DRAFT INTERNATIONAL STANDARD ISO/DIS 26262-4

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 4:
Product development: system level

Véhicules routiers — Sécurité fonctionnelle —

Partie 4: Développement du produit: niveau système

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.

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 26262-4 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.

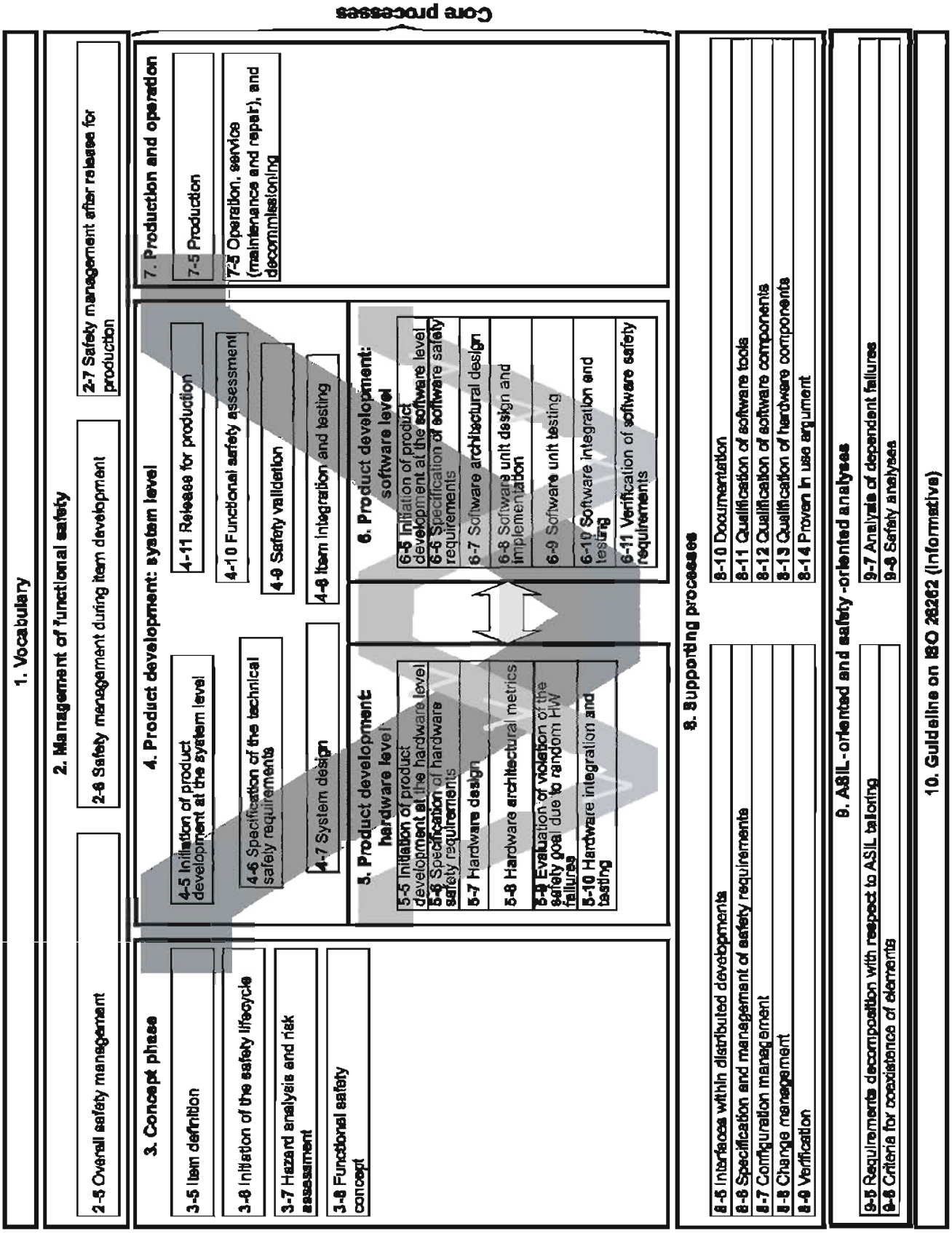

Figure 1 — Overview of ISO 26262

Road vehicles — Functional safety — Part 4: Product development: system level

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 ISO 26262 specifies the requirements on product development at the system level. These include requirements on the initiation of product development at the system level, the specification of the technical safety requirements, the technical safety concept, system design, item integration and testing, safety validation, functional safety assessment and product release.

2 Normative references

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

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

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 26262-8: —[1] *Road vehicles – Functional Safety — Part 8: Supporting processes*

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

---

[1] To be published

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 Initiation of product development at the system level

5.1 Objectives

The objective of the initiation of the product development at the system level is to determine and plan the functional safety activities during the individual subphases of system development. This also includes the necessary supporting processes described in ISO 26262-8.

This planning of system-level safety activities is included in the safety plan.

5.2 General

The necessary activities during the development of a system are given in Figure 2. After the initiation of product development and specification of the technical safety requirements, the system design is performed. The work products of this subphase are the technical safety concept and the system design specification including the allocation of technical safety requirements to hardware and software, and, if applicable, requirements on other technologies. Depending on the complexity of the architecture the requirements for subsystems can be derived iteratively. After the development of the hardware and software elements they are integrated to form a system that is itself integrated into a vehicle. At the vehicle level of integration, validation is performed to provide evidence of functional safety with respect to the safety goals.

Parts 5 and 6 of ISO 26262 describe the development requirements for hardware and software. ISO 26262-4 applies both to development of systems and subsystems.

Figure 2 is an example of a system with multiple levels of integration, illustrating the application of ISO 26262-4, ISO 26262-5, and ISO 26262-6.

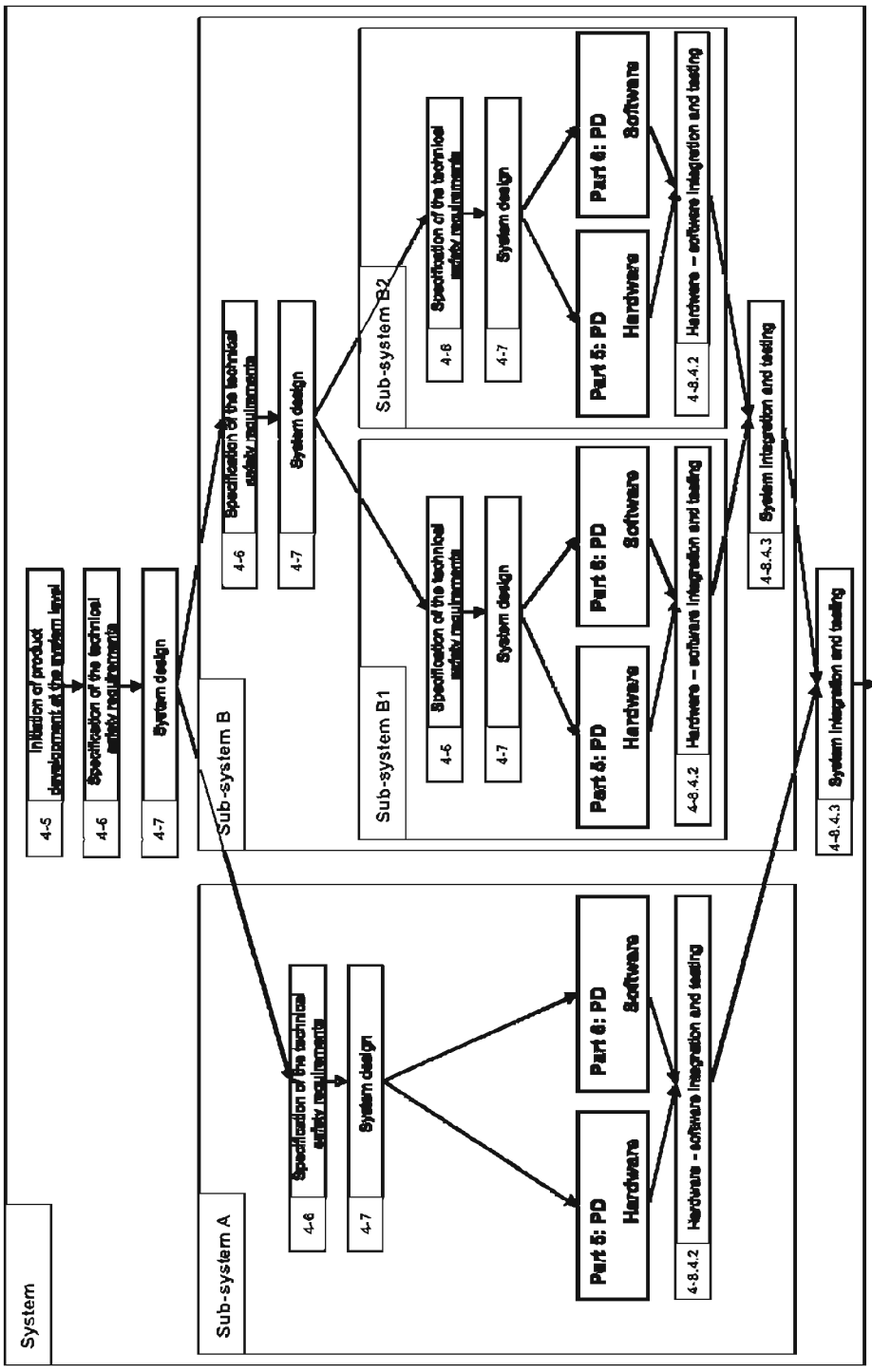

Figure 2 — Example of a product development at the system level

5.3 Inputs to this clause

5.3.1 Prerequisites

The following information shall be available:

— Functional safety concept (see ISO 26262-3: —, 8.5.1)

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

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

— Functional safety assessment plan (see ISO 26262-2: —, 6.5.6)

5.3.2 Further supporting information

The following information may be considered:

— Preliminary architectural assumptions (from external source, see ISO 26262-3: —, 8.3.2)

— Item definition (see ISO 26262-3: —, 5.5)

5.4 Requirements and recommendations

5.4.1 The safety activities for the product development at the system level shall be planned and detailed, including determination of appropriate methods and measures during design and integration. This task shall be completed previous to start of the associated subphase.

