INTERNATIONAL STANDARD

ISO 26262-4

First edition
2011-11-15

Road vehicles — Functional safety —

Part 4:
Product development at the system level

Véhicules routiers — Sécurité fonctionnelle —

Partie 4: Développement du produit au niveau du système

Reference number
ISO 26262-4:2011(E)

COPYRIGHT PROTECTED DOCUMENT

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

Published in Switzerland

Contents

Page

Foreword

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

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

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

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

ISO 26262-4 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 at the system level*

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

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

— *Part 7: Production and operation*

— *Part 8: Supporting processes*

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

— *Part 10: Guideline on ISO 26262*

Introduction

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

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

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

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

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

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

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

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

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

e) provides requirements for relations with suppliers.

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

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

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

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

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

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

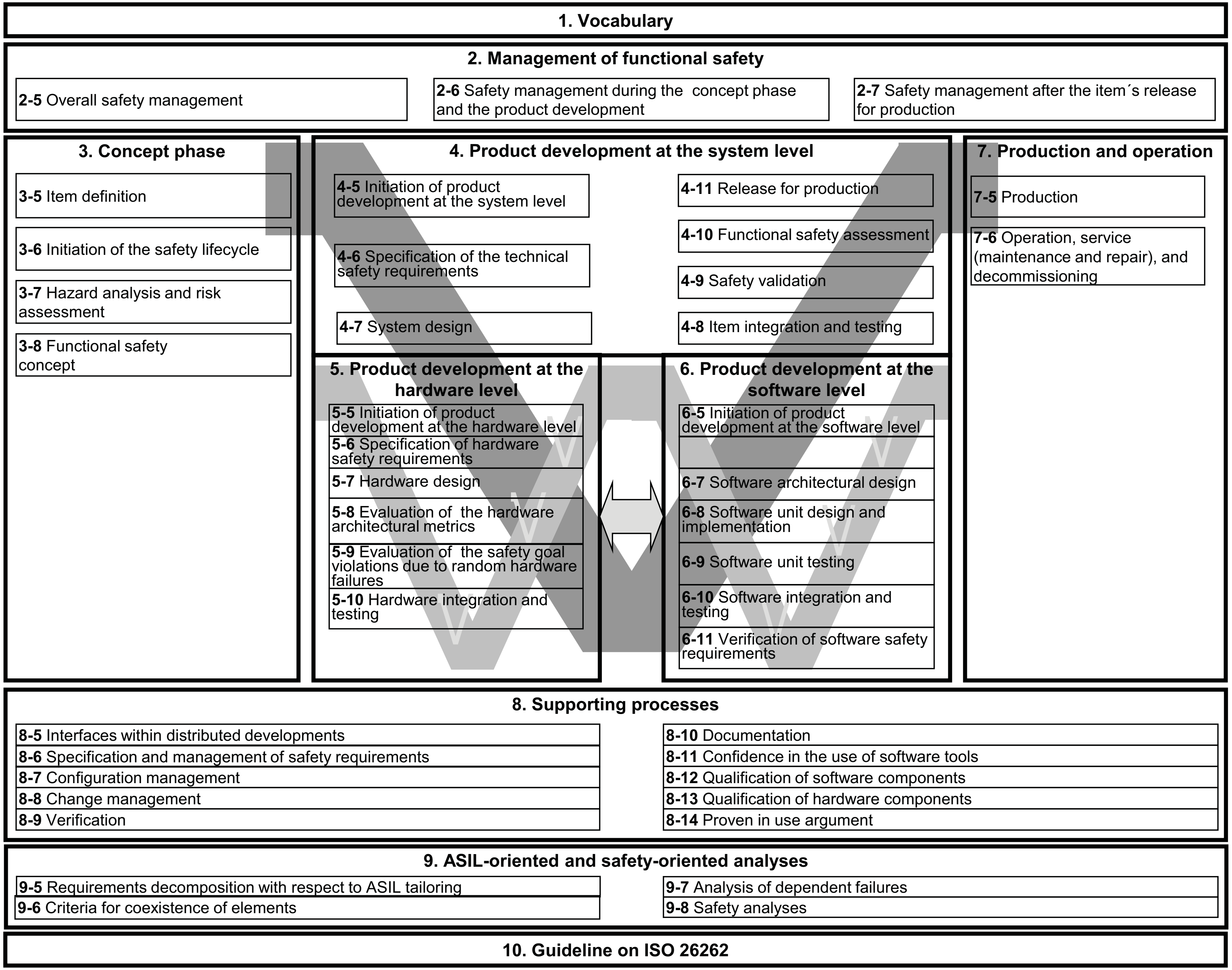


Figure 1 — Overview of ISO 26262

Road vehicles — Functional safety —

Part 4:
Product development at the system level

1 Scope

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

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

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

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

This part of ISO 26262 specifies the requirements for product development at the system level for automotive applications, including the following:

— requirements for the initiation of product development at the system level,

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

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

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

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

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

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

ISO 26262-8:2011, *Road vehicles — Functional safety — Part 8: Supporting processes*

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

3 Terms, definitions and abbreviated terms

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

4 Requirements for compliance

4.1 General requirements

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

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

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

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

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

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

4.2 Interpretations of tables

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

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

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

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

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

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

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

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

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

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

4.3 ASIL-dependent requirements and recommendations

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

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

5 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.

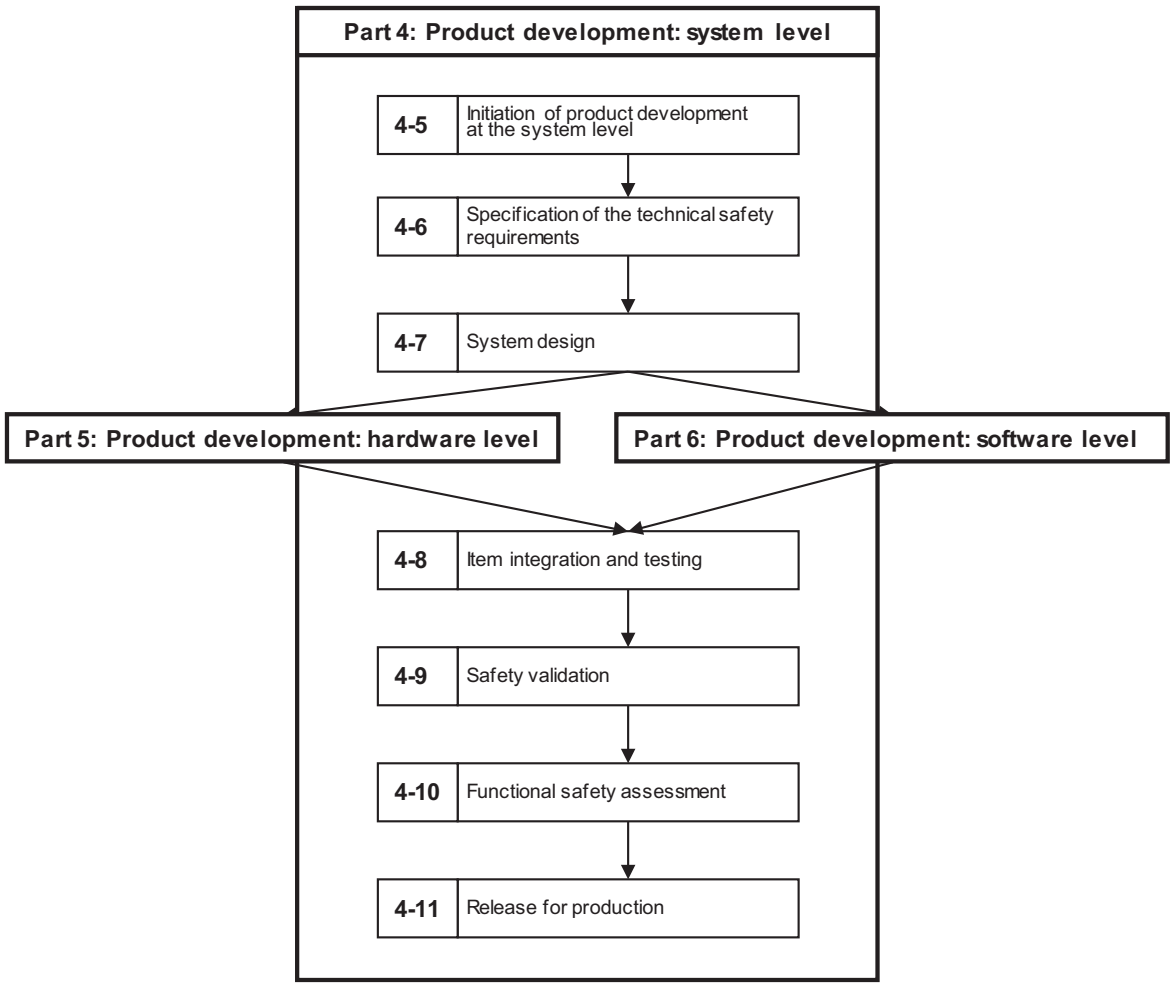
This planning of system-level safety activities will be included in the safety plan.

