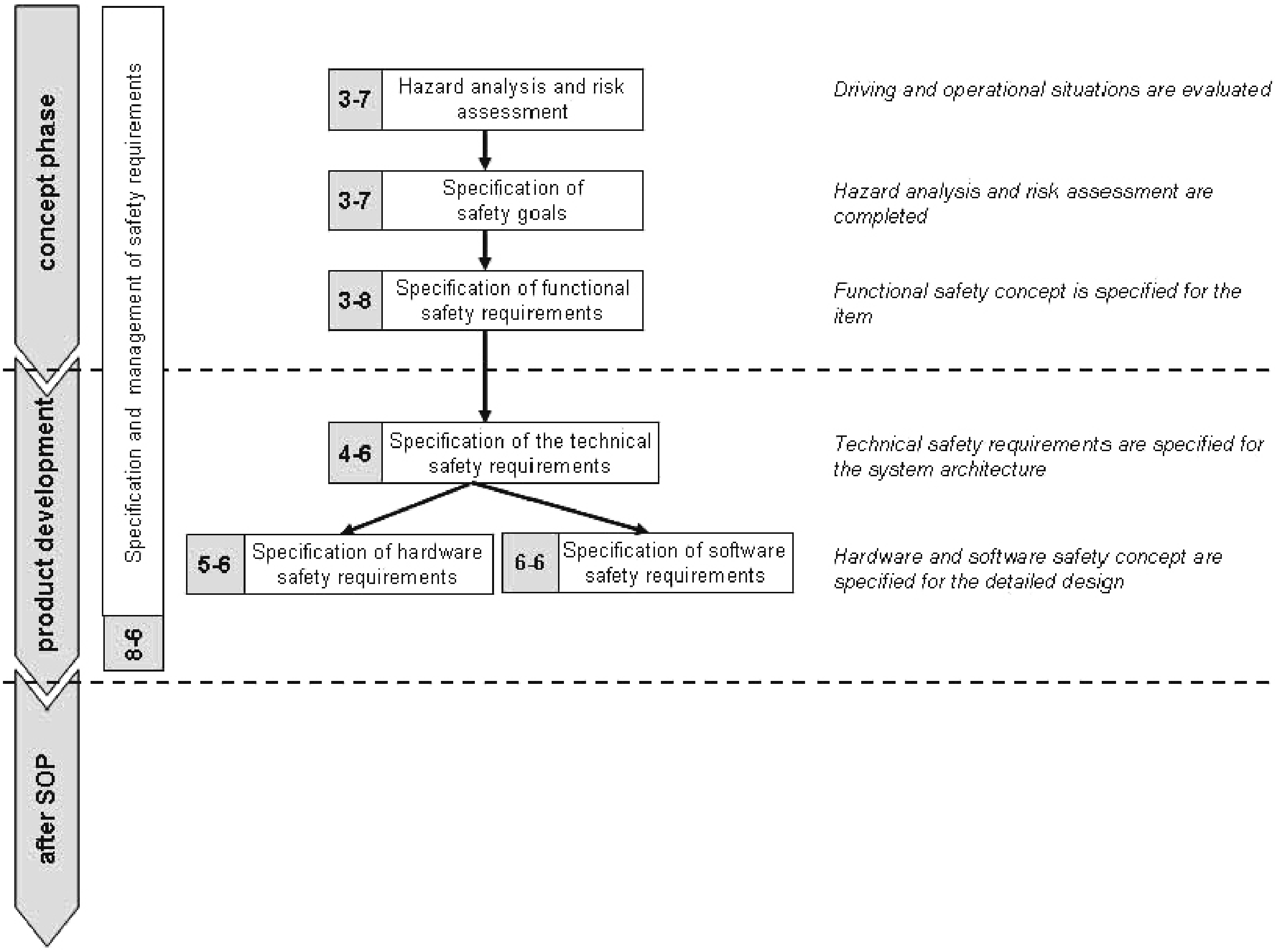
concept phase
product development
after SOP
Specification and management of safety requirements
8-6
3-7
Hazard analysis and risk assessment
3-7
Specification of safety goals
3-8
Specification of functional safety requirements
4-6
Specification of the technical safety requirements
5-6
Specification of hardware safety requirements
6-6
Specification of software safety requirements
Driving and operational situations are evaluated
Hazard analysis and risk assessment are completed
Functional safety concept is specified for the item
Technical safety requirements are specified for the system architecture
Hardware and software safety concept are specified for the detailed design

Figure 2 — Structuring of safety requirements

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 26262-2, ISO 26262-3, ISO 26262-4, ISO 26262-5 and ISO 26262-6.

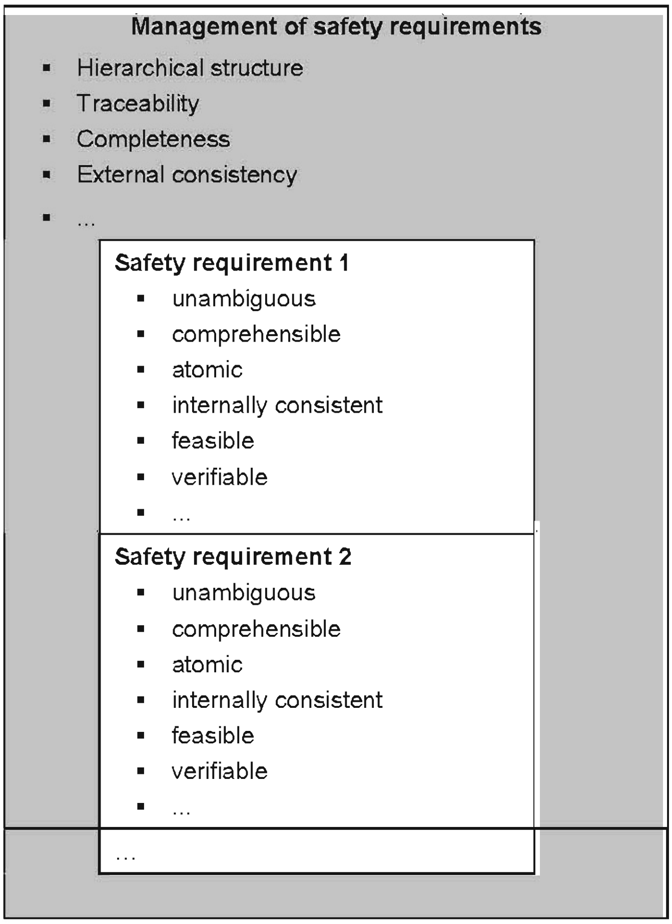

Figure 3 — Relationship between management of safety requirements and particular safety requirements

6.3 Inputs to this clause

6.3.1 Prerequisites

The following information shall be available:

— Safety plan (see ISO 26262-2, 6.5.1)

6.3.2 Further supporting information

None

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[a]	++	++	+	+
1b	Semi-formal notations for requirements specification[a]	+	+	++	++
1c	Formal notations for requirements specification[a]	+	+	+	+

[a] In the case of model-based development, safety requirements at each level need to be described with the same combination of methods used for the software safety 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 meet 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 a).

