INTERNATIONAL STANDARD

ISO 26262-5

First edition
2011-11-15

Road vehicles — Functional safety —

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

Véhicules routiers — Sécurité fonctionnelle —

Partie 5: Développement du produit au niveau du matériel

Reference number
ISO 26262-5:2011(E)

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 ... v
Introduction ... vi
1 Scope ... 1
2 Normative references ... 2
3 Terms, definitions and abbreviated terms ... 2
4 Requirements for compliance ... 2
4.1 General requirements ... 2
4.2 Interpretations of tables ... 3
4.3 ASIL-dependent requirements and recommendations ... 3
5 Initiation of product development at the hardware level ... 3
5.1 Objectives ... 3
5.2 General ... 4
5.3 Inputs to this clause ... 5
5.4 Requirements and recommendations ... 5
5.5 Work products ... 5
6 Specification of hardware safety requirements ... 5
6.1 Objectives ... 5
6.2 General ... 6
6.3 Inputs to this clause ... 6
6.4 Requirements and recommendations ... 6
6.5 Work products ... 8
7 Hardware design ... 8
7.1 Objectives ... 8
7.2 General ... 8
7.3 Inputs to this clause ... 9
7.4 Requirements and recommendations ... 9
7.5 Work products ... 13
8 Evaluation of the hardware architectural metrics ... 13
8.1 Objectives ... 13
8.2 General ... 13
8.3 Inputs of this clause ... 14
8.4 Requirements and recommendations ... 15
8.5 Work products ... 17
9 Evaluation of safety goal violations due to random hardware failures ... 18
9.1 Objectives ... 18
9.2 General ... 18
9.3 Inputs to this clause ... 18
9.4 Requirements and recommendations ... 19
9.5 Work products ... 26
10 Hardware integration and testing ... 26
10.1 Objectives ... 26
10.2 General ... 26
10.3 Inputs of this clause ... 26
10.4 Requirements and recommendations ... 27
10.5 Work products ... 29
Annex A (informative) **Overview of and workflow of product development at the hardware level** ... 30

Annex B (informative) **Failure mode classification of a hardware element** 32

Annex C (normative) **Hardware architectural metrics** 34

Annex D (informative) **Evaluation of the diagnostic coverage** 39

Annex E (informative) **Example calculation of hardware architectural metrics: “single-point fault metric” and “latent-fault metric”** 66

Annex F (informative) **Application of scaling factors** 72

Bibliography 75

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 26262-5 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.