NOTE 1 The project plan and safety plan, as work products of ISO 26262-2 —, Clause 6, are updated and maintained.

NOTE 2 The results of planning of the verification activities during design in accordance with 6.4.12 and 7.4.11 are part of the safety plan while the planning of item integration and testing in accordance with 8.4.2, 8.4.3 and 8.4.4 is represented in a separate item integration and testing plan.

5.4.2 The validation activities shall be planned.

5.4.3 The functional safety assessment activities for the product development shall be planned and detailed (see also ISO 26262-2: —, 6.4.6).

NOTE An example of an agenda for the assessment of functional safety is provided in ISO 26262-2: —, Annex E.

5.4.4 The tailoring of the lifecycle (see ISO 26262-2: —, 5.4.5) at shall be based on the reference phase model given in Figure 3.

NOTE The project plan can be used to provide the relationship between the individual subphases of product development at the system level and the hardware and software development phases, including the integration steps at each level.

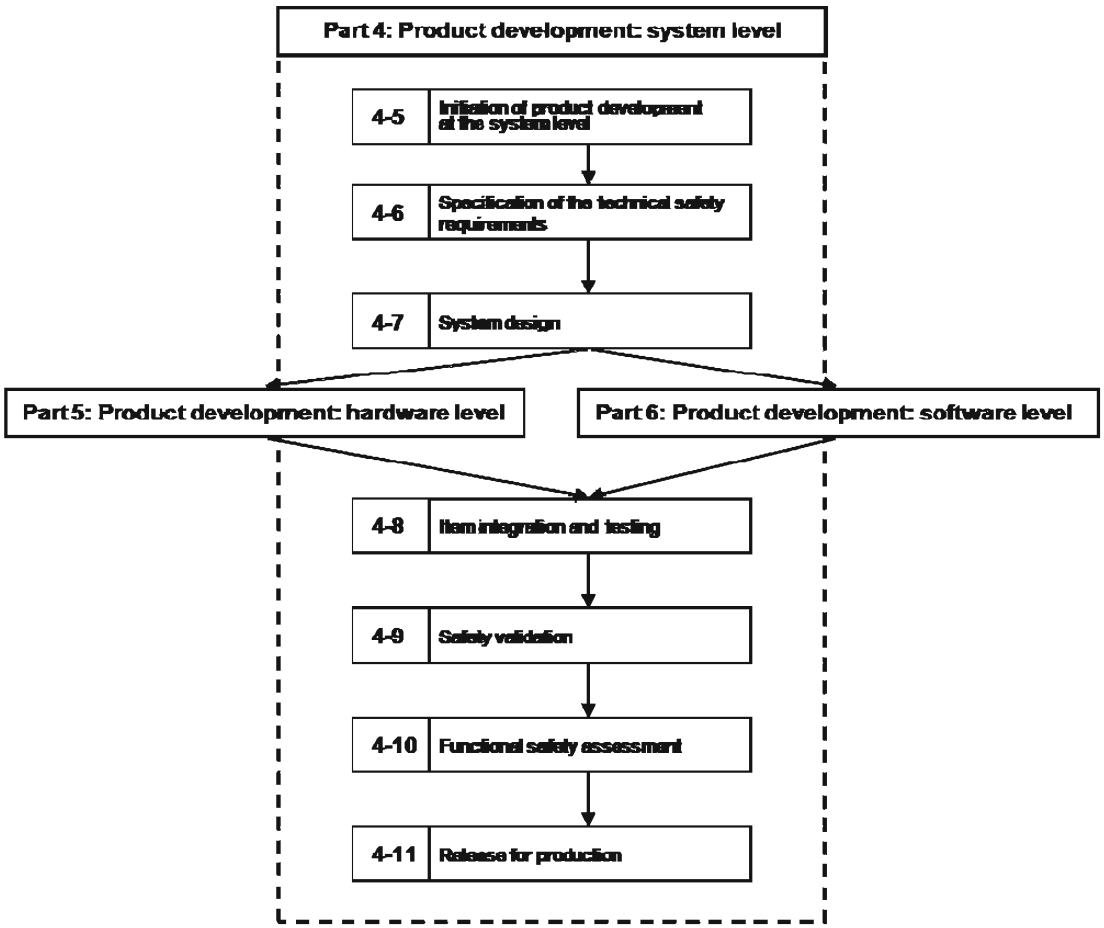

Figure 3 — Reference phase model for the development of a safety-related item

5.5 Work products

5.5.1 **Overall project plan (refined)** resulting from requirements 5.4.1

5.5.2 **Safety plan (refined)** resulting from requirements 5.4.1

5.5.3 **Validation plan** resulting from requirement 5.4.2

5.5.4 **Functional safety assessment plan (refined)** resulting from requirement 5.4.3

5.5.5 **Item integration and testing plan** resulting from requirement 5.4.1

6 Specification of the technical safety requirements

6.1 Objectives

The first objective of this subphase is to develop the technical safety requirements. The technical safety requirements specification refines the functional safety concept considering the functional concept and the preliminary architectural design (see ISO 26262-3).

The second objective is to verify through analysis that the technical safety requirements comply with the functional safety requirements.

6.2 General

Within the overall development lifecycle, the technical safety requirements describe how to implement the functional safety concept. It is intended to detail the item-level functional safety requirements into system-level technical safety requirements, down to the allocation to hardware and software elements.

6.3 Inputs to this clause

6.3.1 Prerequisites

The following information shall be available:

— Functional safety concept (see ISO 26262-3: —, 8.5.1)

— Validation plan (see 5.5.3)

6.3.2 Further supporting information

The following information may be considered:

— Safety goals (see ISO 26262-3: —, 7.5.2)

— Functional concept (from external source)

— Preliminary architectural assumptions (from external source, see ISO 26262-3: —, 8.3.2)

6.4 Requirements and recommendations

6.4.1 The technical safety requirements shall be specified in accordance with the functional safety requirements and the preliminary architectural assumptions of the item. The consistency of the preliminary architectural assumptions in ISO 26262-3: —, 8.3.2 and the preliminary architecture assumptions in this subphase shall be ensured.

6.4.2 In addition to the technical safety requirements, the system properties shall be defined in accordance with:

a) the external interfaces, such as communication and user interfaces, if applicable;

b) the constraints, e.g. environmental conditions or functional constraints;

NOTE 1 The consistency of documents concerning specification and constraints is ensured

c) the system configuration requirements.

NOTE 2 The ability to reconfigure a system for alternative applications is a well-known strategy to reuse existing systems, e.g. calibration data is frequently used to customise electronic engine control units for alternate vehicles.

6.4.3 The specification of the safety-related requirements concerning production, operation, maintenance, repair and decommissioning, addressed in ISO 26262-7, shall be initiated during this subphase.

NOTE There are two aspects for assuring safety during production, operation, maintenance, repair and decommissioning. The first aspect relates to those measures performed during the development phase which are given in requirements 6.4.3, and 7.4.7, while the second aspect relates to those measures performed during the production and operation phase, which are addressed in ISO 26262-7.

6.4.4 Other functional and non-functional requirements, in addition to those technical safety requirements specified in accordance with 6.4.1, and implemented by the system or in elements, shall be specified, or reference shall be made to their specification.

6.4.5 The response of the system or elements to stimuli, including failures, and relevant combinations of stimuli, shall be specified for each technical safety requirement in combination with each possible operating mode and defined system state.

6.4.6 The technical safety requirements shall specify safety-related functional and safety-related non-functional dependencies between systems or elements of the item and between the item and other systems.