5.2 General

The necessary activities during the development of a system are given in Figure 2. After the initiation of product development and the specification of the technical safety requirements, the system design is performed. During system design the system architecture is established, the technical safety requirements are allocated to hardware and software, and, if applicable, on other technologies. In addition, the technical safety requirements are refined and requirements arising from the system architecture are added, including the hardware-software interface (HSI). Depending on the complexity of the architecture, the requirements for subsystems can be derived iteratively. After their development, the hardware and software elements are integrated and tested to form an item that is then integrated into a vehicle. Once integrated at the vehicle level, safety validation is performed to provide evidence of functional safety with respect to the safety goals.

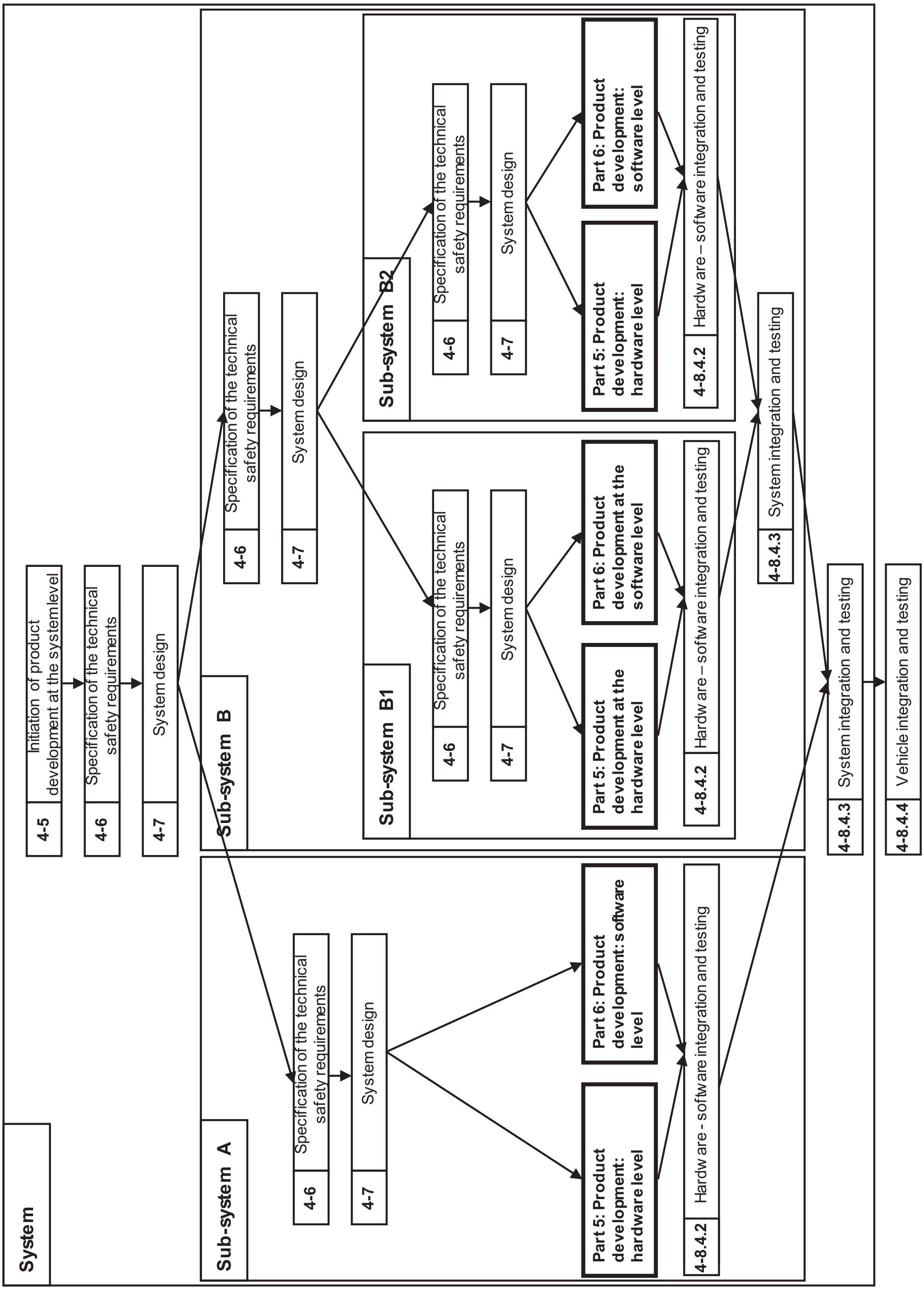
ISO 26262-5 and ISO 26262-6 describe the development requirements for hardware and software. This part of ISO 26262 applies to both the development of systems and subsystems. Figure 3 is an example of a system with multiple levels of integration, illustrating the application of this part of ISO 26262, ISO 26262-5 and ISO 26262-6.

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



NOTE 2 Within the figure, the specific clauses of each part of ISO 26262 are indicated in the following manner: “m-n”, where “m” represents the number of the part and “n” indicates the number of the clause, e.g. “4-5” represents Clause 5 of ISO 26262-4.

Figure 2 — Reference phase model for the development of a safety-related item



NOTE Within the figure, the specific clauses of each part of ISO 26262 are indicated in the following manner: "m-n", where "m" represents the number of the part and "n" indicates the number of the clause, e.g. "4-5" represents Clause 5 of ISO 26262-4.

Figure 3 — 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:

— project plan (refined) in accordance with ISO 26262-2:2011, 6.5.2;

— safety plan in accordance with ISO 26262-3:2011, 6.5.2;

— functional safety assessment plan in accordance with ISO 26262-2:2011, 6.5.4; and

— functional safety concept in accordance with ISO 26262-3:2011, 8.5.1.