6.4.2.2 Safety requirements shall inherit the ASIL from the safety requirements from which they are derived.

NOTE As safety goals are the top level safety requirements the inheritance of ASILs starts at the safety goal level (see ISO 26262-1, 1.105).

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;

b) atomic;

NOTE 1 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 2 Consistency has two different aspects. External consistency means that the safety requirements do not contradict each other. Internal consistency means that a safety requirement itself contains no contradictions. In this case the internal consistency is addressed.

d) feasible; and

e) verifiable.

6.4.2.5 Safety requirements shall have the following attributes:

a) unique identification remaining unchanged throughout the safety lifecycle;

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

b) status; and

EXAMPLE 2 A status of a safety requirement may be *proposed, assumed, agreed,* or *reviewed*

c) ASIL.

6.4.3 Management of safety requirements

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

a) hierarchical structure;

NOTE 1 Hierarchical structure means that safety requirements are structured in several successive levels as presented in Figure 2. These levels are always allocated to corresponding design phases.

b) organizational structure according to an appropriate grouping scheme;

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

c) completeness;

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

d) external consistency;

NOTE 4 Consistency has two different aspects. External consistency means that the safety requirements do not contradict each other. Internal consistency means that a safety requirement itself contains no contradictions. In this case, the external consistency is addressed.

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

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

f) maintainability.

NOTE 6 Maintainability means that the requirements are modifiable or extendable.

6.4.3.2 Safety requirements shall be traceable with 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 (9.4.2).

NOTE Additionally, traceability supports:

— Impact analysis if changes are made to particular safety requirements; and

— The assessment of functional safety.

6.4.3.3 Safety requirements shall be verified to ensure compliance with the requirements in Clause 6.

6.4.3.4 Safety requirements shall be subject to configuration management in accordance with Clause 7.

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

6.5 Work products

6.5.1 Safety plan (refined) resulting from requirements in 6.4.2.1, 6.4.2.2, 6.4.2.3, 6.4.3.1 and 6.4.3.2.

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 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 is usually applied according to ISO TS 16949, 4.2.3, ISO 10007:2003.

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

7.3 Inputs to this clause

7.3.1 Prerequisites

None.

7.3.2 Further supporting information

The following information may be considered:

— Safety plan (see ISO 26262-2 6.5.1).

7.4 Requirements and recommendations

7.4.1 The configuration management process shall comply with the respective requirements of the quality management system such as ISO TS 16949, 4.2.3 or the respective requirement in ISO 9001, and with the requirements specific for software development according to ISO 12207, 6.2.

7.4.2 Work products listed in ISO 26262 shall be subject to configuration management and shall be identified, defined and baselined according to the configuration management strategy and that should be documented in the configuration management plan**.**

7.4.3 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 to 7.4.3.

8 Change management

8.1 Objectives

The objective of change management is the analysis and management of changes to safety-related work products occurring throughout the safety lifecycle.

8.2 General

Change management ensures the systematic planning, controlling, monitoring, implementing and documenting changes, while maintaining the consistency of each work product. Before changes are made, potential impacts on functional safety have first to be assessed. For this purpose, decision-making processes for change are introduced and established, and responsibilities assigned between the parties involved.

NOTE Here, change is understood as correction due to: anomalies, removals, additions, and enhancements.

8.3 Inputs to this clause

8.3.1 Prerequisites

The following information shall be available:

— Configuration management plan (see 7.5.1)

8.3.2 Further supporting information

The following information may be considered:

— Overall project plan (see ISO 26262-2, 6.5.2).

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.

NOTE As a minimum, the change management process is applied to each work product listed in ISO 26262 and subjected to configuration management

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

8.4.1.4 The change management process shall include:

a) change requests;

b) analysis of change requests;

c) decision regarding change requests; and

d) implementing and documenting the changes.

8.4.2 Change requests

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

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

a) date

b) reason for the requested change;

c) an exact description of the requested change; and

d) configuration on which it is based.

NOTE If a change request is submitted due to an error, the error is described along with the necessary conditions and the configuration under which the error occurred.

8.4.3 Analysis of the change requests

8.4.3.1 An impact analysis on the existing system and its interfaces and connected systems shall be carried out for each change request. The following points shall be addressed:

a) type of change request;

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

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

c) in case of a distributed development, the identification and involvement of parties affected;

d) the impact analysis of the functional safety change; and

e) the schedule for the realisation of the change.

8.4.3.2 Any changes to work products shall initiate the return to an applicable phase of the safety lifecycle. Subsequent phases shall be carried out in compliance with ISO 26262.

8.4.4 Deciding on a change request

8.4.4.1 The change request shall be evaluated on the basis of the impact analysis (see requirement 8.4.3.1) and a decision by authorized persons shall be made regarding acceptance, rejection or delay.

EXAMPLE Typically the authorised persons are:

- project manager;
- safety manager;
- person in charge of quality assurance; and
- developers involved.

NOTE It is recommended that accepted changes be prioritised and combined with change requests of a similar type .

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

8.4.5 Carrying out and documenting the change

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

8.4.5.2 Prior to release, if the change carried out has an impact on safety-related functions, the assessment of functional safety (see ISO 26262-2, 6.4.6) shall be updated.

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

a) changed work products at an appropriate level including configurations and versions, according to the configuration management strategy (see Clause 7) and documentation requirements (see Clause 10);

b) details of the performed change; and

c) planned date for the deployment of the change.

8.5 Work products

8.5.1 **Change management plan** resulting from requirements 8.4.1.1 to 8.4.1.4.