EXAMPLE The Adaptive Cruise Control (ACC) ECU disables the ACC functionality if the brake system ECU signals that the Vehicle Stability Control functionality is unavailable.

6.4.7 The safety mechanisms shall be specified by technical safety requirements (see ISO 26262-8: —, Clause 6) including:

a) the measures related to the detection, indication and control of faults in the system itself (self-monitoring of the system or elements);

NOTE 1 This includes the self-monitoring of the system or elements to detect random hardware faults and, if appropriate, to detect systematic failures.

b) the measures related to the detection, indication and control of faults in external devices interacting with the system;

EXAMPLE External devices include other electronic control units, power supply or communication devices

c) the measures that enable the system to achieve or maintain a safe state;

NOTE 2 This includes prioritisation and arbitration logic in the case of conflicting safety mechanisms.

d) the measures to detail and implement the warning and degradation concept;

e) the measures which prevent faults from being latent (see 6.4.10)

NOTE 3 These measures are usually related to tests of measures a) to d) during power up (pre-drive checks), operation, power down (post-drive checks) and as part of maintenance.

6.4.8 Validation criteria concerning functional safety of the item shall be specified.

NOTE The system validation planning and the system validation specifications are developed in parallel to the technical safety requirements (see Clause 8).

6.4.9 For each safety mechanism that enables an item to achieve or maintain a safe state the following shall be specified:

a) the transition to the safe state, including the requirements to control the actuators ;

b) the fault-tolerant time interval;

c) the emergency operation interval if the safe state cannot be reached by immediately switching off;

d) the measures to maintain the safe state.

EXAMPLE A safety mechanism for a brake-by-wire application, which depends on the power supply, can include the specification of a secondary power supply or storage device (capacity, time to activate and operate, etc.)

6.4.10 Avoidance of latent faults

6.4.10.1 This subclause applies to ASILs (A), (B), C, and D, in accordance with 4.3: If applicable safety mechanisms shall be specified to prevent faults from being latent.

NOTE 1 Concerning random faults only multiple point faults carry the potential to include latent faults because single point faults either have to be controlled and indicated or have to lead to a safe state which will not be left in the event of a further fault.

NOTE 2 Such safety mechanisms include on-board tests, which verify the status of components during the different operation modes as power up, power down, at runtime or in an additional test mode.

Example Valve, relay or lamp function tests during power up routines

NOTE3 For ASIL A and B, the criteria are derived in accordance with sound engineering practice. For ASIL C and D the latent failure metric provides evaluation criteria.

6.4.10.2 The multiple point fault detection interval shall be specified to avoid multiple point failures. The following parameters should be considered:

a) the reliability of the hardware component;

b) the ASIL rating for the related safety goal and its corresponding parameter E "probability of exposure".

NOTE The use of the following measures depends on the time constrains:

— periodic testing of the system or elements during operation;

— on board tests of elements during power-up or power down;

— testing the system or elements during maintenance

6.4.10.3 Safety mechanisms which prevent dual point faults from being latent shall be developed in accordance with:

— ASIL B for ASIL D safety goals

— ASIL A for ASIL B and C safety goals

— engineering judgement for ASIL A safety goals

6.4.11 Newly identified hazards, not already reflected in a safety goal, shall be introduced and evaluated in the hazard analysis and risk assessment in accordance with the change management process in ISO 26262-8: —, Clause 8.

NOTE Newly identified hazards, not already reflected in a safety goal, are usually non-functional hazards. If those non-functional hazards are outside the scope of ISO 26262 then it is recommended that they are annotated in the hazard analysis and risk assessment with the following statement "No ASIL is assigned to this hazard as it is not within the scope of ISO 26262". However, an ASIL is allowed for reference purposes.

6.4.12 The technical safety requirements specification shall be verified through analysis to provide compliance with the functional safety concept and the preliminary architectural design (see ISO 26262-8: —, Clause 9).

6.5 Work products

6.5.1 Technical safety requirements specification resulting from requirements 6.4.1 to 6.4.10

6.5.2 Validation plan (refined) resulting from requirement 6.4.8.

6.5.3 System-level verification report resulting from requirement 6.4.12.

7 System design

7.1 Objectives

The first objective of this subphase is to develop the system design and the technical safety concept that comply with the functional requirements and the technical safety requirements specification of the item.

The second objective of this subphase is to verify that the system design and the technical safety concept comply with the technical safety requirements specification.

7.2 General

The development of the system design and the technical safety concept is based on the technical safety requirements specification derived from the functional safety concept. This subphase can be applied iteratively, if the system comprises subsystems.

7.3 Inputs to this clause

7.3.1 Prerequisites

The following information shall be available:

— Technical safety requirements specification (see 6.5.1)

— Item integration and testing plan (see 5.5.5)

7.3.2 Further supporting information

The following information may be considered:

— Preliminary architectural assumptions (from external source, see ISO 26262-3: —, 8.3.2)

— Functional concept (from external source)

— Functional safety concept (see ISO 26262-3: —, 8.5.1)

7.4 Requirements and recommendation

7.4.1 System design specification and technical safety concept

7.4.1.1 The system design shall be specified based on the functional concept, the preliminary architectural assumptions and the technical safety requirements specification. The consistency of the preliminary architectural assumptions in ISO 26262-3: —, 8.3.2 and the preliminary architecture assumptions in this subphase shall be ensured. The implementation of the technical safety requirements shall be specified in the technical safety concept and the system design specification.

7.4.1.2 The following shall be considered in the system design development:

a) the verifiability of the system design;

b) the effectiveness of the hardware and software development ;

c) the testability during system integration.

7.4.2 Architectural requirements

7.4.2.1 The architecture of each system or subsystem shall enable compliance with the technical safety requirements at their respective ASILs.

7.4.2.2 This subclause applies to ASILs (B), C, and D, in accordance with 4.3:

Any architectural element shall be treated as safety related unless:

— either the element is independent from the safety related elements of the item, or

— the implementation meets the criteria for coexistence, in accordance with ISO 26262-9: —, Clause 6.

7.4.2.3 If requirements with different ASILs are allocated to the same architectural element, this element shall be developed in compliance with the highest ASIL unless its implementation meets the criteria for coexistence, in accordance with ISO 26262-9**: —**, Clause 6.

7.4.2.4 Internal and external interfaces of safety-related elements shall be defined precisely, in order to avoid other elements having adverse safety-related effects on the safety-related elements.

7.4.2.5 If ASIL decomposition is applied, it shall be applied in accordance with ISO 26262-9**: —**, Clause 5.

7.4.3 Measures for the avoidance of systematic failures

7.4.3.1 Deductive and inductive analysis to identify causes and effects of systematic failures shall be applied in accordance with Table 1 and ISO 26262-9**: —**, Clause 8.

Table 1 — System design analysis

	Methods	ASIL			
		A	B	C	D
1	Deductive analysis[a]	o	+	++	++
2	Inductive analysis[b]	++	++	++	++
[a] Deductive analysis methods include FTA, reliability block diagrams.					
[b] Inductive analysis methods include FMEA, ETA, Markov modelling.					

NOTE 1 The purpose of these analyses is to assist in specifying the design. At this stage, qualitative analyses are likely to be appropriate and sufficient. Quantitative analyses can be performed if appropriate.

NOTE 2 The analysis is conducted at an appropriate level of detail.

7.4.3.2 Sources of systematic failures within the item itself that could contribute to the violation of a safety goal should be identified and avoided. If such failures cannot be completely avoided, their consequences shall be mitigated.

7.4.3.3 Sources of adverse safety effects on the item from other systems outside the item shall be identified and avoided or else their consequences shall be mitigated.

7.4.3.4 Use of well-trusted design principles

7.4.3.4.1 To reduce the likelihood of failures associated with new designs, well-trusted design principles for automotive systems should be applied. These include the following:

a) Re-use of well-trusted safety architecture;

b) Re-use of well-trusted design principles or designs for elements, hardware and software components;

c) Re-use of well-trusted mechanisms for the detection and control of failures;

d) Re-use of well-trusted or standardised interfaces.

7.4.3.4.2 Well trusted design principles or elements shall be analysed to ensure adequacy in the new application.

NOTE Adequacy includes diagnosis feasibilities, environmental constraints, time constraints, compatibility with available resources, robustness.

7.4.3.4.3 This requirement applies to ASIL D: A decision not to re-use well-trusted design principles should be justified.

7.4.3.5 In order to achieve an adequate level of granularity, and to avoid failures resulting from high complexity, the following modular design properties shall be achieved:

1) This requirement applies to ASILs (A), (B), C, and D, in accordance with 4.3: Hierarchical design

2) This requirement applies to ASILs (A), (B), C, and D, in accordance with 4.3: Avoidance of unnecessary complexity of HW components and SW components

3) This requirement applies to ASILs (A), B, C, and D, in accordance with 4.3: Avoidance of unnecessary complexity of interfaces

4) This requirement applies to ASILs (A), (B), (C), and (D), in accordance with 4.3: Maintainability during service

5) This requirement applies to ASILs (A), (B), C, and D, in accordance with 4.3: Testability

NOTE Testability includes testability during development and operation.