5.3.2 Further supporting information

The following information can be considered:

— preliminary architectural assumptions (from external source); and

— item definition (see ISO 26262-3:2011, 5.5).

5.4 Requirements and recommendations

5.4.1 The safety activities for the product development at the system level shall be planned including determination of appropriate methods and measures during design and integration.

NOTE The results of planning of the verification activities during design in accordance with 6.4.6 (Verification and validation) and 7.4.8 (Verification of system design) are part of the safety plan while the planning of item integration and testing in accordance with 8.4.2 (hardware/software), 8.4.3 (element integration) and 8.4.4 (item integration) is represented in a separate item integration and testing plan in accordance with requirement 8.4.1.3.

5.4.2 The validation activities shall be planned.

5.4.3 The functional safety assessment activities for the product development at the system level shall be planned (see also ISO 26262-2).

NOTE An example of a functional safety assessment agenda is provided in ISO 26262-2:2011, Annex E.

5.4.4 The tailoring of the lifecycle for product development at system level shall be performed in accordance with ISO 26262-2, and based on the reference phase model given in Figure 2.

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. This can include the integration steps at each level.

5.5 Work products

5.5.1 **Project plan (refined)** resulting from requirement 5.4.4.

5.5.2 **Safety plan (refined)** resulting from requirement 5.4.1 to 5.4.4.

5.5.3 **Item integration and testing plan** resulting from requirement 5.4.1.

5.5.4 **Validation plan** resulting from requirement 5.4.2.

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

6 Specification of the technical safety requirements

6.1 Objectives

The first objective of this subphase is to specify the technical safety requirements. The technical safety requirements specification refines the functional safety concept, considering both the functional concept and the preliminary architectural assumptions (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 are the technical requirements necessary to implement the functional safety concept, with the intention being to detail the item-level functional safety requirements into the system-level technical safety requirements.

NOTE Regarding the avoidance of latent faults, requirements elicitation can be performed after a first iteration of the system design subphase.

6.3 Inputs to this clause

6.3.1 Prerequisites

The following information shall be available:

— functional safety concept in accordance with ISO 26262-3:2011, 8.5.1; and

— validation plan in accordance with 5.5.4.

6.3.2 Further supporting information

The following information can be considered:

— safety goals (see ISO 26262-3:2011, 7.5.2);

— functional concept (from external source, see ISO 26262-3:2011, 5.4.1); and

— preliminary architectural assumptions (from external source, see ISO 26262-3:2011, 8.3.2).

6.4 Requirements and recommendations

6.4.1 Specification of the technical safety requirements

6.4.1.1 The technical safety requirements shall be specified in accordance with the functional safety concept, the preliminary architectural assumptions of the item and the following system properties:

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

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

c) the system configuration requirements.

NOTE The ability to reconfigure a system for alternative applications is a strategy to reuse existing systems.

EXAMPLE Calibration data (see ISO 26262-6:2011, Annex C) is frequently used to customise electronic engine control units for alternate vehicles.

6.4.1.2 The consistency of the preliminary architectural assumptions in ISO 26262-3:2011, 8.3.2 and the preliminary architecture assumptions in this subphase shall be ensured.

6.4.1.3 If other functions or requirements are implemented by the system or its elements, in addition to those functions for which technical safety requirements are specified in accordance with 6.4.1 (Specification of the technical safety requirements), then these functions or requirements shall be specified or references made to their specification.

EXAMPLE Other requirements are coming from Economic Commission for Europe (ECE) rules, Federal Motor Vehicle Safety Standard (FMVSS) or company platform strategies.

6.4.1.4 The technical safety requirements shall specify safety-related dependencies between systems or item elements and between the item and other systems.

6.4.2 Safety mechanisms

6.4.2.1 The technical safety requirements shall specify the response of the system or elements to stimuli that affect the achievement of safety goals. This includes failures and relevant combinations of stimuli in combination with each relevant operating mode and defined system state.

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

6.4.2.2 The technical safety requirements shall specify the necessary safety mechanisms (see ISO 26262-8:2011, Clause 6) including:

a) the measures relating to the detection, indication and control of faults in the system itself;

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

NOTE 2 This includes measures for the detection and control of failure modes of the communication channels (e.g. data interfaces, communication buses, wireless radio link).

b) the measures relating to the detection, indication and control of faults in external devices that interact 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 3 This includes prioritization and arbitration logic in the case of conflicting safety mechanisms.

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

e) the measures which prevent faults from being latent [see 6.4.4 (Avoidance of latent faults)].

NOTE 4 These measures are usually related to tests that take place during power up (pre-drive checks), as in the case of measures a) to d), during operation, during power-down (post-drive checks), and as part of maintenance.

6.4.2.3 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;

NOTE 1 This includes the requirements to control the actuators.

b) the fault tolerant time interval;

NOTE 2 In-vehicle testing and experimentation can be used to determine the fault tolerant time interval.

c) the emergency operation interval, if the safe state cannot be reached immediately; and

NOTE 3 In-vehicle testing and experimentation can be used to determine the emergency operation interval.

EXAMPLE 1 Switching off can be an emergency operation.

d) the measures to maintain the safe state.

EXAMPLE 2 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.).

6.4.3 ASIL Decomposition

6.4.3.1 If ASIL decomposition is applied during the specification of the technical safety requirements it shall be applied in accordance with ISO 26262-9:2011, Clause 5 (Requirements decomposition with respect to ASIL tailoring).

6.4.4 Avoidance of latent faults

6.4.4.1 This requirement 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 have the potential to include latent faults.

EXAMPLE On-board tests are safety mechanisms which verify the status of components during the different operation modes such as power-up, power-down, at runtime or in an additional test mode to detect latent faults. Valve, relay or lamp function tests that take place during power up routines are examples of such on-board tests.

NOTE 2 Evaluation criteria that identify the need for safety measures preventing faults from being latent are derived in accordance with good engineering practice. The latent fault metric, given in ISO 26262-5:2011, Clause 8, provides evaluation criteria.

6.4.4.2 This requirement applies to ASILs (A), (B), C, and D, in accordance with 4.3: to avoid multiple-point failures, the multiple-point fault detection interval shall be specified for each safety mechanism implemented in accordance with 6.4.4 (Avoidance of latent faults).

6.4.4.3 This requirement applies to ASILs (A), (B), C, and D, in accordance with 4.3: to determine the multiple-point fault detection interval, the following parameters should be considered:

a) the reliability of the hardware component with consideration given to its role in the architecture;

b) the probability of exposure of the corresponding hazardous event(s);

c) the specified quantitative target values for the maximum probability of violation of each safety goal due to hardware random failures (see requirement 7.4.4.3); and

d) the assigned ASIL of the related safety goal.

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

— periodic testing of the system or elements during operation;

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

— testing the system or elements during maintenance.

6.4.4.4 This requirement applies to ASILs (A), (B), C, and D, in accordance with 4.3: the development of safety mechanisms that prevent dual point faults from being latent shall comply with:

a) ASIL B for technical safety requirements assigned ASIL D;

b) ASIL A for technical safety requirements assigned ASIL B and ASIL C; and

c) engineering judgement for technical safety requirements assigned ASIL A.