8.5.2 **Change request** resulting from requirements 8.4.2 and 8.4.4.

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

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

9 Verification

9.1 Objectives

The first objective of verification is to ensure that the work products are correct, complete and consistent.

The second objective of verification is to ensure that the work products meet the requirements of ISO 26262.

9.2 General

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

- in the concept phase, verification ensures that the concept is correct, complete and consistent to the boundary conditions of the system as well as the boundary conditions themselves and therefore the concept can be realised.
- In the development phase, verification is conducted in different forms:
  - 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 meet 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.

EXAMPLE Design phases are ISO 26262-4, Clause 7, ISO 26262-5, Clause 7, ISO 26262-6, Clause 7 and ISO 26262-6, Clause 8.

  - In the test phases, verification is the testing of the work products to ensure that they comply with their requirements by executing a work product in a test environment. The tests are planned, specified, executed, evaluated and documented in a systematic manner.

- In the production and operation phase, verification ensures that:
  - the safety requirements are appropriately transformed into a production process, user manuals or repair and maintenance instructions; and that
  - the safety-related properties of the item or product are met by using control measures.

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, Clause 9, for further details.

9.3 Inputs to this clause

9.3.1 Prerequisites

The following information shall be available:

- Safety plan (see ISO 26262-2, 6.5.1)

9.3.2 Further supporting information

None

9.4 Requirements and recommendations

9.4.1 Planning of verification

9.4.1.1 The planning of verification shall be carried out for each phase and subphase of the safety lifecycle including the following:

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

b) methods used for verification;

NOTE 1 Methods for verification include review, walkthrough, inspection, model-checking, simulation, engineering analyses, demonstration, and testing. Typically verification applies a combination of these and further methods.

c) the pass and fail criteria for the verification;

d) verification environment;

EXAMPLE A verification environment can be a test or simulation environment

e) tools used for verification;

NOTE 2 Software-tools for verification are qualified according to Clause 11.

f) actions to be taken if anomalies are detected; and

g) regression strategy.

NOTE 3 A regression strategy specifies how verification is repeated after changes have been made to the object. Verification can be repeated fully or partially and can include other objects 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) the prior experiences; and

NOTE This includes information noted in a service history as well as the degree to which proven in use argument is achieved.

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

9.4.2 Specification of verification

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

a) review or analysis checklists;

b) simulation scenarios; or

c) test cases and test data.

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

a) unique identification;

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

c) preconditions and configurations;

d) environmental conditions, if appropriate;

NOTE 1 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) input data, their time sequence and their values; and

f) expected behaviour which includes output data, output data of variable values boundaries as well as time behaviour and tolerance behaviour.

NOTE 2 When specifying the expected behaviour, it might be necessary to specify the initial output data in order to detect changes.

NOTE 3 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) test environment;

b) logical and temporal dependencies; and

c) resources.

9.4.3 Execution and evaluation of verification

9.4.3.1 The verification shall be executed as planned (see 9.4.1) and specified (see 9.4.2).

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

a) unique identification of the verified work product;

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

c) configuration of the verification environment and the verification tools together with the calibration data;

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

e) an unambiguous statement whether the verification passed or failed; including the rationale for failure and possible 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) 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 Specification of verification resulting from requirements 9.4.2.1, 9.4.2.2 and 9.4.2.3.

9.5.4 Verification report resulting from requirements 9.4.3.1 and 9.4.3.2.

10 Documentation

10.1 Objectives

The objective of the documentation is to develop a documentation management strategy, so that every phase of the entire safety lifecycle can be worked through effectively and can be reproduced.

10.2 General

The purpose of the documentation process is to develop and maintain a record of the information produced during the safety lifecycle.

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 expressively 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: in paper form, on data media, databases, etc.

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

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

10.3 Inputs to this clause

10.3.1 Prerequisites

None.

10.3.2 Further supporting information

The following information may be considered:

— Safety plan (see ISO 26262-2 6.5.1).

10.4 Requirements and recommendations

10.4.1 The documentation shall be made available as follows:

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) to carry out the assessment of functional safety.

10.4.2 The identification of a work product in ISO 26262 shall be interpreted as a requirement for documentation containing complete 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 together that contain the complete information for a work product.

10.4.3 The documents shall be:

a) precise and concise;

b) structured in a clear manner;

c) easy to understand by their intended audience; and

d) maintainable.

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

EXAMPLE Documentation tree

10.4.5 Each document shall contain 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, the date and a short description

e) the state.

EXAMPLE "draft", "released"

10.4.6 It shall be possible to identify the current revision (version) of a document or information.

10.5 Work products

10.5.1 Document management plan resulting from requirement 10.4.1.

10.5.2 Documentation requirements resulting from requirements 10.4.3 to 10.4.5

11 Qualification of software tools

11.1 Objectives

The objective of the qualification of software tools is to provide evidence of software tool suitability for use when developing a safety-related item or element, such that confidence can be achieved in the correct execution of activities and tasks required by ISO 26262.

11.2 General

The use of software tools simplifies or automates activities and tasks required for the development of a safety-related item or element by ISO 26262.

To determine the required level of confidence in a software tool, its use-cases are analysed. This analysis evaluates firstly that if a malfunctioning software tool and its erroneous output can lead to the violation of any safety requirement allocated to the safety-related item or element to be developed, and secondly that the probability of preventing or detecting such errors in its output. The evaluation considers measures internal to the software tool (e.g. monitoring) as well as measures external to the software tool implemented in the development process for the safety-related item or element (e.g. guidelines, tests, reviews).

The required confidence level together with the ASIL of the safety-related item or element that is to be developed using the software tool, allows the selection of the appropriate qualification methods. If the qualification requirements can already be demonstrated for a given software tool no further qualification activities are needed, otherwise the appropriate qualification methods need to be applied.

11.3 Inputs to this clause

11.3.1 Prerequisites

The following information shall be available:

- Pre-determined maximum ASIL
- Safety plan (see ISO 26262-4, 5.5.2)
- Validation plan (see ISO 26262-4, 5.5.3)
- Prerequisites of the phases of the safety lifecycle where qualification of software tools is applied and the related work products.

11.3.2 Further supporting information

The following information may be considered:

- 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

11.4.1.1 If the classification or qualification of a software tool is performed independently from the development of a particular safety-related item or element, the validity of its classification or qualification shall be confirmed prior to the software tool being used for the development of a particular safety-related item or element.