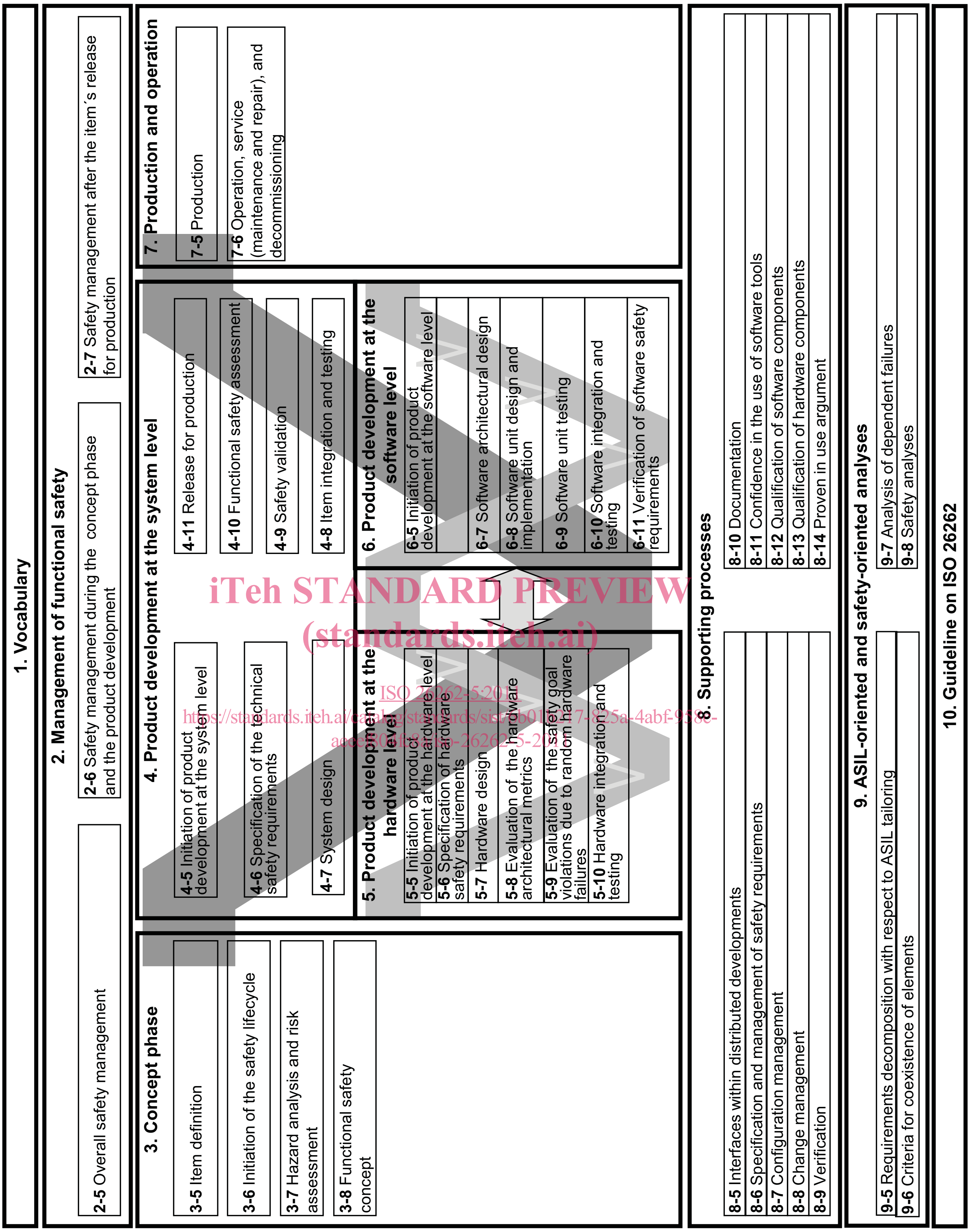

1. Vocabulary
2. Management of functional safety
2-5 Overall safety management
2-6 Safety management during the concept phase and the product development
2-7 Safety management after the item´s release for production
3. Concept phase
3-5 Item definition
3-6 Initiation of the safety lifecycle
3-7 Hazard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

Figure 1 — Overview of ISO 26262

Road vehicles — Functional safety —

Part 5: Product development at the hardware 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 hardware level for automotive applications, including the following:

- requirements for the initiation of product development at the hardware level,
- specification of the hardware safety requirements,
- hardware design,
- hardware architectural metrics, and
- evaluation of violation of the safety goal due to random hardware failures and hardware integration and testing.

The requirements of this part of ISO 26262 for hardware elements are applicable both to non-programmable and programmable elements, such as ASIC, FPGA and PLD. Furthermore, for programmable electronic elements, requirements in ISO 26262-6, ISO 26262-8:2011, Clause 11, and ISO 26262-8:2011, Clause 12, are applicable.

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

5.1 Objectives

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

This planning of hardware-specific safety activities is included in the safety plan (see ISO 26262-2:2011, 6.4.3, and ISO 26262-4:2011, 5.4).

5.2 General

The necessary activities and processes needed to develop hardware that meets the safety requirements are planned. Figure 2 illustrates the hardware level product development process steps in order to comply with the requirements of this part of ISO 26262, and the integration of these steps within the ISO 26262 framework.