6.4.5 Production, operation, maintenance and decommissioning

6.4.5.1 The technical safety requirements concerning functional safety of the item or its elements during production, operation, maintenance, repair and decommissioning, addressed in ISO 26262-7, shall be specified.

NOTE There are two aspects that assure safety during production, operation, maintenance, repair and decommissioning. The first aspect relates to those activities performed during the development phase which are given in requirement 6.4.5.1 and 7.4.7 (Requirements for production, operation, service and decommissioning), while the second aspect relates to those activities performed during the production and operation phase, which are addressed in ISO 26262-7.

6.4.6 Verification and validation

6.4.6.1 The technical safety requirements shall be verified in accordance with ISO 26262-8:2011, Clause 9, to provide evidence for their:

a) compliance and consistency with the functional safety concept; and

b) compliance with the preliminary architectural design assumptions.

6.4.6.2 The criteria for safety validation of the item shall be refined based on the technical safety requirements.

NOTE The system validation planning and the system validation specifications are developed in parallel with the technical safety requirements (see Clause 9).

6.5 Work products

6.5.1 **Technical safety requirements specification** resulting from requirements 6.4.1 to 6.4.5.

6.5.2 **System verification report** resulting from requirement 6.4.6.

6.5.3 **Validation plan (refined)** resulting from requirement 6.4.6.2.

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 is comprised of subsystems.

In order to develop a system architectural design, functional safety requirements, technical safety requirements and non-safety-related requirements are implemented. Hence in this subphase safety-related and non-safety-related requirements are handled within one development process.

7.3 Inputs to this clause

7.3.1 Prerequisites

The following information shall be available:

— item integration and testing plan in accordance with 5.5.3; and

— technical safety requirements specification in accordance with 6.5.1.

7.3.2 Further supporting information

The following information can be considered:

— preliminary architectural assumptions (from external source, see ISO 26262-3:2011, 8.3.2);

— functional concept (from external source); and

— functional safety concept (see ISO 26262-3:2011, 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 based on the functional concept, the preliminary architectural assumptions and the technical safety requirements. The consistency of the preliminary architectural assumptions in ISO 26262-3:2011, 8.3.2 and the preliminary architectural assumptions in this subphase shall be ensured.

7.4.1.2 The technical safety requirements shall be allocated to the system design elements.

7.4.1.3 The system design shall implement the technical safety requirements.

7.4.1.4 With regard to the implementation of the technical safety requirements the following shall be considered in the system design:

a) the ability to verify the system design;

b) the technical capability of the intended hardware and software design with regard to the achievement of functional safety; and

c) the ability to execute tests during system integration.

7.4.2 System architectural design constraints

7.4.2.1 The system and subsystem architecture shall comply with the technical safety requirements at their respective ASILs.

7.4.2.2 Each element shall inherit the highest ASIL from the technical safety requirements that it implements.

7.4.2.3 If an element is comprised of sub-elements with different ASILs assigned, or of non-safety-related sub-elements and safety-related sub-elements, then each of these shall be treated in accordance with the highest ASIL, unless the criteria for coexistence, in accordance with ISO 26262-9:2011, Clause 6, are met.

7.4.2.4 Internal and external interfaces of safety-related elements shall be defined, 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 to the safety requirements during system design, it shall be applied in accordance with ISO 26262-9:2011, Clause 5.

7.4.3 Measures for the avoidance of systematic failures

7.4.3.1 Safety analyses on the system design to identify the causes of systematic failures and the effects of systematic faults shall be applied in accordance with Table 1 and ISO 26262-9:2011, 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, Ishikawa diagram.

[b] Inductive analysis methods include FMEA, ETA, Markov modelling.

NOTE 1 The purpose of these analyses is to assist in the design. Therefore at this stage, qualitative analysis is likely to be sufficient. Quantitative analysis can be performed if necessary.

NOTE 2 The analysis is conducted at the level of detail necessary to identify or exclude causes and effects of systematic failures.

7.4.3.2 Identified internal causes of systematic failures shall be eliminated or their effects mitigated.

7.4.3.3 Identified external causes of systematic failures shall be eliminated or their effects mitigated.

7.4.3.4 To reduce systematic failures, well-trusted automotive systems design principles should be applied. These may include the following:

a) re-use of well-trusted technical safety concepts;

b) re-use of well-trusted designs for elements, including hardware and software components;

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

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

7.4.3.5 To ensure the suitability of well-trusted design principles or elements in the new item, the results of their application shall be analysed and the underlying assumptions checked before reuse.

NOTE The impact analysis includes the capability and feasibility of the determined diagnostics, environmental constraints, timing constraints, compatibility of the determined resources, and the robustness of the system design.

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

7.4.3.7 This requirement applies to ASILs (A), (B), C, and D, in accordance with 4.3: in order to avoid failures resulting from high complexity, the architectural design shall exhibit all of the following properties by use of the principles in Table 2:

a) modularity;

b) adequate level of granularity; and

c) simplicity.

Table 2 — Properties of modular system design

Properties		ASIL			
		A	B	C	D
1	Hierarchical design	+	+	++	++
2	Precisely defined interfaces	+	+	+	+
3	Avoidance of unnecessary complexity of hardware components and software components	+	+	+	+
4	Avoidance of unnecessary complexity of interfaces	+	+	+	+
5	Maintainability during service	+	+	+	+
6	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 mitigation of random hardware failures shall be specified with respect to the system design given in 7.4.1 (System design specification and technical safety concept).

EXAMPLE 1 Such measures can be hardware diagnostic features 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 single-point fault metric and latent-point fault metric (see ISO 26262-5:2011, Clause 8), shall be specified for final evaluation at the item level (see requirement 9.4.3.3).

7.4.4.3 This requirement applies to ASILs (B), C, and D, in accordance with 4.3: one of the alternative procedures of evaluation of violation of the safety goal due to random hardware failures (see ISO 26262-5:2011, Clause 9) shall be chosen and the target values shall be specified for final evaluation at item level (see requirement 9.4.3.3).

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

a) the target values of the metrics in ISO 26262-5:2011, Clause 8; and

b) the procedures in ISO 26262-5:2011, Clause 9.

7.4.4.5 This requirement applies to ASILs (B), C, and D, in accordance with 4.3: for distributed developments (see ISO 26262-8:2011, Clause 5), the derived target values shall be communicated to each relevant party.

NOTE Architectural constraints described in ISO 26262-5:2011, Clauses 8 and 9, are not directly applicable to COTS parts and components. This is because suppliers usually cannot 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 made available by the part supplier in order to allow the estimation of architectural constraints at overall hardware architecture level.

7.4.5 Allocation to hardware and software

7.4.5.1 The technical safety requirements shall be allocated directly or by further refinement to hardware, software or both.

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

NOTE The evidence of compliance with an allocated safety requirement for some of those hardware elements can be provided through qualification measures in accordance with ISO 26262-8:2011, Clause 13, if the criteria for applying this clause are met.

7.4.5.3 The system design shall comply with the allocation and partitioning decisions.

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

7.4.6 Hardware-software interface specification (HSI)

7.4.6.1 The HSI specification shall specify the hardware and software interaction and be consistent with the technical safety concept. The HSI specification shall include the component's hardware devices that are controlled by software and hardware resources that support the execution of software.

EXAMPLE The aspects and characteristics detailed in the HSI are given in Annex B.

7.4.6.2 The HSI specification shall include the following characteristics:

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

   EXAMPLE 1 Operating modes of hardware devices such as: default, init, test or advanced modes.