NOTE Typically, the qualification of software tools is a cross-organisational activity. This facilitates the collection of information about the software tool and thus the qualification itself.

11.4.1.2 Before using a qualified software tool, it shall be evaluated that its use-cases, determined environmental or functional constraints and general conditions are maintained.

EXAMPLE Use of the identical version and configuration settings as documented in its qualification report, for the same use-cases with the same measures for the detection of malfunctions or erroneous output.

11.4.2 Planning of qualification of a software tool

11.4.2.1 The planning of qualification of a software tool shall determine the following:

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

EXAMPLE commercial tools, freeware tools, shareware tools or tools developed in-house by the user.

b) configuration of the software tool;

EXAMPLE The configuration of a compiler is defined by setting compiler switches and "#pragma" statements in the source text.

c) use-cases of the software tool;

d) environment in which the software tool is executed;

e) the pre-defined maximum ASIL of any safety requirement which might be violated if the software tool is malfunctioning or producing erroneous output; and

NOTE Instead of an assumed pre-defined maximum ASIL, the specific maximum ASIL of a particular safety-related item or element to be developed can be used.

f) methods to qualify the software tool according to Tables 2, 3 and 4.

11.4.2.2 To ensure the proper usage, correct classification and qualification of the software tool, the following information shall be available:

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

b) description of the installation process for the software tool;

c) the user manual;

d) description of the environment required for its operation;

e) description of the expected behaviour of the software tool under anomalous operating conditions;

EXAMPLE 1 Anomalous operating conditions may 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 could suppress generation of an output or an user indication or report.

f) description of known software tool malfunctions and the appropriate safeguards, avoidance or work-around measures; and

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

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

g) determined measures for the detection of malfunctions or erroneous output of the software tool evaluated during the tool classification analysis.

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

EXAMPLE 5 comparison of outputs of redundant software tools, tests, static analyses, reviews or analyses of log-files.

11.4.3 Classification of a software tool

11.4.3.1 The description of the software tool use-cases used during the development of a safety-related item or element shall contain the following information:

a) intended purpose;

EXAMPLE 1 Simulation of a function, the generation of source code, or the test of embedded software, the automation of activities of ISO 26262

b) output; and

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

c) environmental and functional constraints.

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

11.4.3.2 The relevant software tool use-cases shall be analysed and evaluated to determine:

a) the possibility that a safety requirement, allocated to the safety-related item or element is violated if the software tool is malfunctioning or producing erroneous output, is expressed by the classes of classes of ***TI***:

— TI0 shall be chosen when there is an argument that there is no such possibility;

— TI1 shall be chosen in all other cases

NOTE 1 TI is an abbreviation for "Tool Impact"

b) the probability of preventing or detecting that the software tool is malfunctioning or producing erroneous output is expressed by the classes of ***TD***:

— TD1 shall be chosen if there is a high degree of confidence that a malfunction or an erroneous output from the software tool will be prevented or detected;

— TD2 shall be chosen if there is a medium degree of confidence that a malfunction or an erroneous output from the software tool will be prevented or detected;

- TD3 shall be chosen if there is a low degree of confidence that a malfunction or an erroneous output from the software tool will be prevented or detected; and

- TD4 shall be chosen in all other cases

NOTE 2 TD is an abbreviation for "Tool error Detection"

NOTE 3 TD4 typically applies if there are no systematic verification measures in the subsequent development phases available and therefore malfunctions or erroneous outputs of the considered software tool can only be detected randomly.

NOTE 4 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 5 The level of detail for such a use case analysis only needs to permit the proper determination of both of the classes of TI and TD.

11.4.3.3 If the correct selection of the classes of TI or TD is unclear or doubtful, TI and TD shall be estimated conservatively.

11.4.3.4 Based on the values determined to the classes of TI and TD (see 11.4.3.2 or 11.4.3.3) the required software tool confidence level shall be determined according to the following list:

- TCL1 shall be selected for TI0;

- TCL1 shall be selected for TI1 and TD1;

- TCL2 shall be selected for TI1 and TD2;

- TCL3 shall be selected for TI1 and TD3; and

- TCL4 shall be selected in all other cases

NOTE 1 TCL is an abbreviation for "Tool Confidence Level", with TCL 4 being the highest level of confidence required and TCL1 being the lowest level of confidence required.

NOTE 2 The resulting confidence level TCL of a software tool B used for verification purposes might be similar or higher than that of software-generating tool A (e.g. code generator) in a development process. When tool B is used to increase the TD for possible errors in the output of software tool A and as a result lowers the required confidence level TCL and qualification needs of this software tool A.

11.4.4 Qualification of a software tool

11.4.4.1 A software tool classified at TCL1 needs no qualification measures..

11.4.4.2 To demonstrate that a software tool classified at TCL2, TCL3 or TCL4 fulfils its use cases with the required level of confidence, methods for the qualification of software tools as listed in Table 2, Table 3 and Table 4 shall be applied.

Table 2 — Qualification of software tools classified TCL4

Methods		ASIL			
		A	B	C	D
1a	Increased confidence from use	++	++	+	o
1b	Evaluation of the development process	++	++	++	+
1c	Validation of the software tool	+	+	++	++
1d	Development in compliance 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.

NOTE 1 Those methods may be used directly or in a suitable combination of the different qualification methods mentioned in 11.4.4. At least one of the chosen qualification methods shall be recommended as suitable up to the ASIL in question. A different combination of the methods is possible, but needs to be justified.

EXAMPLE 1 Development of the software tool according to ISO 26262, IEC 61508 or RTCA DO 178 B

Table 3 —Qualification of software tools classified TCL3

Methods		ASIL			
		A	B	C	D
1a	Increased confidence from use	++	++	++	+
1b	Evaluation of the development process	++	++	++	++
1c	Validation of the software tool	+	+	+	++
1d	Development in compliance 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.

NOTE 2 Those methods may be used directly or in a suitable combination of the different qualification methods mentioned in 11.4.4. At least one of the chosen qualification methods shall be recommended as suitable up to the ASIL in question. A different combination of the methods is possible, but needs to be justified.

EXAMPLE 2 Development of the software tool according to ISO 26262, IEC 61508 or RTCA DO 178 B

Table 4 — Qualification of software tools classified TCL2

Methods		ASIL			
		A	B	C	D
1a	Increased confidence from use	++	++	++	++
1b	Evaluation of the development process	++	++	++	++
1c	Validation of the software tool	+	+	+	+
1d	Development in compliance 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.