7.4.4 Measures for control of random hardware failures during operation

7.4.4.1 Measures for detection and control, or control, of random hardware failures shall be specified with respect to the system design.

EXAMPLE 1 Specification of diagnostics features of the hardware and their usage by the software to detect random hardware failures.

EXAMPLE 2 A hardware design which directly leads to the safe state in the case of a random hardware failure controls a failure even without detection.

7.4.4.2 This requirement applies to ASILs (B), C, and D, in accordance with 4.3**:** The target values for both metrics of ISO 26262-5: —, Clause 8, shall be specified for final evaluation at the item level (see also 9.4.3.4).

7.4.4.3 This requirement applies to ASILs (B), C, and D, in accordance with 4.3**:** One of the alternative procedures of ISO 26262-5: —, Clause 9 shall be chosen and the target values for final validation at item level (see also 9.4.3.4) shall be specified.

7.4.4.4 This requirement applies to ASILs (B), C, and D, in accordance with 4.3: Appropriate targets for failure rates and diagnostic coverage should be specified at element level in order to comply with the

target values of the metrics in ISO 26262-5: —, Clause 8 and the procedures in ISO 26262-5: —, Clause 9.

NOTE 1 Architectural constraint described in ISO 26262-5: —, Clause 8 are not directly applicable to COTS parts and components because suppliers usually can not foresee the usage of their products in the end-item and the potential safety implications. In such a case, basic data such as failure rate, failure modes, failure rate distribution per failure modes, built-in diagnosis, etc. are to be provided by the part supplier in order to allow estimation of architectural constraints at overall hardware architecture level.

NOTE 2 If a system contains different types of components with significantly different reliability levels, compliance with safety architectural metrics could only focus on the type of components with the highest magnitude of failure rates.. The prescription of appropriate metric target values for each kind of component helps to avoid this side effect.

EXAMPLE In the case of the Single Point Fault metric, the target values could be met with a safety mechanism controlling the failures of wire / fuses / connectors with poor reliability, whereas the failures of electronic components with higher reliability would not be controlled.

7.4.4.5 In the case of distributed developments (see ISO 26262-8: —, Clause 5), the derived target values shall be communicated to each relevant party.

7.4.5 Allocation to hardware and software

7.4.5.1 Every technical safety requirement shall be allocated to hardware, software or both, either directly or by further refinement.

NOTE To achieve independence and to avoid propagation of failures, the system design considers the partitioning of functions and components.

7.4.5.2 The system design specification shall include the results of the decisions concerning allocation and partitioning.

7.4.5.3 If technical safety requirements are allocated to custom hardware elements that incorporate programmable behaviour (such as ASICs, FPGA or other form of digital hardware) an adequate development process, combining requirements from ISO 26262-5 and ISO 26262-6, should be defined and implemented.

7.4.6 Hardware software interface specification (HSI)

7.4.6.1 The HSI shall be specified during system design and shall be detailed during hardware development (see ISO 26262-5: —, Clause 6 and Clause 7) and during software development (see ISO 26262-6: —, Clause 6).

7.4.6.2 The HSI requirements shall identify and detail each part of the HSI that is involved in a technical safety concept. It shall include hardware devices of the component that are controlled by software and hardware resources that support execution of software.

NOTE A list of examples of interfaces, aspects and characteristics detailed in the HSI is given in Annex B.

7.4.6.3 The HSI specification shall include the following characteristics:

a) the relevant operating modes of hardware devices and relevant configuration parameters;

EXAMPLE 1 Operating modes of hardware devices can be: default, init, test or advanced modes

EXAMPLE 2 Configuration parameters can be: gain control, band pass frequency or clock prescaler

b) the hardware features that ensure independence between elements and support software partitioning;

c) shared and exclusive use of hardware resources;

EXAMPLE 3 Memory mapping, allocation of registers, timers, interrupts I/O ports

d) the access mechanism to hardware devices;

EXAMPLE 4 Serial, parallel, slave, master/slave

e) the timing constraints defined for each service involved in the technical safety concept.

7.4.6.4 The relevant diagnostic capabilities of the hardware shall be specified and their use by the software shall be provided in the HSI specification.

a) the hardware diagnostic features shall be defined ;

EXAMPLE protection against over-current, short-circuit or over-temperature

b) the diagnostic features concerning the hardware to be implemented by the software shall be defined.

7.4.7 Requirements for production, operation, service and decommissioning

7.4.7.1 Appropriate measures to support field monitoring and to collect data shall be established. The extent of collected data shall be based on results of the safety analysis and the implemented safety mechanisms.

7.4.7.2 The system design should include the specification of diagnostic features to allow fault identification by workshop staff when servicing.

7.4.7.3 The requirements for production, operation, service and decommissioning identified during system design shall be specified (see ISO 26262-7). These include:

a) the requirements on assembly instructions;

b) the safety-related special characteristics;

c) the requirements dedicated to ensure proper identification of systems or elements;

EXAMPLE Labelling of elements

d) the verification measures for production;

e) the requirements on service including diagnostic data and service notes;

f) the requirements on decommissioning, such as decommissioning instructions.

7.4.8 Verification of system design

7.4.8.1 System design shall be verified for compliance and completeness with regard to the technical safety concept. In this aim, the methods and measures in Table 2 shall be considered.

Table 2 — System design verification

Methods		ASIL			
		A	B	C	D
1a	System design inspection[a]	+	++	++	++
1b	System design walkthrough[a]	++	+	o	o
2a	Simulation[b]	+	+	++	++
2b	System prototyping and vehicle tests[b]	+	+	++	++
3	Safety analyses[c]	see Table 1			

[a] Methods 1a and 1b serve as check of complete and correct detailing and implementation of the technical safety requirements into system design.

[b] Methods 2a and 2b can be used advantageously as a fault injection technique.

[c] For conducting safety analyses, see ISO 26262-9: —, Clause 8.

NOTE System design safety anomalies regarding the technical safety requirements are reported, in accordance with ISO 26262-2: —, 5.4.2.3.

7.4.8.2 An analysis of possible hazards, introduced by the system design, shall be carried out. Newly identified hazards not already reflected in a safety goal shall be introduced and evaluated in the hazard analysis and risk assessment in accordance with the change management process in ISO 26262-8: —, Clause 8.

NOTE Newly identified hazards, not already reflected in a safety goal, are usually non-functional hazards. If those non-functional hazards are outside the scope of ISO 26262 then it is recommended that they are annotated in the hazard analysis and risk assessment with the following statement "No ASIL is assigned to this hazard as it is not within the scope of ISO 26262". However, an ASIL is allowed for reference purpose.

7.4.9 Product development shall be continued at the hardware level as given in ISO 26262-5 and at the software level as given in ISO 26262-6.

7.4.10 After sufficient completion of hardware and software development in accordance with ISO 26262-5 and ISO 26262-6, the system integration in accordance with Clause 8 shall be started.

7.4.11 To enable the system integration subphase in accordance with Clause 8 the following shall be made available:

a) the item integration and testing plan at the system and vehicle level shall be detailed including specification of integration tests, thus ensuring that open issues from hardware and software verifications are included.

b) the item integration and testing plan at the system and vehicle level shall consider interfaces between vehicle sub-systems (internal and external concerning the item) and environment.

NOTE 1 The planning of integration and verification at the vehicle level might consider it sufficient to provide evidence of correct behaviour under vehicle typical conditions and environment, and to exclude extreme conditions (see Table 3).

NOTE 2 The planning of integration and testing at hardware software integration and item level needs to consider the interface and interaction between hardware and software

c) If the system uses configurations or calibration data the verification at the system or vehicle level shall provide evidence of compliance with safety requirements for each configuration at implementation level or for every configuration that is intended for serial production at a generic level.

7.5 Work products

7.5.1 Technical safety concept resulting from requirements 7.4.1 to 7.4.4 and 7.4.6.

7.5.2 System design specification resulting from requirements 7.4.1 to 7.4.4 and 7.4.6.

7.5.3 Requirements for production, operation, service and decommissioning resulting from requirements 7.4.7.1 to 7.4.7.3.

7.5.4 Item integration and testing plan (refined) resulting from requirement 7.4.11.

7.5.5 System-level verification report (refined) resulting from requirement 7.4.8.1.

7.5.6 Hardware Software Interface Specification (HSI) resulting from requirements 7.4.6.1 to 7.4.6.4.

8 Item integration and testing

8.1 Objectives

The first objective of the item integration and testing is to integrate the elements of an item and, if applicable, systems or elements of other technologies and external measures or systems step by step into the entire item. The integrated item is tested to comply with each safety requirement in accordance with its specification and ASIL classification.

The second objective of the item integration and testing is to verify that the "System design" (see Clause 7) is correctly implemented by the entire item.