   EXAMPLE 2 Configuration parameters such as: gain control, band pass frequency or clock prescaler.

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

   EXAMPLE 4 Serial, parallel, slave, master/slave.

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

7.4.6.3 The relevant diagnostic capabilities of the hardware and their use by the software shall be specified in the HSI specification:

a) the hardware diagnostic features shall be defined; and

   EXAMPLE Detection of over-current, short-circuit or over-temperature.

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

7.4.6.4 The HSI shall be specified during the system design and will be refined during hardware development (see ISO 26262-5:2011, Clause 7) and during software development (see ISO 26262-6:2011, Clause 7).

7.4.7 Requirements for production, operation, service and decommissioning

7.4.7.1 Diagnostic features shall be specified to provide the required data that enables field monitoring for the item or its elements during operation, with consideration being given to the results of safety analyses and the implemented safety mechanisms.

7.4.7.2 To maintain functional safety, diagnostic features shall be specified that allow fault identification by workshop staff when servicing is needed.

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

a) the assembly instructions requirements;

b) the safety-related special characteristics;

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

EXAMPLE 1 Labelling of elements.

d) the verification methods and measures for production;

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

f) the decommissioning requirements.

EXAMPLE 2 Decommissioning instructions.

7.4.8 Verification of system design

7.4.8.1 The system design shall be verified for compliance and completeness with regard to the technical safety concept using the verification methods listed in Table 3.

Table 3 — 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	System design analyses[c]	see Table 1			

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

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

[c] For conducting safety analyses, see ISO 26262-9:2011, Clause 8.

NOTE Anomalies and incompleteness identified between the system design, regarding the technical safety concept, will be reported in accordance with ISO 26262-2:2011, 5.4.2.

7.4.8.2 Newly identified hazards by the system design not covered in a safety goal shall be introduced and evaluated in the hazard analysis and risk assessment in accordance with ISO 26262-3 and the change management process in ISO 26262-8:2011, Clause 8.

NOTE Newly identified hazards, not already reflected in a safety goal, are usually non-functional hazards. Non-functional hazards are outside the scope of ISO 26262, but they can be 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 might be assigned for reference purpose.

7.5 Work products

7.5.1 Technical safety concept resulting from requirements 7.4.1 and 7.4.5.

7.5.2 System design specification resulting from requirements 7.4.1 to 7.4.5.

7.5.3 Hardware-software interface specification (HSI) resulting from requirements 7.4.6.

7.5.4 Specification of requirements for production, operation, service and decommissioning resulting from requirements 7.4.7.

7.5.5 System verification report (refined) resulting from requirement 7.4.8.

7.5.6 Safety analysis reports resulting from requirement 7.4.3.

8 Item integration and testing

8.1 Objectives

The integration and testing phase comprises three phases and two primary goals as described below: the first phase is the integration of the hardware and software of each element that the item comprises. The second phase is the integration of the elements that comprise an item to form a complete system. The third phase is the integration of the item with other systems within a vehicle and with the vehicle itself.

The first objective of the integration process is to test compliance with each safety requirement in accordance with its specification and ASIL classification.

The second objective is to verify that the “System design” covering the safety requirements [see Clause 7 (System design)] are correctly implemented by the entire item.

8.2 General

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

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 (Item integration and testing) can start.

8.3 Inputs to this clause

8.3.1 Prerequisites

The following information shall be available:

— safety goals in accordance with ISO 26262-3:2011, 7.5.2;

— functional safety concept in accordance with ISO 26262-3:2011, 8.5.1;

— item integration and testing plan in accordance with 5.5.3;

— technical safety concept in accordance with 7.5.1;

— system design specification in accordance with 7.5.2; and

— hardware-software interface specification (HSI) in accordance with 7.5.6.

8.3.2 Further supporting information

The following information can be considered:

— vehicle architecture (from external source);

— technical safety concepts of other vehicle systems (from external source); and

— safety analysis reports (see 7.5.6).

8.4 Requirements and recommendation

8.4.1 Planning and specification of integration and testing

8.4.1.1 To demonstrate that the system design is compliant with the functional and technical safety requirements, integration testing activities shall be performed in accordance with ISO 26262-8:2011, Clause 9.

NOTE The following test goals are addressed in Tables 4 to 18:

a) the correct implementation of functional safety and technical safety requirements;

b) the correct functional performance, accuracy and timing of safety mechanisms;

c) the consistent and correct implementation of interfaces;

d) the effectiveness of a safety mechanism's diagnostic or failure coverage; and

e) the level of robustness.

8.4.1.2 An integration and test strategy shall be defined, which is based on the system design specification, the functional safety concept, the technical safety concept and the item integration and testing plan and provides evidence that the test goals are covered sufficiently. The integration and test strategy shall cover both E/E elements and elements of other technologies considered in the safety concepts.

NOTE Usually the integration levels are HW/SW, System, and Vehicle level.

8.4.1.3 To enable the system integration subphase the following shall be performed:

a) the integration and testing plan shall be refined for the hardware-software integration and testing;

b) the item integration and testing plan shall be refined to include the specification of integration tests for the system and vehicle levels. It shall ensure that open issues from hardware-software verifications are addressed; and

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

NOTE 1 When planning the vehicle level integration and testing, the correct vehicle behaviour under typical and extreme vehicle conditions and environments can be considered, but with a subset being sufficient (see Table 4).

NOTE 2 Integration and testing planning, carried out at the hardware-software integration and item levels, considers the interface and interaction between hardware and software.

8.4.1.4 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.

NOTE If a complete verification of each configuration at the system or vehicle level is not feasible, then a reasonable subset might be selected.

8.4.1.5 The test equipment shall be subject to the control of a monitoring quality system.

8.4.1.6 Each functional and technical safety requirement shall be verified (if applicable by testing) at least once in the complete integration subphase.

NOTE 1 A common practice is to verify a safety requirement at the next higher level of integration to which it has been specified.

NOTE 2 Safety anomalies identified during integration testing are reported in accordance with ISO 26262-2:2011, 5.4.2.

8.4.1.7 To enable the appropriate specification of test cases for the integration tests, test cases shall be derived using an appropriate combination of methods, as listed in Table 4, and by considering the integration level.

Table 4 — Methods for deriving test cases for 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	Error guessing based on knowledge or experience	+	+	++	++
1f	Analysis of functional dependencies	+	+	++	++
1g	Analysis of common limit conditions, sequences, and sources of dependent failures	+	+	++	++
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 Hardware-software integration

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

8.4.2.1.2 This requirement applies to ASILs C, and D, in accordance with 4.3: the hardware-software interface (HSI) requirements shall be tested with appropriate coverage, with consideration to the ASIL or a rationale shall be given that no issues with respect to the HSI remain.

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

8.4.2.2 Test goals and test methods during hardware-software testing

8.4.2.2.1 To detect systematic faults, present in the system design, during hardware-software integration, the test goals resulting from the requirements 8.4.2.2.2 to 8.4.2.2.6 shall be addressed by the application of adequate test methods, as given in the corresponding tables.

NOTE Depending on the function implemented, its complexity or the distributed nature of the system, it can be reasonable to move test methods to other integration subphases with adequate rationale.

8.4.2.2.2 The correct implementation of the technical safety requirements at the hardware-software level shall be demonstrated using feasible test methods given in Table 5.