NOTE 3 Those methods may be used directly or in a suitable combination of the different qualification methods mentioned in 11.4.4. At least one of the chosen qualification methods shall be recommended as suitable up to the ASIL in question. A different combination of the methods is possible, but needs to be justified.

EXAMPLE 3 Development of the software tool according to ISO 26262, IEC 61508 or RTCA DO 178 B

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

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

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

c) the pre-determined maximum ASIL, or specific ASIL, of any safety requirement which might be violated if the software tools is malfunctioning or producing erroneous output.

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

e) person or organisation who carried out the qualification;

f) the methods applied for qualification (see 11.4.4.2);

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

h) usage constraints and malfunctions identified during the qualification.

11.4.5 Increased confidence from use

11.4.5.1 A software tool shall only be characterised as having increased confidence from use, if there is evidence to demonstrate the following:

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

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

c) no violation of a safety requirement allocated to a previously developed safety-related item or element occurred as a consequence of malfunctions or erroneous outputs of this software tool. To create such evidence, data about the occurrence of malfunctions or of erroneous output of the software tool, observed or detected during previous developments shall be accumulated in a systematic way and made available.

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

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

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

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

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

c) documentation of malfunctions or erroneous output of the software tool with details of the conditions leading to it;

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

e) the safeguards, avoidance measures or work-arounds for the known malfunctions, or detection measures for a resulting erroneous output.

EXAMPLE 2 Sources for the usage report may be a log-book; the version history provided by the supplier of the software tool or published errata sheets

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

11.4.6 Evaluation of the development process

11.4.6.1 The development process applied for the development of the software tool shall comply with an appropriate national or international standard.

11.4.6.2 The evaluation of the development process applied for the development of the software tool shall be provided by an assessment.

NOTE This assessment covers the development of an adequate subset of the features of the software tool.

EXAMPLE Using an assessment method according to Automotive SPICE, CMMI or ISO 15504

11.4.7 Validation of the software tool

The validation of a software tool shall fulfil the following criteria:

a) the validation measures shall demonstrate that the software tool fulfils its specified requirements with the determined coverage of requirements;

EXAMPLE 1 A validation suite with test cases designed to achieve a determined functional and structural coverage

EXAMPLE 2 The standard for a programming language helps to define the requirements for validating the associated compiler.

b) the malfunctions or 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;

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

EXAMPLE 3 foreseeable misuse, incomplete update of the software tool, use of prohibited combinations of configuration settings

d) the robustness of the software tool shall be examined.

EXAMPLE 4 Tests based on complex or excessive inputs

NOTE Validation of the software tool can be automated largely by using a validation suite. The validation suite contains the tests determined to ensure correctness and robustness of the functionality that is later used for the development of a particular safety-related item or element.

11.4.8 Verification of qualification of software tools

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

The qualification of software tools shall be verified to ensure:

a) correct classification of the software tool; and

b) appropriate qualification of the software tool according to its classification.

11.5 Work products

11.5.1 Software tool classification analysis resulting from requirement 11.4.2 and 11.4.3.

11.5.2 Software tool qualification plan resulting from requirements 11.4.2 and 11.4.4.

11.5.3 Software tool documentation resulting from requirement 11.4.2.2.

11.5.4 Software tool qualification report resulting from requirements 11.4.3, 11.4.4, 11.4.5, 11.4.6, 11.4.7 and 11.4.8.

12 Qualification of software components

12.1 Objectives

The first objective of the qualification of software components is to enable the re-use of existing software components as part of items, systems or elements developed in compliance with ISO 26262 without completely re-engineering the software components.

The second objective of the qualification of software components is to show their suitability for re-use.

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 be software libraries from third-party suppliers (COTS), as well as in-house components already in use in electronic control units or generic components designed and developed for re-use across projects.

EXAMPLE Graphical libraries, mathematical libraries, operating systems, operating system services, databases, device driver software

12.3 Inputs to this clause

12.3.1 Prerequisites

The following information shall be available:

- Pre-determined maximum target ASIL

- Requirements of the software component.

12.3.2 Further supporting information

The following information may be considered:

- Results of previous verification measures of the software component.

12.4 Requirements and recommendations

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

a) specification of the software component (see 12.4.3.1);

b) evidence that the software component complies with its requirements (see 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 (see 12.4.4).

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

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

a) unique identification of the software component;

b) the pre-determined 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) requirements of the software component;

EXAMPLE 1:

- 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 case of failure;
- response time;
- resource usage;
- requirements on the runtime environment; and
- behaviour in an overload situation (robustness).

b) description of the configuration;

NOTE 1 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) interfaces description;

d) application manual;

e) description of the software component integration;

NOTE 2 Description might include the development tools required to integrate and use the software component;

f) reactions of the functions under anomalous operating conditions;

EXAMPLE 2 Re-entrant calling of non-re-entrant software component functions.

g) dependencies with other software components; and

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

12.4.3.2 To show that a software component complies with its requirements the verification of this software component shall meet the following criteria:

a) the verification shall show a requirement coverage in accordance with ISO 26262-6:—, Clause 9 for the maximum target ASIL;

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

EXAMPLE 1 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) The verification shall cover both normal operating conditions and behavior in case of failure;

c) The software component errors occurring during verification shall be analysed; together with information on their possible consequences and with measures to avoid or detect them.

EXAMPLE 2 Functional errors, runtime errors, incorrect timing, violation of data integrity, erroneous operating and resource usage

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:—, 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 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) unique identification and configuration of the software component;

b) person or organisation who carried out the qualification;

c) the environment used for qualification;

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

e) the pre-determined maximum target ASIL of any safety requirement which 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 may 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 planned 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 requirements 12.4.3.5.

12.5.3 Safety plan (refined), resulting from requirements 12.4.2

13 Qualification of hardware components

13.1 Objectives

The first objective of qualification of hardware components is to show 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.

The second objective of qualification of hardware components is to provide relevant information regarding their failure modes and their distribution, and their diagnostic capability with regard to the safety concept for the item.

13.2 General

Every component and part used within the scope of ISO 26262 has to be qualified to address general functional performance, conformity of production, environmental endurance and robustness.