8.2 General

The integration of the elements of an item is carried out in a systematic way starting from software-hardware integration and going through integration of systems up to vehicle integration. Specified integration tests are performed at each integration stage to provide evidence that the integrated elements interact correctly.

8.3 Inputs to this clause

8.3.1 Prerequisites

The following information shall be available:

— System design specification (see 7.5.2)

— Safety goals (see ISO 26262-3: —, 7.5.2)

— Functional safety concept (see ISO 26262-3: —, 8.5.1)

— Technical safety concept (see 7.5.1)

— Hardware Software Interface Specification (HSI) (see 7.5.6)

— Item integration and testing plan (refined) (see 7.5.4)

8.3.2 Further supporting information

The following information may be considered:

— Vehicle architecture (from external source)

— Technical safety concepts of other vehicle systems (from external source)

8.4 Requirements and recommendation

8.4.1 General requirements on integration and testing

8.4.1.1 Integration testing activities shall be performed in accordance with ISO 26262-8**: —**, Clause 9.

8.4.1.2 The aim of this phase is to verify, by integration tests, the fulfilment of functional and technical safety requirements.

8.4.1.3 An integration and test strategy shall be detailed based on the system design specification, functional safety concept and the item integration and testing plan.

8.4.1.4 Each functional and technical safety requirement shall be tested at least once in the complete integration phase. The test level shall be sufficiently representative.

NOTE 1 A common practice is to verify a safety requirement at a level of integration that is not the one at which it has been specified.

NOTE 2 Safety anomalies identified during integration testing are reported in accordance with ISO 26262-2: —, 5.4.2.3.

8.4.1.5 To ensure the appropriate specification of test cases for the selected item integration test methods, test cases shall be derived using an appropriate combination of methods listed in Table 3 considering the level of integration.

Table 3 — Methods for deriving test cases for item integration testing

Methods		ASIL			
		A	B	C	D
1a	Analysis of requirements	++	++	++	++
1b	Analysis of external and internal interfaces	+	++	++	++
1c	Generation and analysis of equivalence classes for hardware software integration	+	+	++	++
1d	Analysis of boundary values	+	+	++	++
1e	Knowledge or experience based error guessing	+	+	++	++
1f	Analysis of functional dependencies	+	+	++	++
1g	Analysis of common limit conditions, sequences, and sources of common cause	+	+	++	++
1h	Analysis of environmental conditions and operational use cases	+	++	++	++
1i	Analysis of field experience	+	++	++	++

8.4.2 Hardware-software integration and testing

8.4.2.1 This requirement applies to ASILs C, and D: The hardware-software interface (HSI) requirements, as described in Clause 7.4.6, shall be completely tested by hardware-software integration testing or a rationale shall be provided that no remaining issue of the HSI exists.

8.4.2.2 The hardware developed in accordance with ISO 26262-5 and the software developed in accordance with ISO 26262-6 shall be integrated to serve as the subject for the test activities in Tables 4 to 8.

NOTE The use of production-intent hardware and software is preferred. Modified hardware or software might be used where necessary for particular test techniques.

8.4.2.3 In order to detect systematic faults within the implementation of system design during hardware-software integration, the test goals resulting from the requirements 8.4.2.3.1 to 8.4.2.3.5 shall be addressed by application of adequate test methods as given in the corresponding tables.

NOTE Depending on the function implemented, and depending on the complexity or distributed nature of the system, it can be reasonable to move tests methods to other integration subphases provided that there is an adequate rationale.

8.4.2.3.1 The correct implementation of the system design specification and the technical safety requirements shall be ensured by applying feasible test methods given in Table 4.

Table 4 — Correctness of implementation of system design specification and technical safety requirements

Methods		ASIL			
		A	B	C	D
1a	Requirements-based test[a]	++	++	++	++
1b	Fault injection test[b]	+	++	++	++
1c	Back-to-back test[c]	+	+	++	++

[a] A requirements-based test denotes a test against functional and non-functional requirements.

[b] A fault injection test uses special means to introduce faults into the test object during runtime. This can be done within the software via a special test interface or specially prepared hardware. The method is often used to improve the test coverage of the safety requirements, because during normal operation safety mechanisms are not invoked.

[c] A back-to-back test compares the responses of the test object with the responses of a simulation model to the same stimuli, to detect differences between the behaviour of the model and its implementation.

8.4.2.3.2 The correct functional performance of the safety mechanisms including accuracy and timing shall be ensured by applying feasible test methods given in Table 5.

Table 5 — Correctness of functional performance of safety mechanisms

Methods		ASIL			
		A	B	C	D
1a	Back-to-back test[a]	+	+	++	++
1b	Performance test[b]	+	++	++	++

[a] A back-to-back test compares the responses of the test object with the responses of a simulation model to the same stimuli, to detect differences between the behaviour of the model and its implementation.

[b] A performance test can verify the performance concerning e.g. task scheme, timing, power output in the context of the whole test object, and can verify the ability of the hardware to run with the intended control software.

8.4.2.3.3 The consistency and correctness of the implementation of the external and internal interfaces shall be ensured by applying feasible test methods given in Table 6.

Table 6 — Consistency and correctness of implementation of external and internal interfaces

Methods		ASIL			
		A	B	C	D
1a	Test of external interfaces[a]	+	++	++	++
1b	Test of internal interfaces[a]	+	++	++	++
1c	Interface consistency check[a]	+	++	++	++

[a] Interfaces tests of the test object include tests of analogue and digital inputs and outputs, boundary tests and equivalent-class tests to completely test the specified interfaces, compatibility, timings and other specified ratings for the test object. Internal interfaces of an ECU are tested by static tests for the compatibility of software and hardware as well as dynamic tests of SPI- or I^2C-communications or any other interface between elements of an ECU.

8.4.2.3.4 The effectiveness of the diagnostic coverage of the hardware fault detection mechanisms, with respect to the fault models, shall be ensured by applying feasible test methods given in Table 7.

NOTE For references to fault models see ISO 26262-5: —, Annex D, Table D.1

Table 7 — Effectiveness of diagnostic coverage of hardware fault detection mechanisms

Methods		ASIL			
		A	B	C	D
1a	Fault injection test[a]	+	+	++	++
1b	Error guessing test[b]	+	+	++	++

[a] A fault injection test uses special means to introduce faults into the test object during runtime. This can be done within the software via a special test interface or specially prepared hardware. The method is often used to improve the test coverage of the safety requirements, because during normal operation safety mechanisms are not invoked.

[b] An error guessing test uses expert knowledge and data collected through lessons learned to anticipate errors in the test object. Then a set of tests along with adequate test facilities is designed to check for these errors. Error guessing is an effective method given a tester who has previous experience with similar test objects.

8.4.2.3.5 The level of robustness of the elements shall be ensured by applying feasible test methods given in Table 8.

Table 8 — Level of robustness

Methods		ASIL			
		A	B	C	D
1a	Resource usage test[a]	+	+	+	++
1b	Stress test[b]	+	+	+	++

[a] A resources usage test can be done statically e.g. by checking for code sizes or analyzing the code regarding interrupt usage, in order to verify that worst-case scenarios do not run out of resources, or dynamically by runtime monitoring.

[b] A stress test verifies the test object for correct operation under high operational loads or high demands from the environment. Therefore, tests under high loads on the test object, or with exceptional interface loads, or values (bus loads, electrical shocks etc.), as well as tests with extreme temperatures, humidity or mechanical shocks, can be applied.

8.4.3 System integration and testing

8.4.3.1 The individual elements incorporated in the system shall be integrated in accordance with the system design and tested in accordance with the system integration tests (see 7.4.11), and any tests resulting from ISO 26262-5 and ISO 26262-6 shall be completed.

NOTE The tests are intended to provide evidence that each element of the system interacts correctly and complies with the technical and functional safety concepts, and to give an adequate level of confidence that unintended behaviours, that could violate a safety goal, are absent.

8.4.3.2 In order to detect systematic faults during system integration, the test goals, resulting from the requirements 8.4.3.2.1 to 8.4.3.2.5, shall be addressed by the application of adequate test methods, as given in the corresponding tables.

NOTE Depending on the function implemented, and depending on the complexity or distributed nature of the item, it can be reasonable to move tests methods to other integration subphases provided that there is an adequate rationale.

8.4.3.2.1 The correct implementation of the system design specification, the technical and functional safety requirements shall be ensured by applying feasible test methods given in Table 9.

Table 9 — Correctness of implementation of system design specification, technical and functional safety requirements

Methods		ASIL			
		A	B	C	D
1a	Requirement-based test[a]	++	++	++	++
1b	Fault injection test[b]	+	+	++	++
1c	Back-to-back test[c]	o	+	+	++

[a] A requirements-based test denotes a test against functional and non-functional requirements.