Table 5 — Correct implementation of technical safety requirements at the hardware-software level

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.

NOTE The differences in the level of effort applied for Clause 1b in Table 5 and Table 10 result from the amount of efforts to conduct fault injection tests at system level.

8.4.2.2.3 This requirement applies to ASIL (A), B, C, and D, in accordance with 4.3: the correct functional performance, accuracy and timing of the safety mechanisms at the hardware-software level shall be demonstrated using feasible test methods given in Table 6.

Table 6 — Correct functional performance, accuracy and timing of safety mechanisms at the hardware-software level

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 (e.g. task scheduling, timing, power output) in the context of the whole test object, and can verify the ability of the intended control software to run with the hardware.

8.4.2.2.4 This requirement applies to ASIL (A), B, C, and D, in accordance with 4.3: the consistent and correct implementation of the external and internal interfaces at the hardware-software level shall be demonstrated using feasible test methods given in Table 7.

Table 7 — Consistent and correct implementation of external and internal interfaces at the hardware-software level

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

[a] Interface tests of the test object include tests of analogue and digital inputs and outputs, boundary tests and equivalence-class tests to completely test the specified interfaces, compatibility, timings and other specified ratings for the test object. Internal interfaces of an ECU can be tested by static tests for the compatibility of software and hardware as well as dynamic tests of Serial Peripheral Interface- (SPI) or Integrated Circuit- (IC) communications or any other interface between elements of an ECU.

8.4.2.2.5 This requirement applies to ASIL (A), (B), C, and D, in accordance with 4.3: the effectiveness of the hardware fault detection mechanisms' diagnostic coverage at the hardware-software level, with respect to the fault models, shall be demonstrated using feasible test methods given in Table 8.

NOTE For references to fault models, see ISO 26262-5:2011, Annex D.

Table 8 — Effectiveness of a safety mechanism's diagnostic coverage at the hardware-software level

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.

8.4.2.2.6 This requirement applies to ASIL (A), (B), (C), and D, in accordance with 4.3: the level of robustness of the elements at the hardware-software level shall be demonstrated using feasible test methods given in Table 9.

Table 9 — Level of robustness at the hardware-software level

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 System integration

8.4.3.1.1 The individual elements incorporated in the system shall be integrated in accordance with the system design, tested in accordance with the system integration tests and tested in accordance with the specified system integration tests of ISO 26262-5 and ISO 26262-6.

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

8.4.3.2 Test goals and test methods during system testing

8.4.3.2.1 To detect systematic faults during system integration, the test goals resulting from the requirements 8.4.3.2.2 to 8.4.3.2.6 shall be addressed by the application of adequate test methods, as given in the corresponding tables.

NOTE Depending on the function implemented, its complexity or the distributed nature of the system, it can be reasonable to move test methods to other integration subphases with adequate rationale.

8.4.3.2.2 The correct implementation of the functional and technical requirements at the system level shall be demonstrated using feasible test methods given in Table 10.

Table 10 — Correct implementation of functional safety and technical safety requirements at the system level

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 system. This can be done within the system 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.

8.4.3.2.3 This requirement applies to ASIL (A), (B), (C), and D, in accordance with 4.3: the correct functional performance, accuracy and timing of the safety mechanisms at the system level shall be demonstrated using feasible test methods given in Table 11.

Table 11 — Correct functional performance, accuracy and timing of safety mechanisms at the system level

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 (e.g. actuator speed or strength, whole system response times) of the safety mechanisms concerning the system.

8.4.3.2.4 The consistent and correct implementation of the external and internal interfaces at the system level shall be demonstrated using feasible test methods given in Table 12.

Table 12 — Consistent and correct implementation of external and internal interfaces at the system level

	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	Test of interaction/communication[b]	++	++	++	++

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

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

8.4.3.2.5 This requirement applies to ASIL (A), (B), C, and D, in accordance with 4.3: the effectiveness of the safety mechanisms' failure coverage at the system level shall be demonstrated using feasible test methods given in Table 13.

Table 13 — Effectiveness of a safety mechanism's failure coverage at the system level

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

[a] A fault injection test uses special means to introduce faults into the system. This can be done within the system 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 and field experience to anticipate errors in the system. 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 systems.

8.4.3.2.6 The level of robustness at the system level shall be demonstrated using feasible test methods given in Table 14.

Table 14 — Level of robustness at the system level

	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 system level resource, usage testing is usually performed in dynamic environments (e.g. lab cars or prototypes). Issues to test include power consumption and bus load.

[b] A stress test verifies the correct operation of the system under high operational loads or high demands from the environment. Therefore, tests under high loads on the system, 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 (e.g. see [2], [3]).

8.4.4 Vehicle integration and testing

8.4.4.1 Vehicle integration

8.4.4.1.1 The item shall be integrated into the vehicle and the vehicle integration tests shall be completed.

8.4.4.1.2 The verification of the interface specification of the item with the in-vehicle communication network and the in-vehicle power supply network shall be performed.

8.4.4.2 Test goals and test methods during vehicle testing

8.4.4.2.1 To detect systematic faults during vehicle integration, the test goals, resulting from the requirements 8.4.4.2.2 to 8.4.4.2.6, shall be addressed by the application of adequate test methods as given in the corresponding tables.

NOTE Depending on the function implemented, its complexity or the distributed nature of the item, it can be reasonable to move test methods to other integration subphases with adequate rationale.

8.4.4.2.2 The correct implementation of the functional safety requirements at the vehicle level shall be demonstrated using feasible test methods given in Table 15.

Table 15 — Correct implementation of the functional safety requirements at the vehicle level

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. These tests can have limitations if necessary to ensure the safety of the testers, e.g. with additional safety measures or disabled actuators.

8.4.4.2.3 This requirement applies to ASIL (A), (B), C, and D, in accordance with 4.3: the correct functional performance, accuracy and timing of the safety mechanisms at the vehicle level shall be demonstrated using feasible test methods given in Table 16.

Table 16 — Correct functional performance, accuracy and timing of safety mechanisms at the vehicle level

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 (e.g. fault tolerant time intervals and vehicle controllability in the presence of faults) of the safety mechanisms concerning the item.

[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. These tests can have limitations if necessary to ensure the safety of the testers, e.g. with additional safety measures or disabled actuators.

8.4.4.2.4 This requirement applies to ASIL (A), (B), C, and D, in accordance with 4.3: the consistency and correctness of the implementation of the external interfaces at the vehicle level shall be demonstrated using feasible test methods given in Table 17.

Table 17 — Consistent and correct implementation of internal and external interfaces at the vehicle level

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 vehicle systems 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.

8.4.4.2.5 This requirement applies to ASIL (A), (B), C, and D, in accordance with 4.3: the effectiveness of the safety mechanisms' failure coverage at the vehicle level shall be demonstrated using feasible test methods given in Table 18.

Table 18 — Effectiveness of a safety mechanism's failure coverage at the 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.

8.4.4.2.6 This requirement applies to ASIL (A), (B), C, and D, in accordance with 4.3: the level of robustness at the vehicle level shall be demonstrated using feasible test methods given in Table 19.

Table 19 — Level of robustness at the vehicle level

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 include 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 (e.g. see [2], [3]).

[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 Item integration and testing plan (refined) resulting from requirement 8.4.1.