EXAMPLE 1 Qualification in accordance with ISO 16750 or AEC Q 100, Q200 standards for electronic parts

For basic parts (passive component, discrete semiconductor), standard qualification is sufficient. These basic parts can then be used in a HW 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) etc.

Qualification as described in this clause aims at showing the suitability of the intermediate level HW components or parts for their use as elements of an item and showing that the failure modes are adequately identified for the purpose of the safety concept.

If the component does not contribute to any safety requirement by itself, qualification in accordance with this clause is sufficient.

If the component contributes to at least one safety requirement, and depending on its level, in addition to qualification in accordance with to this clause the component is integrated and tested in accordance with ISO 26262-4 or ISO 26262-5 or both .

Usually the qualification of hardware components or parts can be applied to components or parts whose failure modes or malfunctions are known and which are adequately testable regarding their possible defects.

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 an particular safety-related item with regard to functional performance of the sensor, its malfunctions and as long as 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 may be omitted and the integration activities may be carried out directly following ISO 26262-4 with regard to the technical safety requirements allocated to the sensor.

Table 5 — Qualification, integration and test activities to be conducted depending on the level of HW part or component

	Basic HW part		Intermediate HW part		Intermediate HW component		Complex HW component
	No contribution to a safety requirement	Contribution to a safety requirement	No contribution to a safety requirement	Contribution to a safety requirement	No contribution to a safety requirement	Contribution to a safety requirement	A safety requirement is fully implemented by the HW component
	(resistors, transistors…)		(HS CAN transceiver)	(gray code decoder)		(fuel pressure sensor)	(ECU)
Standard qualification	▨	▨	▨	▨			
Qualification in accordance with ISO26262-8:—, Clause 13			▨	▨	▨	▨	
Integration/test in accordance with ISO26262-5:—				*		▨ *	▨
Integration/test in accordance with ISO26262-4:—						▨	▨

* means that the HW element will be integrated in accordance with ISO 26262-4:— , or ISO 26262-5:—, or both ISO 26262-5:— and ISO 26262-4:— depending on "its level".

Qualification of hardware components or parts can be done using 2 different methods: testing or analysis. These methods can be used individually or in combinations depending on the hardware components.

- When testing, the hardware component is exposed to the same environmental and operational conditions it is intended for, and compliance with its functional requirements ought to be assessed. Reproducing exact environmental conditions is difficult and also any extrapolations are subject to error, therefore the limitations of such tests 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 procedures are used, the final results are available in a qualification report (which may 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 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) (see ISO 26262-5:—, Clause 6); and

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

13.3.2 Further supporting information

The following information may be considered:

— test criteria (see ISO 26262-5:—, 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

The following goals shall be achieved by the qualification of HW components:

a) ensure that the functional performance of components is adequate for the purposes of the safety concept;

b) identify failure modes and models (quantification of their distribution) by using appropriate tests (as Over limit test, accelerated test...) or analyses; and

c) ensure sufficient robustness and evaluate limitations of component use.

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

a) analyses

b) testing.

13.4.3 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 used;

c) the strategy of qualification and the rationale;

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

d) the criteria allowing to assess qualification of an element as passed or failed;

e) the necessary tools and equipment enabling this strategy; and

f) the party responsible or carrying out this strategy.

13.4.4 Qualification by analyses

13.4.4.1 A comprehensive argument that the performance of the hardware component achieves or exceeds its required performance 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.

13.4.4.2 Comprehensive evidence shall be made available and shall be based on a combination of the following types of information:

a) analytical methods and assumptions used;

b) data from operational experience; or

c) existing testing results.

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

13.4.4.4 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 and similar methods.

13.4.4.5 The analyses shall consider all the environmental conditions to which the hardware component 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).

13.4.5 Qualification by Testing

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

a) description of the functions of the hardware component;

NOTE For complex hardware components, a description of intended functions is sufficient.

b) number and sequence of tests to be conducted;

c) requirements for assembly and connections;

d) procedure for accelerated aging, considering the operating conditions of the hardware component;

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.

13.4.5.2 A standardised testing specifications shall be used, such as the ISO 16750 series or equivalent company standards.

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

13.4.6 Qualification report

13.4.6.1 The qualification report shall state whether the hardware component 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, notes on interpretation etc.

13.4.6.2 The qualification report shall be verified.

13.5 Work products

13.5.1 Qualification plan resulting from requirement 13.4.3.

13.5.2 Hardware component testing plan if applicable, resulting from requirement 13.4.5.1.

13.5.3 Qualification report resulting from requirements 13.4.6.1.

14 Proven in use argument

14.1 Objectives

The objective of this clause is to provide guidance for proven in use argument. Proven in use argument is an alternate means of compliance with ISO 26262 requirements that may be used in 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 does not mean 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, may be a candidate for 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 argument for proven in use includes:

- automotive application in commercial use intended to be partly or completely carried over for another target; or
- ECU in operation intended to implement an additional function; or
- candidate being in the field prior to the release of ISO 26262; or
- candidate being used in other safety-related industries; or
- candidate being a widely spread 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 control 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 may have impacted the candidate since its previous use taken for reference of service period (see 14.4.4).

NOTE 2 With regard to the relevance of field data, 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 the item or element from project-dependent safety management activities: proven in use credit is described in the safety plan and data and work products resulting from 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:

a) 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.

b) regarding the previous use of a candidate:

- field data from service period (from external source).

14.3.2 Further supporting information

The following information may be considered:

a) regarding the previous use of a candidate:

- Safety case (see ISO 26262-2, 6.5.3).

NOTE For a candidate not developed according to ISO 26262 (e.g. COTS products, candidates developed under a safety standard other than ISO 26262 such as IEC61508 or RTCA DO178), some work products of the safety case might not be available. In such a case, they are substituted by available data resulting from the development of the candidate.

14.4 Requirements and recommendations

14.4.1 General

The following requirements refer to the ASIL 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 given as the result of a proven in use argument only when the candidate complies with the requirements 14.4.2 to 14.4.5.

14.4.2.2 The expected proven in use credit resulting from a proven in use argument shall be stated according to ISO 26262-2, 6.4.3.

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 according to ISO 26262-4, Clause 8 at the appropriate level.