[b] A fault injection test uses special means to introduce faults into the item. This can be done within the item via a special test interface or specially prepared elements or communication devices. The method is often used to improve the test coverage of the safety requirements, because during normal operation safety mechanisms are not invoked.

[c] A back-to-back test compares the responses of the test object with the responses of a simulation model to the same stimuli, to detect differences between the behaviour of the model and its implementation.

8.4.3.2.2 The correct functional performance of the safety mechanisms including accuracy and timing shall be ensured by applying feasible test methods given in Table 10.

Table 10 — Correctness of functional performance, accuracy and timing of safety mechanisms

Methods		ASIL			
		A	B	C	D
1a	Back-to-back test[a]	O	+	+	++
1b	Performance test[b]	o	+	+	++

[a] A back-to-back test compares the responses of the test object with the responses of a simulation model to the same stimuli, to detect differences between the behaviour of the model and its implementation.

[b] A performance test can verify the performance of the safety mechanisms concerning the system e.g. actuator speed or strength, whole system response times etc.

8.4.3.2.3 The consistency and correctness of the implementation of the external and internal interfaces shall be ensured by applying feasible test methods given in Table 11.

Table 11 — Consistency and correctness of implementation of external and internal interfaces

Methods		ASIL			
		A	B	C	D
1a	Test of external interfaces[a]	+	++	++	++
1b	Test of internal interfaces[a]	+	++	++	++
1c	Interface consistency check[a]	o	+	++	++
1d	Communication test[b]	++	++	++	++
1e	Test of interaction/communication[b]	++	++	++	++

[a] An interface test of the system includes tests of analogue and digital inputs and outputs, boundary tests, and equivalent-class tests, to completely test the specified interfaces, compatibility, timings, and other specified characteristics of the system. Internal interfaces of the system are tested by static tests, (e.g. match of plug connectors). as well as by dynamic tests concerning bus communications or any other interface between elements of the system.

[b] A communication and interaction test includes tests of the communication between the elements of the system as well as between the system under test and other vehicle systems during runtime against functional and non-functional requirements.

8.4.3.2.4 The effectiveness and the failure coverage by safety mechanisms at the item level shall be ensured by applying feasible test methods given in Table 12.

Table 12 — Effectiveness of diagnostic failure coverage of safety mechanisms at item level

Test methods		ASIL			
		A	B	C	D
1a	Fault injection test[a]	+	+	++	++
1b	Error guessing test[b]	+	+	++	++
1c	Test derived from field experience[c]	o	+	++	++

[a] A fault injection test uses special means to introduce faults into the item. This can be done within the item via a special test interface, specially prepared elements, or communication devices. The method is often used to improve the test coverage of the safety requirements, because during normal operation safety measures are not invoked.

[b] An error guessing test uses expert knowledge and data collected through lessons learned to anticipate errors in the item. Then a set of tests along with adequate test facilities is designed to check for these errors. Error guessing is an effective method given a tester who has previous experience with similar items.

[c] A test derived from field experience uses the experience and data gathered from the field. Erroneous system behaviour or newly discovered operational situations are analysed and a set of tests is designed to check the system with respect to the new findings.

8.4.3.2.5 The level of robustness of the item shall be ensured by applying feasible test methods given in Table 13.

Table 13 — Level of robustness

Methods		ASIL			
		A	B	C	D
1a	Resource usage test[a]	o	+	++	++
1b	Stress test[b]	o	+	++	++
1c	Test for interference resistance and robustness under certain environmental conditions[c]	++	++	++	++

[a] At the item level resource usage testing is usually performed in dynamic environments e.g. lab cars or prototypes. Issues to test are e.g. power consumption and bus load.

[b] A stress test verifies the correct operation of the item under high operational loads or high demands from the environment. Therefore, tests under high loads on the item, or with extreme user inputs or requests from other systems, as well as tests with extreme temperatures, humidity or mechanical shocks, can be applied.

[c] A test for interference resistance and robustness under certain environmental conditions is a special case of stress testing. This includes EMC and ESD tests.

8.4.4 Vehicle integration and testing

8.4.4.1 The item shall be integrated into the vehicle architecture and the vehicle integration tests shall be completed (see 7.4.11).

8.4.4.2 The verification of the on-board communication network and the on-board power supply network interaction shall be performed.

8.4.4.3 In order to detect systematic faults during vehicle integration, the test goals, resulting from the requirements 8.4.4.3.1 to 8.4.4.3.5, shall be addressed by the application of adequate test methods as given in the corresponding tables.

NOTE Depending on the function implemented, and depending on the complexity or distributed nature of the item, it can be reasonable to move tests methods to other integration subphases provided that there is an adequate rationale.

8.4.4.3.1 The correct implementation of the functional safety requirements shall be ensured by applying feasible test methods given in Table 14.

Table 14 — Correctness of implementation of functional safety requirements

Methods		ASIL			
		A	B	C	D
1a	Requirement-based test[a]	++	++	++	++
1b	Fault injection test[b]	++	++	++	++
1c	Long term test[c]	++	++	++	++
1d	User test under real-life conditions[c]	++	++	++	++

[a] A requirements-based test denotes a test against functional and non-functional requirements.

[b] A fault injection test uses special means to introduce faults into the item. This can be done within the item via a special test interface or specially prepared elements or communication devices. The method is often used to improve the test coverage of the safety requirements, because during normal operation safety mechanisms are not invoked

[c] A long term test and a user test under real-life conditions are similar to tests derived from field experience but use a larger sample size, normal users as testers, and are not bound to prior specified test scenarios, but performed under real-life conditions during everyday life.

8.4.4.3.2 The correct functional performance of the safety mechanisms including accuracy and timing shall be ensured by applying feasible test methods given in Table 15.

Table 15 — Correctness of functional performance, accuracy and timing of safety mechanisms

Methods		ASIL			
		A	B	C	D
1a	Performance test[a]	+	+	++	++
1b	Long term test[b]	+	+	++	++
1c	User test under real-life conditions[b]	+	+	++	++

[a] A performance test can verify the performance of the safety mechanisms concerning the item e.g. fault tolerant time intervals and vehicle controllability in the presence of faults.

[b] A long term test and a user test under real-life conditions are similar to tests derived from field experience but use a larger sample size, normal users as testers, and are not bound to prior specified test scenarios, but performed under real-life conditions during everyday life.

8.4.4.3.3 The consistency and correctness of the implementation of the external interfaces shall be ensured by applying feasible test methods given in Table 16.

Table 16 — Consistency and correctness of implementation of external interfaces

Methods		ASIL			
		A	B	C	D
1a	Test of external interfaces[a]	o	+	++	++
1b	Test of interaction/communication[b]	o	+	++	++

[a] An interface test at the vehicle level tests the interfaces of the systems of the vehicle for compatibility. This can be done statically by validating value ranges, ratings or geometries as well as dynamically during operation of the whole vehicle.

[b] A communication and interaction test includes tests of the communication between the systems of the vehicle during runtime against functional and non-functional requirements.

8.4.4.3.4 The effectiveness and the failure coverage by safety mechanisms at vehicle level shall be ensured by applying feasible test methods given in Table 17.

Table 17 — Effectiveness and failure coverage of safety mechanisms at vehicle level

Methods		ASIL			
		A	B	C	D
1a	Fault injection test[a]	o	+	++	++
1b	Error guessing test[b]	o	+	++	++
1c	Test derived from field experience[c]	o	+	++	++

[a] A fault injection test uses special means to introduce faults into the vehicle. This can be done within the vehicle via a special test interface, specially prepared hardware or communication devices. The method is often used to improve the test coverage of the safety requirements, because during normal operation safety measures are not invoked.

[b] An error guessing test uses expert knowledge and data collected through lessons learned to anticipate errors in the vehicle. Then a set of tests along with adequate test facilities is designed to check for these errors. Error Guessing is an effective method given a tester who has previous experience with similar vehicle applications.

[c] A test derived from field experience uses the experience and data gathered from the field. Erroneous vehicle behaviour or newly discovered operational situations are analysed and a set of tests is designed to check the vehicle with respect to the new findings.

8.4.4.3.5 The level of robustness of the item shall be ensured by applying feasible test methods given in Table 18.

Table 18 — Level of robustness

Methods		ASIL			
		A	B	C	D
1a	Resource usage test[a]	o	+	++	++
1b	Stress test[b]	o	+	++	++
1c	Test for interference resistance and robustness under certain environmental conditions[c]	o	+	++	++
1d	Long term test[d]	o	+	++	++

[a] At the item level resource usage testing is usually performed in dynamic environments e.g. lab cars or prototypes. Issues to test are e.g. item internal resources, power consumption or limited resources of other vehicle systems.

[b] A stress test verifies the correct operation of the vehicle under high operational loads or high demands from the environment. Therefore tests under high loads on the vehicle or with extreme user inputs or requests from other systems as well as tests with extreme temperatures, humidity or mechanical shocks can be applied.