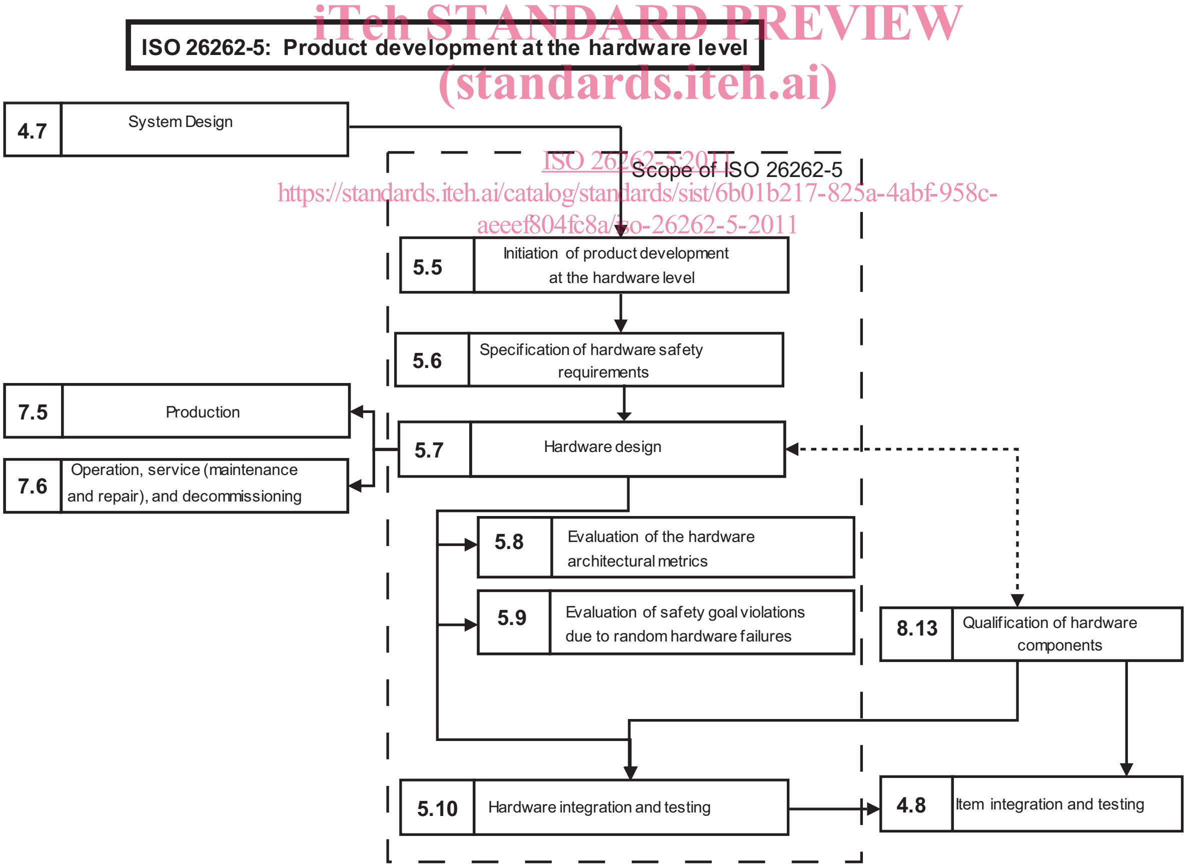
The necessary activities and processes for the product development at the hardware level include:

- the hardware implementation of the technical safety concept;
- the analysis of potential hardware faults and their effects; and
- the coordination with software development.

By contrast to the software development subphases, this part of ISO 26262 contains two clauses describing quantitative evaluations of the overall hardware architecture of the item.

Clause 8 describes two metrics to evaluate the effectiveness of the hardware architecture of the item and the implemented safety mechanisms to cope with random hardware failures.

As a complement to Clause 8, Clause 9 describes two alternatives to evaluate whether the residual risk of safety goal violations is sufficiently low, either by using a global probabilistic approach or by using a cut-set analysis to study the impact of each identified fault of a hardware element upon the violation of the safety goals.


ISO 26262-5: Product development at the hardware level
4.7
System Design
Scope of ISO 26262-5
5.5
Initiation of product development at the hardware level
5.6
Specification of hardware safety requirements
7.5
Production
5.7
Hardware design
7.6
Operation, service (maintenance and repair), and decommissioning
5.8
Evaluation of the hardware architectural metrics
5.9
Evaluation of safety goal violations due to random hardware failures
8.13
Qualification of hardware components
5.10
Hardware integration and testing
4.8
Item integration and testing

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. “4.7” represents Clause 7 of ISO 26262-4.

Figure 2 — Reference phase model for the product development at the hardware level

5.3 Inputs to this clause

5.3.1 Prerequisites

The following information shall be available:

- project plan (refined) in accordance with ISO 26262-4:2011, 5.5.1;
- safety plan (refined) in accordance with ISO 26262-4:2011, 5.5.2; and
- item integration and testing plan (refined) in accordance with ISO 26262-4:2011, 5.5.3.

5.3.2 Further supporting information

The following information can be considered:

- qualification report (of hardware components or parts), if applicable (see ISO 26262-8:2011, 13.5.3).

5.4 Requirements and recommendations

5.4.1 The safety plan in accordance with ISO 26262-2 shall be detailed, including determination of appropriate methods and measures, with respect to the activities for the product development at the hardware level, consistent with the planning of activities in ISO 26262-6.

5.4.2 The hardware development process for the hardware of the item, including methods and tools, shall be consistent across all subphases of the hardware development, and consistent with system and software subphases, so that the requirement flow retains its accuracy and consistency during the hardware development.

5.4.3 The tailoring of the safety lifecycle activities for product development at the hardware level shall be performed in accordance with ISO 26262-2:2011, 6.4.5, and based on the reference phase model given in Figure 2.

5.4.4 The reuse of hardware components, or the use of qualified hardware components or parts, shall be identified and the resulting tailoring of the safety activities shall be described.

5.5 Work products

5.5.1 **Safety plan** (refined) resulting from requirements 5.4.1 to 5.4.4.

6 Specification of hardware safety requirements

6.1 Objectives

The first objective of this clause is to specify the hardware safety requirements. They are derived from the technical safety concept and system design specification.

The second objective is to verify that the hardware safety requirements are consistent with the technical safety concept and the system design specification.