8.5.2 Integration testing specification(s) resulting from requirements 8.4.1.

8.5.3 Integration testing report(s) resulting from requirements 8.4.2, 8.4.3 and 8.4.4.

9 Safety validation

9.1 Objectives

The first objective is to provide evidence of compliance with the safety goals and that the functional 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 the 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 in representative vehicle(s) aims to provide evidence of appropriateness for the intended use and aims to confirm the adequacy of the safety measures for a class or set of vehicles. Safety validation does cover assurance, that the safety goals are sufficient and have been achieved, based on examination and tests.

9.3 Inputs to this clause

9.3.1 Prerequisites

The following information shall be available:

— hazard analysis and risk assessment in accordance with ISO 26262-3:2011, 7.5.1;

— safety goals in accordance with ISO 26262-3:2011, 7.5.2; and

— functional safety concept in accordance with ISO 26262-3:2011, 8.5.1.

9.3.2 Further supporting information

The following information can be considered:

— project plan (refined) (see 5.5.1);

— technical safety concept (see 7.5.1);

— functional concept (from external source); and

— item integration and testing plan (refined) (see 8.5.1); and

— safety analysis reports (see 7.5.6).

9.4 Requirements and recommendation

9.4.1 Validation environment

9.4.1.1 The safety goals shall be validated for the item integrated in a representative vehicle.

NOTE This integrated item includes, where applicable: system; software; hardware; elements of other technologies, external measures.

9.4.2 Planning of validation

9.4.2.1 The validation plan shall be refined, including:

a) the configuration of the item subjected to validation including its calibration data in accordance with ISO 26262-6:2011, Annex C;

NOTE If a complete validation of each item configuration is not feasible, then a reasonable subset can be selected.

b) the specification of validation 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 as provided for verification testing (see ISO 26262-8:2011, 9.4.2 and 9.4.3) may be applied.

9.4.3.2 The safety goals of the item shall be validated at the vehicle level by evaluating the following:

a) the controllability;

NOTE Controllability can be validated using operating scenarios, including intended use and foreseeable misuse.

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

c) the effectiveness of the external measures; and

d) the effectiveness of the elements of other technologies.

9.4.3.3 This requirement applies to ASILs (B), C, and D of the safety goal: the validation of the metrics for random hardware failures shall be carried out at the item level for:

a) the evaluation of safety goal violations due to random hardware failures as determined in ISO 26262-5:2011, Clause 9, against the target values as defined by requirement 7.4.4.3; and

b) the evaluation of the hardware architectural metrics in accordance with the assessment criteria of ISO 26262-5:2011, Clause 8, against the target values as defined by requirement 7.4.4.2.

NOTE Quantitative evaluation for elements of the item is defined in ISO 26262-5:2011, 9.4.2 and 9.4.3. The whole item is evaluated qualitatively in case other technologies are involved in the item.

9.4.3.4 The validation at the vehicle level, based on the safety goals, the functional safety requirements and the intended use, shall be executed as planned using:

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

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

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

9.4.3.5 An appropriate set of the following methods shall be applied:

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

EXAMPLE 1 positive tests of functions and safety requirements, black box testing, simulation, tests under boundary conditions, fault injection, durability tests, stress tests, highly accelerated life testing (HALT), simulation of external influences.

b) analyses;

EXAMPLE 2 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; and

e) reviews.

9.4.4 Evaluation

9.4.4.1 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 organizational 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 in accordance with ISO 26262-2:2011, 6.5.3;

— safety plan (refined) in accordance with 5.5.2, ISO 26262-5:2011, 5.5.2 and ISO 26262-6:2011, 5.5.2;

— confirmation measure reports in accordance with ISO 26262-2:2011, 6.5.5;

— audit report if available in accordance with ISO 26262-2:2011, 6.5.4; and

— functional safety assessment plan (refined) in accordance with 5.5.5.

10.3.2 Further supporting information

None.

10.4 Requirements and recommendation

10.4.1 This requirement applies to ASILs (B), C, and D of the safety goal: for each step of the safety lifecycle in ISO 26262-2:2011, Figure 2, the specific topics to be addressed by the functional safety assessment shall be identified.

10.4.2 This requirement applies to ASILs (B), C, and D of the safety goal: the functional safety assessment shall be conducted in accordance with ISO 26262-2:2011, 6.4.9 (Functional safety assessment).

10.5 Work products

10.5.1 **Functional safety assessment report** resulting from requirements 10.4.1 and 10.4.2.

11 Release for production

11.1 Objectives

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

11.2 General

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

11.2.2 The evidence of compliance with the prerequisites for serial production is provided by:

— The completion of the verification and validation during the development at the hardware, software, system, item and vehicle level; and

— the successful overall assessment of functional safety.

11.2.3 This release documentation forms a basis for the production of the components, systems or vehicles, and is signed by the person responsible for the release.

11.3 Inputs to this clause

11.3.1 Prerequisites

The following information shall be available:

— functional safety assessment report in accordance with 10.5.1; and

— safety case in accordance with ISO 26262-2:2011, 6.5.3.

11.3.2 Further supporting information

None.

11.4 Requirements and recommendations

11.4.1 Release of production

11.4.1.1 The release for production of the item shall only be approved if the work products listed under 11.3.1 are available, if applicable (depending on the ASIL), and provide confidence of functional safety.

11.4.2 Documentation for release for production

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

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

b) the version(s) of the released item;

c) the configuration of the released item;

d) references to associated documents; and

e) the release date.

NOTE The documentation of functional safety can be part of the release for production documentation 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, and that shall be documented in accordance with ISO 26262-8:2011, Clause 10.

11.4.2.3 Identified safety anomalies shall be addressed in accordance with ISO 26262-2:2011, 5.4.2, and ISO 26262-8:2011, Clause 8.

11.5 Work products

11.5.1 Release for production report resulting from requirements 11.4.1 and 11.4.2.

Annex A
(informative)

Overview 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 subphases of product development at the system level.

Table A.1 — Overview of product development at the system level

Clause	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 will be included in the safety plan.	Project plan (refined) (see ISO 26262-2:2011, 6.5.2) Safety plan (see ISO 26262-2:2011, 6.5.1) Functional safety concept (see ISO 26262-3:2011, 8.5.1)	5.5.1 Project plan (refined) 5.5.2 Safety plan (refined) 5.5.3 Item integration and testing plan(s) 5.5.4 Validation plan 5.5.5 Functional safety assessment plan (refined)
6 Specification of the technical safety requirements	The first objective of this subphase is to specify the technical safety requirements. The technical safety requirements specification refines the functional safety concept, considering both the functional concept and the preliminary architectural assumptions (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 26262-3:2011, 8.5.1) Validation plan (see 5.5.4)	6.5.1 Technical safety requirements specification 6.5.2 System verification report 6.5.3 Validation plan (refined)
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.	Item integration and testing plan (see 5.5.3) Technical safety requirements specification (see 6.5.1)	7.5.1 Technical safety concept 7.5.2 System design specification 7.5.3 Hardware-software interface specification (HSI) 7.5.4 Specification of requirements for production, operation, service and decommissioning 7.5.5 System verification report (refined) 7.5.6 Safety analysis reports resulting from requirement 7.4.3

Table A.1 (*continued*)