[c] A test for interference resistance and robustness under certain environmental conditions is a special case of stress testing. This includes EMC and ESD tests.

[d] A long term test and a user test under real-life conditions are similar to tests derived from field experience but use a larger sample size, normal users as testers, and are not bound to prior specified test scenarios, but performed under real-life conditions during everyday life.

8.5 Work products

8.5.1 Integration testing specification resulting from requirements8.4.1.3, to 8.4.1.5.

8.5.2 Integration testing report(s) resulting from requirements 8.4.2, to 8.4.4.

9 Safety validation

9.1 Objectives

The first objective is to provide evidence of due compliance with the functional safety goals and that the safety concepts are appropriate for the functional safety of the item.

The second objective is to provide evidence that the safety goals are correct, complete and fully achieved at vehicle level.

9.2 General

The purpose of the preceding verification activities (e.g. design verification, safety analyses, hardware, software, and item integration and testing) is to provide evidence that the results of each particular activity comply with the specified requirements.

The validation of the integrated item aims to provide evidence of appropriateness for the intended use and confirming the adequacy of the safety measures.

9.3 Inputs to this clause

9.3.1 Prerequisites

The following information shall be available:

— Validation plan (refined) (see 6.5.2)

— Safety goals (see ISO 26262-3: —, 7.5.2)

— Functional safety concept (see ISO 26262-3: —,8.5.1)

— Hazard analysis and risk assessment (see ISO 26262-3: —, 7.5.1)

9.3.2 Further supporting information

The following information may be considered:

— Overall project plan (refined) (see 5.5.1)

— Technical safety concept (see 7.5.1)

— Functional concept (from external source)

— Item integration and testing plan (refined) (see 7.5.4)

9.4 Requirements and recommendation

9.4.1 Intent of safety validation

The validation of the safety goals shall be applied to the item integrated at the vehicle level. This integrated item includes:

a) E/E system;

b) software, if applicable;

c) hardware;

d) elements of other technologies;

e) external measures

9.4.2 Planning of validation

The validation plan shall be detailed, including:

a) the configuration of the item subjected to validation including the calibration data;

NOTE If a complete validation of each configurations of an item is not feasible, then a reasonable subset might be selected.

b) the specification of validation test procedures, test cases, driving manoeuvres, and acceptance criteria; and

c) the equipment and the required environmental conditions.

9.4.3 Execution of validation

9.4.3.1 If testing is used for validation then the same requirements for testing as provided for verification (see ISO 26262-8, 9.4.2 and 9.4.3), apply.

9.4.3.2 The characteristics of the item shall be validated at the vehicle level based on the safety goals, the functional safety requirements and the intended use, including:

a) the controllability;

b) the effectiveness of safety measures for controlling random and systematic failures;

c) the external measures;

d) the elements of other technologies.

9.4.3.3 The validation activities should provide an argument concerning the absence of erroneous activation of safety mechanisms due to operational situations, system or feature interactions, or use cases.

9.4.3.4 This requirement applies to ASILs (B), C, and D, in accordance with 4.3**:** The validation of random hardware failures shall be carried out at the item level in accordance with the metrics of ISO 26262-5: —, Clause 8 and in accordance with the assessment criteria of ISO 26262-5: —, Clause 9.

NOTE Quantitative evaluation for E/E elements of the item is provided by ISO 26262-5: —, 9.4.3 and 9.4.4. The whole item is evaluated qualitatively in case other technologies are involved in the item.

9.4.3.5 The validation at the vehicle level based on the safety goals, the functional safety requirements and the intended use, shall include:

a) the validation test procedures and test cases for each safety goal including detailed pass/fail criteria;

b) the scope of application. This may include issues such as configuration, environmental conditions, driving situation, operational use cases, etc.

NOTE Operational use cases can be created to help focus the safety validation at the vehicle level.

9.4.3.6 The following methods shall be applied:

a) reproducible tests with specified test procedures, test cases, and pass/fail criteria;

EXAMPLE positive tests of functions and safety requirements, black box, simulation, tests under boundary conditions, fault injection, durability tests, stress tests, highly accelerated life testing (HALT), simulation of external influences

b) analyses (e.g. FMEA, FTA, ETA, simulation);

c) long-term tests, such as vehicle driving schedules and captured test fleets;

d) user tests under real-life conditions, panel or blind tests, expert panels;

e) reviews.

9.4.4 The results of the validation shall be evaluated.

9.5 Work products

9.5.1 **Validation plan (refined)** resulting from requirement 9.4.2.

9.5.2 **Validation report** resulting from requirements 9.4.3 and 9.4.4

10 Functional safety assessment

10.1 Objectives

The objective of the requirements in this clause is to assess the functional safety that is achieved by the item.

10.2 General

The organisational entity with responsibility for functional safety (e.g. the vehicle manufacturer or the supplier, if the latter is responsible for functional safety) initiates an assessment of functional safety.

10.3 Inputs to this clause

10.3.1 Prerequisites

The following information shall be available:

— Safety case (see ISO 26262-2: —, 6.5.3)

— Safety plan (refined) (see 5.5.2, ISO 26262-5:—, 5.5.2 and ISO 26262-6:—, 5.5.2)

— Functional safety assessment plan (refined) (see 5.5.4)

10.3.2 Further supporting information

None

10.4 Requirements and recommendation

10.4.1 For each step of the safety lifecycle in ISO 26262-2: —, Figure 2, the specific topics to be addressed by the functional safety assessment shall be identified.

10.4.2 The functional safety assessment shall be conducted in accordance with ISO 26262-2: —, 6.4.6.7

10.5 Work products

Functional safety assessment report resulting from requirements 10.4.1, 10.4.2 and ISO 26262-2: —, 6.4.6.

11 Release for production

11.1 Objectives

The objective of this clause is to specify the criteria for the release for production at the completion of the item development. The release for production confirms that the item complies with the requirements for functional safety at vehicle level.

11.2 General

The release for production confirms that the item is ready for series-production and operation.

After completion of the verification and validation during the development at the hardware, software, system, item and vehicle level, as well as after the successful overall assessment of functional safety evidence of compliance with the prerequisites for serial production is provided.

This release documentation as basis for the production of the components, systems or vehicles is signed by the person in charge of the release.

11.3 Information required

11.3.1 Prerequisites

The following information shall be available:

— Functional safety assessment report (see 10.5)

— Safety case (see ISO 26262-2: —, 6.5.3)

11.3.2 Further supporting information

None

11.4 Requirements and recommendation

11.4.1 The release for production of the item shall only be approved if the work products listed under 11.3.1 are available and provide confidence of functional safety.

11.4.2 Documentation of functional safety for release for production

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

a) the name and signature of the person in charge of release;

b) the version/s of the released item;

c) the configuration of the released item;

d) references to associated documents;

e) the release date.

NOTE The release documentation of functional safety can be part of the document for release for production of the item, or it can be a separate document.

11.4.2.2 At release for production, a baseline for software and a baseline for hardware shall be available, that shall be documented in accordance with ISO 26262-8: —, Clause 10. The baselines shall be under configuration management in accordance with ISO 26262-8: —, Clause 7.

11.4.2.3 Identified safety anomalies shall be addressed in accordance with ISO 26262-2: —, 5.4.2.4 and ISO 26262-8: —, Clause 8.

11.5 Work products

Release for production report resulting from requirements 11.4.1 and 11.4.2.

Annex A
(informative)

Overview on and document flow of product development at the system level

Table A.1 provides an overview of objectives, prerequisites and work products of the particular phases of product development at the system level.

Table A.1 — Product development at the system level: Overview

Clause	Title	Objectives	Prerequisites	Work products
5	Initiation of product development at the system level	The objective of the initiation of the product development at the system level is to determine and plan the functional safety activities during the individual subphases of system development. This also includes the necessary supporting processes described in ISO 26262-8. This planning of system-level safety activities are included in the safety plan.	- Functional safety concept (see ISO 26262-3: —, 8.5.1) - Overall project plan (refined) (see ISO 26262-2: —, 6.5.2) - Safety plan (see ISO 26262-2: —, 6.5.1) - Functional safety assessment plan (see ISO 26262-2: —, 6.5.6)	5.5.1 Overall project plan (refined) 5.5.2 Safety plan (refined) 5.5.3 Validation plan 5.5.4 Functional safety assessment plan (refined) 5.5.5 Item integration and testing plan
6	Specification of the technical safety requirements	The first objective of this subphase is to develop the technical safety requirements. The technical safety requirements specification refines the functional safety concept considering the functional concept and the preliminary architectural design (see ISO 26262-3). The second objective is to verify through analysis that the technical safety requirements comply with the functional safety requirements.	- Functional safety concept (see ISO 26262-3: —, 8.5.1) - Validation plan (see 5.5.3)	6.5.1 Technical safety requirements specification 6.5.2 Validation plan (refined) 6.5.3 System-level verification report
7	System design	The first objective of this subphase is to develop the system design and the technical safety concept that comply with the functional requirements and the technical safety requirements specification of the item. The second objective of this subphase is to verify that the system design and the technical safety concept comply with the technical safety requirements specification.	- Technical safety requirements specification (see 6.5.1) - Item integration and testing plan (see 5.5.5)	7.5.1 Technical safety concept 7.5.2 System design specification 7.5.3 Requirements for production, operation, service and decommissioning 7.5.4 Item integration and testing plan (refined) 7.5.5 System-level verification report (refined) 7.5.6 Hardware Software Interface Specification (HSI)