EXAMPLE In case of an hardware ECU, with a satisfactory service history, that is intended to be 100% carried over for a new type of application, the measures for the development of this hardware element can be substituted by the proven in use argument. However, the measures for developing the application software still need to be applied because software is out of the scope of the proven in use credit. Moreover, the measures for hardware software integration, system and vehicle integration will also need to be applied for the same reason.

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

14.4.2.6 Confirmation measures of an item which embeds proven in use elements shall consider the proven in use arguments and related data according to ISO 26262-4, Clause 10.

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

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

14.4.3 Minimum information on candidate

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

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

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

c) the safety requirements of the candidate in the previous use and the assigned ASIL, if available.

14.4.4 Analysis of changes to the candidate

Changes to candidates and their environment introduced between the use taken for reference of service period and a future application shall be identified.

NOTE 1 Changes to candidates address design changes and implementation changes. Design changes can result from modification of requirements, functional 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 fault 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.

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 upgrading of the components interacting with it or located in its vicinity.

14.4.4.1 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, 6.4.2.

14.4.4.2 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 ISO 26262-8, Clause 8.

14.4.4.3 Changes to candidate independent from future application

Changes to a candidate introduced after its service period, independent of future applications, shall be shown not to invalidate the proven in use argument.

14.4.5 Analysis of field data

14.4.5.1 Configuration management and change control

It shall be shown that the candidate has been kept under configuration management and change control 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 ASIL is not yet assigned to the candidate, ASILD 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 according to 14.4.5.2.3.

14.4.5.2.3 The observation period of each specimen identical to the candidate and running in a vehicle shall exceed the average yearly vehicle's 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 the safety goal in accordance with Table 6 with a single sided lower confidence level of 70%.

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

Table 6 — Limits for observable incident rate

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

NOTE 2 The potential difference between the safety goal violation and the observable incident is considered.

NOTE 3 Table 7 gives an example of the required minimum service period without observable incident to 70% confidence:

Table 7 — Targets for minimum service period of candidate

ASIL	Minimum service period without observable incident
D	$1.2 \cdot 10^{9}$ h
C	$1.2 \cdot 10^{8}$ h
B	$1.2 \cdot 10^{8}$ h
A	$1.2 \cdot 10^{7}$ h

NOTE 4 If observable incidents are found in the collected data of the specimens the necessary minimum service period can be adjusted as follows:

$$\text{service period} = MTTF \cdot \frac{\chi^2_{1-CL;2f+2}}{2}$$

With:

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

MTTF mean time to failure = 1/failure rate

F the number of safety-related incidents

$\chi^2_{\alpha,\nu}$ the chi-squared distribution with error probability α and ν degrees of freedom

14.4.5.2.5 For the application of the proven in use credit to be anticipated, before a proven in use status is obtained (see 14.4.5.2.4), the candidate service period shall demonstrate compliance with the safety goal according to Table 8 with a single sided lower confidence level of 70%.

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

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

- to switch over the observable incident rate of table 6 for the candidate, or alternatively
- to provide evidence that the root cause of the observed incident is fully identified and eliminated according to ISO 26262 requirements, 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 demonstration 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 proven in use argument, for instance in the case of damage linked with fatigue.

NOTE Those measures 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.

NOTE Data collection can rely on the process described in ISO 26262-2, 7.4.5.

14.5 Work products

14.5.1 Proven in use credit resulting from requirement 14.4.2.

14.5.2 Definition of candidate for proven in use argument resulting from the requirements in 14.4.3.

14.5.3 Proven in use analysis reports resulting from the requirements in 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 — Supporting processes: overview

Clause	Title	Objectives	Prerequisites	Work products
5	Interfaces within distributed developments	The objective of this process is to describe the procedures and 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
6	Specification and management of safety requirements	The first objective is to ensure the correct specification of safety requirements with respect to attributes and characteristics. The second objective is to ensure consistent management of safety requirements throughout the entire safety lifecycle	Safety plan (see ISO 26262-2, 6.5.1)	6.5.1 Safety plan (refined)
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.	None	7.5.1 Configuration management plan.
8	Change management	The objective of change management is the analysis and management of changes to safety-related work products occurring throughout the safety lifecycle.	Configuration management plan (see 7.5.1)	8.5.1 Change management plan 8.5.2 Change request 8.5.3 Impact analysis and the change request plan 8.5.4 Change report .
9	Verification	The first objective of verification is to ensure that the work products are correct, complete and consistent. The second objective of verification is to ensure that the work products meet the requirements of ISO 26262.	Safety plan (see ISO 26262-2, 6.5.1)	9.5.1 Verification plan 9.5.2 Specification of verification 9.5.4 Verification report
10	Documentation	The objective of the documentation is to develop a documentation management strategy, so that every phase of the entire safety lifecycle can be worked through effectively and can be reproduced.	None	10.5.1 Document management plan 10.5.2 Documentation requirements

Clause	Title	Objectives	Prerequisites	Work products
11	Qualification of software tools	The objective of the qualification of software tools is to provide evidence of software tool suitability for use when developing a safety-related item or element, such that confidence can be achieved in the correct execution of activities and tasks required by ISO 26262	Pre-determined maximum ASIL Safety plan (see ISO 26262-4, 5.5.2) Validation plan (see ISO 26262-4, 5.5.3) Also refer to the Prerequisites of the phases of the safety lifecycle where qualification of software tools is applied and the related work products.	11.5.1 Software tool classification analysis 11.5.2 Software tool qualification plan 11.5.3 Software tool documentation 11.5.4 Software tool qualification report
12	Qualification of software components	The first objective of the qualification of software components is to enable the re-use of existing software components as part of items, systems or elements developed in compliance with ISO 26262 without completely re-engineering the software components. The second objective of the qualification of software components is to show their suitability for re-use.	Pre-determined maximum target ASIL 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 qualification of hardware components is to show 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. The second objective of qualification of hardware components is to provide relevant information regarding their failure modes and their distribution, and their diagnostic capability with regard to the safety concept for the item	Related safety requirements; Qualification criteria (analysis and tests) (see ISO 26262-5, Clause 6); and Manufacturer's hardware component specification, or, if unavailable, the assumptions on hardware component specification (from an external source)	13.5.1 Qualification plan 13.5.2 Hardware component testing plan 13.5.3 Qualification report
14	Proven in use argument	The objective of this clause is to provide guidance for proven in use argument. Proven in use argument is an alternate means of compliance with ISO 26262 requirements that may be used in 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 Proven in use credit 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

This Annex provides an illustrative example of a Development Interface Agreement (DIA), in accordance with the requirements of ISO 26262-8, Clause 5, especially Clauses 5.4.3 (c) to h)), with organisation-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, 6.4.3.4, and ISO 26262-2, 6.4.4.2 can also be applied.