Clause	Objectives	Prerequisites	Work products
8 Item integration and testing	The integration and testing phase comprises three phases and two primary goals as described below: the first phase is the integration of the hardware and software of each element that the item comprises. The second phase is the integration of the elements that comprise an item to form a complete system. The third phase is the integration of the item with other systems within a vehicle and with the vehicle itself. The first objective of the integration process is to test compliance with each safety requirement in accordance with its specification and ASIL classification. The second objective is to verify that the "System design" covering the safety requirements [see Clause 7 (System design)] are correctly implemented by the entire item.	Safety goals (see ISO 26262-3:2011, 7.5.2) Functional safety concept (see ISO 26262-3:2011, 8.5.1) Item integration and testing plan (see 5.5.3) Technical safety concept (see 7.5.1) System design specification (see 7.5.2) Hardware-software interface specification (HSI) (see 7.5.3)	8.5.1 Item integration and testing plan (refined) 8.5.2 Integration testing specification(s) 8.5.3 Integration testing report(s)
9 Safety validation	The first objective is to provide evidence of compliance with the safety goals and that the functional 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 the vehicle level.	Hazard analysis and risk assessment (see ISO 26262-3:2011, 7.5.1) Safety goals (see ISO 26262-3:2011, 7.5.2) Functional safety concept (see ISO 26262-3:2011, 8.5.1) Validation plan (refined) (see 6.5.3)	9.5.1 Validation plan (refined) resulting from requirement 9.4.2 9.5.2 Validation report resulting from requirements 9.4.3 to 9.4.4
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 26262-2:2011, 6.5.3) Safety plan (refined) (see 5.5.2, ISO 26262-5:2011, 5.5.2 and ISO 26262-6:2011, 5.5.2) Confirmation review reports (see ISO 26262-2:2011, 6.5.5) Audit report if available (see ISO 26262-2:2011, 6.5.5) Functional safety assessment plan (refined) (see 5.5.5)	10.5.1 Functional safety assessment report resulting from requirements 10.4.1 and 10.4.2
11 Product release	The objective of this clause is to specify the release for production criteria at the completion of the item development. The release for production confirms that the item complies with the requirements for functional safety at the vehicle level.	Functional safety assessment report (see 10.5.1) Safety case (see ISO 26262-2:2011, 6.5.3)	11.5.1 Release for production report resulting from requirements 11.4.1 and 11.4.2

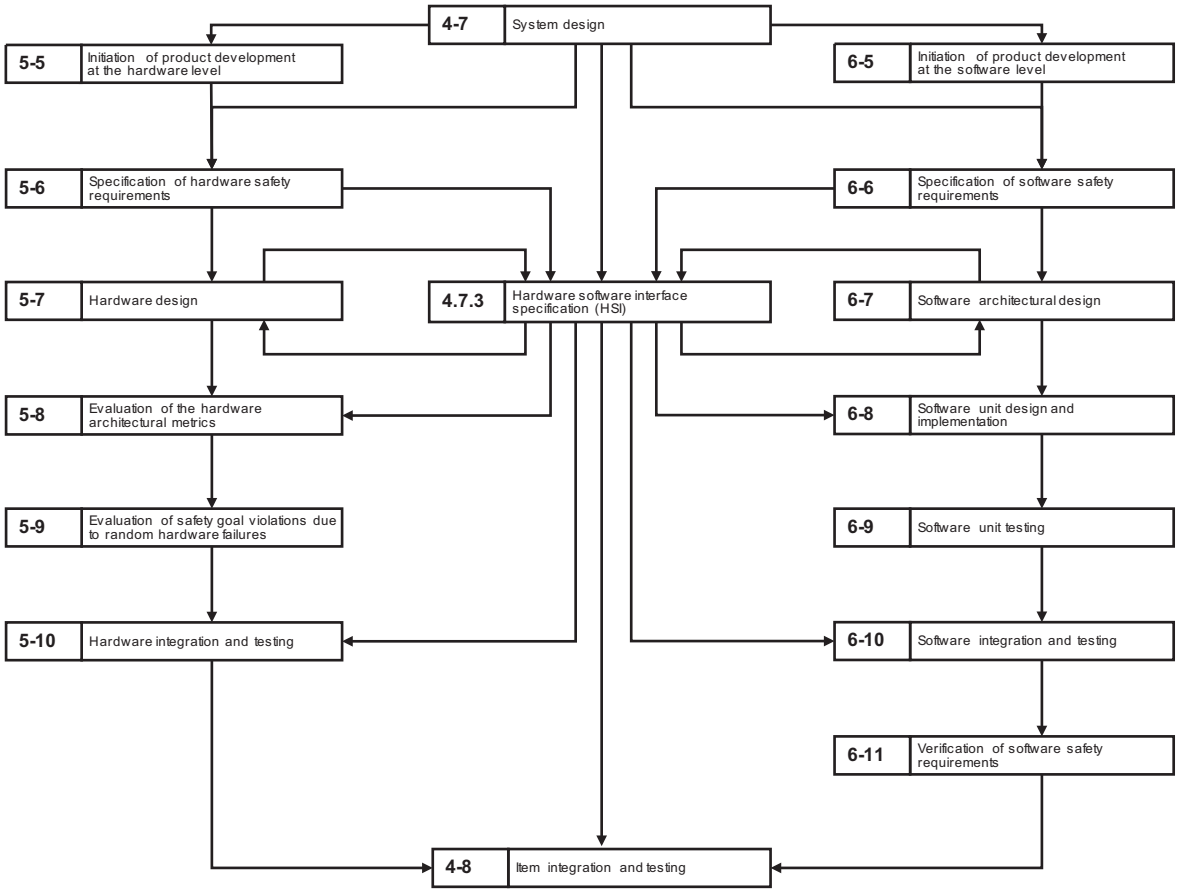
Annex B
(informative)

Example contents of hardware-software interface

B.1 This annex provides further explanation on the hardware-software interface.

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

First, an overview is given in Figure B.1 which provides the relationship between 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 topics relevant to both hardware and software development.



NOTE Within the figure, the specific clauses of each part of ISO 26262 are indicated in the following manner: “m-n”, where “m” represents the number of the part and “n” indicates the number of the clause, e.g. “3-6” represents Clause 6 of ISO 26262-3.

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

Second, to make specifying the hardware-software interface easier, a list of typical hardware-software interface elements is given as well as a non-exhaustive list of implementation characteristics implemented by the elements of the hardware-software interface.

B.2 The following hardware-software interface elements can 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. controller area network (CAN), local interconnect network (LIN), internal high-speed serial link (HSSL)];

c) converter:

   1) A/D converter;

   2) D/A converter;

   3) pulse-width modulation (PWM);

d) multiplexer;

e) electrical I/O;

f) watchdog:

   1) internal;

   2) external.

B.3 The following characteristics of the hardware-software interface can be considered when specifying the hardware-software interface:

a) interrupts;

b) timing consistency;

c) data integrity;

d) initialization:

   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.

Table B.1 provides an example to help with the allocation of hardware-software interface characteristics to hardware-software interface elements.

Table B.1 — Example for inputs of internal signals

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 to 5	0,50 %

Bibliography

[1] ISO 11451 (all parts), *Road vehicles — Vehicle test methods for electrical disturbances from narrowband radiated electromagnetic energy*

[2] IEC 61000-6-1, *Electromagnetic compatibility (EMC) — Part 6-1: Generic standards — Immunity for residential, commercial and light-industrial environments*

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

This page is intentionally blank.

This page is intentionally blank.

This page is intentionally blank.

ICS 43.040.10

Price based on 36 pages