Clause	Title	Objectives	Prerequisites	Work products
8	Item integration and testing	The first objective of the item integration and testing is to integrate the elements of an item and, if applicable, systems or elements of other technologies and external measures or systems step by step into the entire item. The integrated item is tested to comply with each safety requirement in accordance with its specification and ASIL classification. The second objective of the item integration and testing is to verify that the "System design" (see Clause 7) is correctly implemented by the entire item.	- System design specification (see 7.5.2) - Safety goals (see ISO 26262-3: —, 7.5.2) - Functional safety concept (see ISO 26262-3: —, 8.5.1) - Technical safety concept (see 7.5.1) - Hardware Software Interface Specification (HSI) (see 7.5.6) - Item integration and testing plan (refined) (see 7.5.4)	8.5.1 Integration testing specification 8.5.2 Integration testing report(s)
9	Safety validation	The first objective is to provide evidence of due compliance with the functional safety goals and that the safety concepts are appropriate for the functional safety of the item. The second objective is to provide evidence that the safety goals are correct, complete and fully achieved at vehicle level.	- Validation plan (refined) (see 6.5.2) - Safety goals (see ISO 26262-3: —, 7.5.2) - Functional safety concept (see ISO 26262-3: —,8.5.1) - Hazard analysis and risk assessment (see ISO 26262-3: —, 7.5.1)	9.5.1 Validation plan (refined) 9.5.2 Validation report
10	Functional safety assessment	The objective of the requirements in this clause is to assess the functional safety that is achieved by the item.	- Safety case (see ISO 26262-2: —, 6.5.3) - Safety plan (refined) (see 5.5.2, ISO 26262-5:—, 5.5.2 and ISO 26262-6:—, 5.5.2) - Functional safety assessment plan (refined) (see 5.5.4)	10.5 Functional safety assessment report
11	Product release	The objective of this clause is to specify the criteria for the release for production at the completion of the item development. The release for production confirms that the product complies with the requirements for functional safety at vehicle level.	- Functional safety assessment report (see 10.5) - Safety case (see ISO 26262-2: —, 6.5.3)	11.5 Release for production report

Annex B(informative)

Example contents of hardware-software interface

This Annex provides further explanation on the hardware-software interface.

The hardware-software interface is specified in ISO 26262-4 during the subphase "System design". As development continues during the subphases of hardware development (ISO 26262-5) and software development (ISO 26262-6), this specification is detailed.

First, an overview figure is given which provides the relation of product development at the system, hardware, and software level, and the role of the hardware-software interface. The hardware-software interface acts as the linkage between the different levels of development. The hardware-software interface is used to agree on topics relevant to both hardware and software development.

NOTE The hardware-software interface is not to be confused with the hardware abstraction layer (HAL).

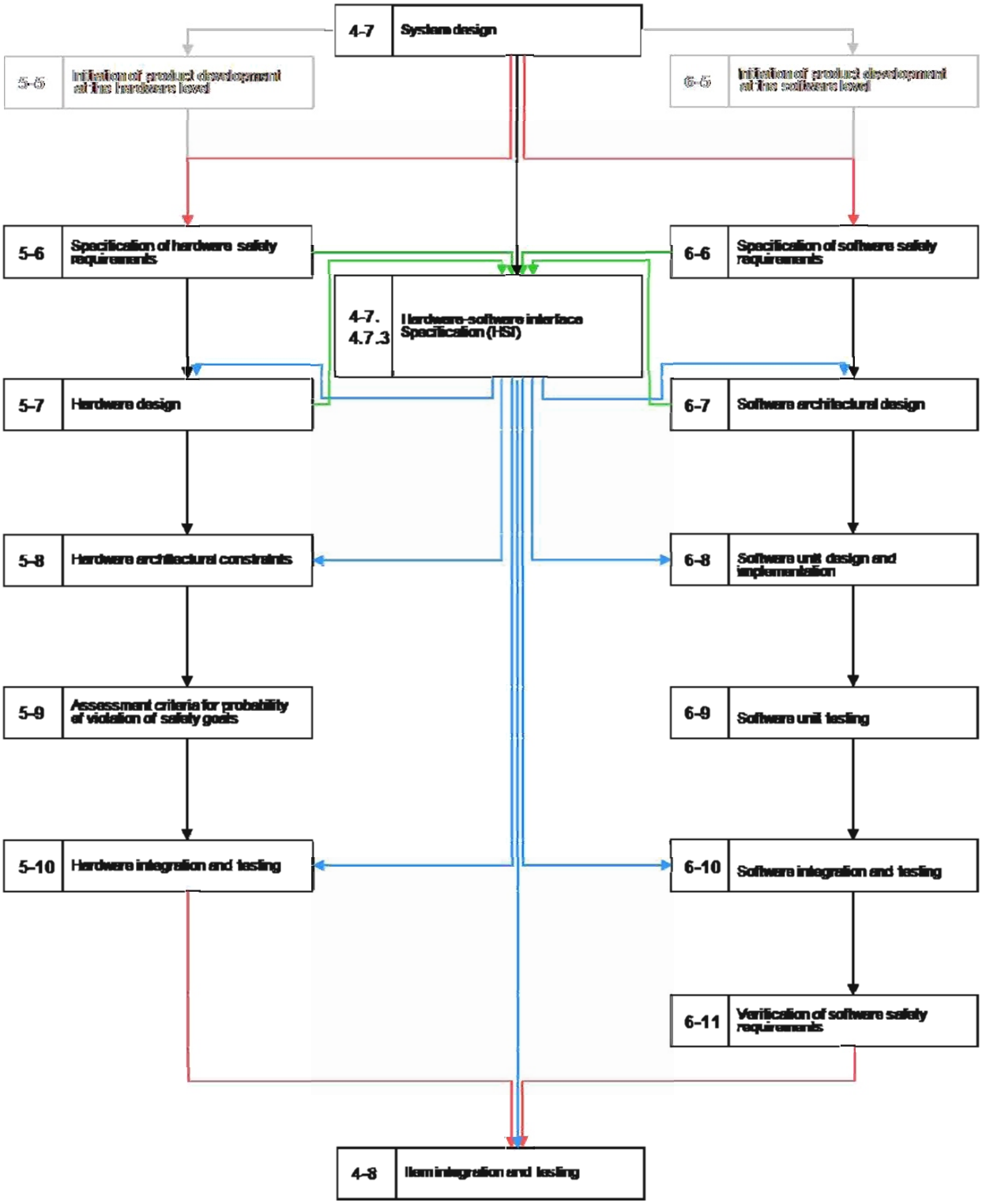

Figure B.1 — Overview on interaction with the hardware-software interface

Second, to ease specifying the hardware-software interface, a list of typical hardware-software interface elements is given as well as a non-concluding list of characteristics to be implemented by the elements of the hardware-software interface.

The following hardware-software interface elements are recommended to be considered when specifying the hardware-software interface:

a) Memory

   1) Volatile memory (e.g. RAM)

   2) Non - volatile memory (e.g. NvRAM)

b) Bus interfaces (e.g. CAN, LIN, internal HSSL)

c) Converter

   1) A/D converter

   2) D/A converter

   3) PWM

d) Mulitplexer

e) Digital I/O

f) Watchdog

   1) Internal

   2) External

The following characteristics of the hardware-software interface are to be considered when specifying the hardware-software interface:

a) Interrupts

b) Timing consistency

c) Data integrity

d) Initialisation

   1) Memory and registers

   2) Boot management

e) Message transfer

   1) Send message

   2) Receive message

f) Network modes

   1) Sleeping

   2) Awakening

g) Memory management

   1) Reading

   2) Writing

3) Diagnostic

4) Address space

5) Data types

h) Real-time counter

1) Start counter

2) Stop counter

3) Freeze counter

4) Load counter

The following table provides an example to help allocating hardware-software interface characteristics to hardware-software interface elements.

Description	HW-Identifier	SW-Identifier	Channel 1	Channel 2	MUX No. - Channel 1	MUX No. - Channel 2	Data type HW Interface	Address Channel 1	Address Channel 2	Unit	Interface Type	Comments	Range of values	Accuracy (% of range of values)
Inputs														
INPUT 1	IN_1	IN_1	x		4		U16	0x8000		V	Analogue - Internal	Analogue Input 1	0-5	0,50%

Table B.1 —Example for inputs of internal signals

Bibliography

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