A further objective of this phase is to detail the hardware-software interface (HSI) specification initiated in ISO 26262-4:2011, Clause 7.

6.2 General

The technical safety requirements are allocated to hardware and software. The requirements that are allocated to both are further partitioned to yield hardware only safety requirements. The hardware safety requirements are further detailed, considering design constraints and the impact of these design constraints on the hardware.

6.3 Inputs to this clause

6.3.1 Prerequisites

The following information shall be available:

- safety plan (refined) in accordance with 5.5;
- technical safety concept in accordance with ISO 26262-4:2011, 7.5.1;
- system design specification in accordance with ISO 26262-4:2011, 7.5.2; and
- hardware-software interface specification in accordance with ISO 26262-4:2011, 7.5.3.

6.3.2 Further supporting information

The following information can be considered:

- software safety requirements specification (see ISO 26262-6:2011, 6.5.1).

6.4 Requirements and recommendations

6.4.1 A hardware safety requirements specification for the hardware elements of the item shall be derived from the technical safety requirements allocated to hardware.

6.4.2 The hardware safety requirements specification shall include each hardware requirement that relates to safety, including the following:

NOTE 1 The hardware safety requirements described in bullets a), b), c), or d) include the attributes needed to ensure the effectiveness of the above safety mechanisms.

a) the hardware safety requirements and relevant attributes of safety mechanisms to control internal failures of the hardware of the element, this includes internal safety mechanisms to cover transient faults when shown to be relevant due, for instance, to the technology used;

EXAMPLE 1 Attributes can include the timing and detection abilities of a watchdog.

b) the hardware safety requirements and relevant attributes of safety mechanisms to ensure the element is tolerant to failures external to the element;

EXAMPLE 2 The functional behaviour required for an ECU in the event of an external failure, such as an open-circuit on an input of the ECU.

c) the hardware safety requirements and relevant attributes of safety mechanisms to comply with the safety requirements of other elements;

EXAMPLE 3 Diagnosis of sensors or actuators.

d) the hardware safety requirements and relevant attributes of safety mechanisms to detect and signal internal or external failures; and

NOTE 2 The hardware safety requirements described in bullet d) include safety mechanisms to prevent faults from being latent.

EXAMPLE 4 The specified fault reaction time for the hardware part of a safety mechanism, so as to be consistent with the fault tolerant time interval.

e) the hardware safety requirements not specifying safety mechanisms.

EXAMPLE 5 Examples are:

- requirements on the hardware elements to meet the target values for random hardware failures as described in 6.4.3 and 6.4.4;
- requirements for the avoidance of a specific behaviour (for instance, “a particular sensor shall not produce an unstable output”);
- requirements allocated to hardware elements implementing the intended functionality; and
- requirements specifying design measures on harnesses or connectors.

6.4.3 This requirement applies to ASIL (B), C, and D of the safety goal. The target values specified to comply with ISO 26262-4:2011, Clause 7, for the metrics of Clause 8 of this part of ISO 26262 shall be considered when deriving values for the hardware elements of the item.

NOTE This activity can include a split of target values in the case of a distributed development as given in ISO 26262-8:2011, Clause 5.

6.4.4 This requirement applies to ASIL (B), C, and D of the safety goal. The target values specified to comply with ISO 26262-4:2011, Clause 7, for the procedures of Clause 9 of this part of ISO 26262 shall be considered when deriving values for the hardware elements of the item.

NOTE This activity can include a split of target values in the case of a distributed development as given in ISO 26262-8:2011, Clause 5.

6.4.5 The hardware safety requirements shall be specified in accordance with ISO 26262-8:2011, Clause 6.

6.4.6 The criteria for design verification of the hardware of the item or element shall be specified, including environmental conditions (temperature, vibration, EMI, etc.), specific operational environment (supply voltage, mission profile, etc.) and component specific requirements:

a) for verification by qualification for hardware components or part of intermediate complexity, the criteria shall meet the needs of ISO 26262-8:2011, Clause 13, and

b) for verification by testing, the criteria shall meet the needs of Clause 10.

6.4.7 The hardware safety requirements shall comply with the fault tolerant time interval for safety mechanisms as specified in ISO 26262-4:2011, 6.4.2.3.

6.4.8 The hardware safety requirements shall comply with the multiple-point fault detection interval as specified in ISO 26262-4:2011, 6.4.4.2.

NOTE 1 In the case of ASIL C and D safety goals, and if the corresponding safety concept does not prescribe specific values, the multiple-point fault detection intervals can be specified to be equal or lower than the item's “power-up to power-down” cycle.

NOTE 2 Appropriate multiple-point fault detection intervals can also be justified by the quantitative analysis of the occurrence of random hardware failures (see Clause 9).