B.1 General (DIA) (informative)

Many factors will affect the type and amount of customer-supplier interactions the example is simplified, based on an application scenario described in B.2 and a set of premises listed in B.3.

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

— Table B.1 approximately corresponds to the requirements of ISO 26262-8, 5.4.2, with some organisation-specific additions, intended to avoid or eliminate risk from a supplier with inadequate capability.

— Table B.2 approximately corresponds to the requirements of ISO 26262-8, 5.4.3, with some organisation-specific additions, intended to avoid or eliminate risk from improper understanding or definition of boundary of Component C and its interactions with its environment.

— Table B.3 approximately corresponds to the requirements of ISO 26262-8, 5.4.5, as applied to hardware Component C.

NOTE A multi-decimal number within parentheses refers to the corresponding ISO 26262 Clause. If the activity or data is organisation-specific and not required in ISO 26262, it is identified with the symbol [*].

B.2 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 comprising 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.3 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, modeling 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 [*] suppliers; project independent criteria; feeds into 5.4.2	Capability assessment questionnaire [*]: • Safety culture (ISO26262-2, 5.4.2); • Competence management (ISO26262-2, 5.4.3; • Quality management (ISO26262-2, 5.4.4); • ISO 26262 Consent e.g.: • Independent assessment (5.4.5); • Functional safety audit (5.4.5.6 and ISO 26262-2, Table 1); • DIA template	
A.2			Acceptance of conditions [*]
A.3			Capability assessment [*] (ISO26262-2, Clause 5) Disclosure [*] Corrective action proposed [*]
A.4		Evaluation: ASILs for which not qualified [*]	
A.5	Qualify suppliers (short-list) [*] 5.4.2	Customer-organisation-specific process adaptation of ISO 26262-2, 5.4.5 incl. methods, languages, tools & usage constraints/guidelines.	
			1st party assessment of compliance. Disclosure. [*] Track record (5.4.2.1). Corrective action proposed. [*] Alternative approach or proposal to meet objectives. [*]
		Iterative evaluation & enquiries about gaps and alternatives. [*]	Iterative revisions to plans and alternatives. [*]
		Evaluation: ASIL-s for which not qualified. [*]	
A.6	Invite proposal 5.4.2.2	RFP/RFQ, including project-specific tailored process (5.4.3 b)), product concept i.e. item definition (ISO26262-3, 5.5) and safety goals (ISO26262-3, 7.5.2).	

A.7			Offer;
			Statement of compliance;
			Updates to previously submitted information. [*]

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 (ISO26262-2, 5.5.2); Organization specific rules and processes (ISO26262-2, 5.5.1), incl. tools, libraries; Preliminary plans, e.g. Safety plan (ISO26262-2, 6.5.1); Confirmation plan (ISO26262-2, 6.5.5)
A.10		Iterative evaluation and enquiries, e.g. re skill gaps. [*]	Iterative revisions addressing OEM concerns. [*]
A.11		Acceptance of DIA. (5.5.2) Selection report (5.5.1)	Acceptance of DIA (5.5.2)
A.12		Contract for concept (ISO26262-3; ISO26262-4) and planning phase (ISO26262-4Clause 5) incl. statement of development work.	Acceptance.

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 (ISO26262-3 Clause 5 to 8)	System level plans Item definition (ISO26262-3, 5.5) and its lifecycle (Figure 1, ISO26262-2, 5.2.2; ISO 26262-2 Figure 2 and ISO 26262, 6.4.3.4)) Functional safety concept (ISO26262-3 Clause 8)	
B.2			Project plan (5.5.3) Safety plan (5.5.4) H&R analysis (5.4.3.1), hardware component behaviour models, incl. fault models (5.4.3 f, ISO26262-5 ANNEX B and ISO26262-5, 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, Clause°14)	Initial safety plan (ISO26262-2 Clasue 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 ISO26262-2 Table1)
B.6		Acceptance	
B.7	System development lifecycle (5.4.3 b))	Technical safety concept (7.5.1), relevant parts of system design specs, hardware specs, design & implementation (D&I) constraints, hardware-software Interface (HIS) specifications (7.5.6).	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 (ISO26262-4, 7.5.2, ISO26262-4, 7.5.5), hardware specifications (ISO26262-5, 7.5.1) relevant to Component C, HSI, allocation, etc.	Feedback about boundary between Component C & its environment.
B.9			Acceptance

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

ID	Activity	Data from Customer-to-Supplier	Data from Supplier-to-Customer
C.1	Plan (5.4.3)	Authorisation for hardware development	
C.2			Plans: Safety plan (5.5.3, and ISO°26262-5,5.5.1), Project plan (5.5.4, and ISO°26262-5,5.5.2), item integration and testing plan (see ISO°26262-4, 5.5.5), planning of DIA (5.4.3) etc. Independent reviews of conformance to planning (5.4.4.1 and 5.4.5)
C.3		Acceptance. Authorisation to commence requirements specification	
C.4	Requirements (5.4.5 and ISO26262-5)		hardware specifications - derived; refined; D&I constraints (ISO262625, 7.5.1). Extension to Verification Plan [*]. HSI change requests, if any (ISO26262-5, 6.5.4 and ISO26262-5, 10.5). Independent safety audit (5.4.5.6) 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, 7.5.1); implementation constraints, incl. architectural (ISO°26262-5, 8). Extension or modification to H&R analysis (ISO°26262-3, 7), if any. Extension to item integration and testing plan (ISO°26262-5-10.5). HSI change requests, if any (ISO°26262-5, 10.5). Independent safety audit (5.4.5.6, 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 OEM feedback and enquiries. Independent assessment (5.4.5 and 5.5.5).
C.8	4.4.5.1 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 (ISO26262-5, 10.5) Independent assessment (5.4.5)
C.11		Integrated evaluation (ISO°26262-4, 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, 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, 7.5)

Bibliography

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

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

[3] IEEE Std 830-1998, *IEEE Recommended Practice for Software Requirements Specifications*

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

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

[6] ISO 15504 (all parts), Information technology – Process assessment

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