INTERNATIONAL STANDARD

ISO 26262-8

First edition
2011-11-15

Road vehicles — Functional safety —

Part 8: Supporting processes

Véhicules routiers — Sécurité fonctionnelle —

Partie 8: Processus d'appui

Reference number
ISO 26262-8:2011(E)

COPYRIGHT PROTECTED DOCUMENT

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

Published in Switzerland

Contents

Page

Foreword

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

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

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

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

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

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

— *Part 1: Vocabulary*

— *Part 2: Management of functional safety*

— *Part 3: Concept phase*

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

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

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

— *Part 7: Production and operation*

— *Part 8: Supporting processes*

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

— *Part 10: Guideline on ISO 26262*

Introduction

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

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

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

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

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

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

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

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

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

e) provides requirements for relations with suppliers.

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

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

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

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

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

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

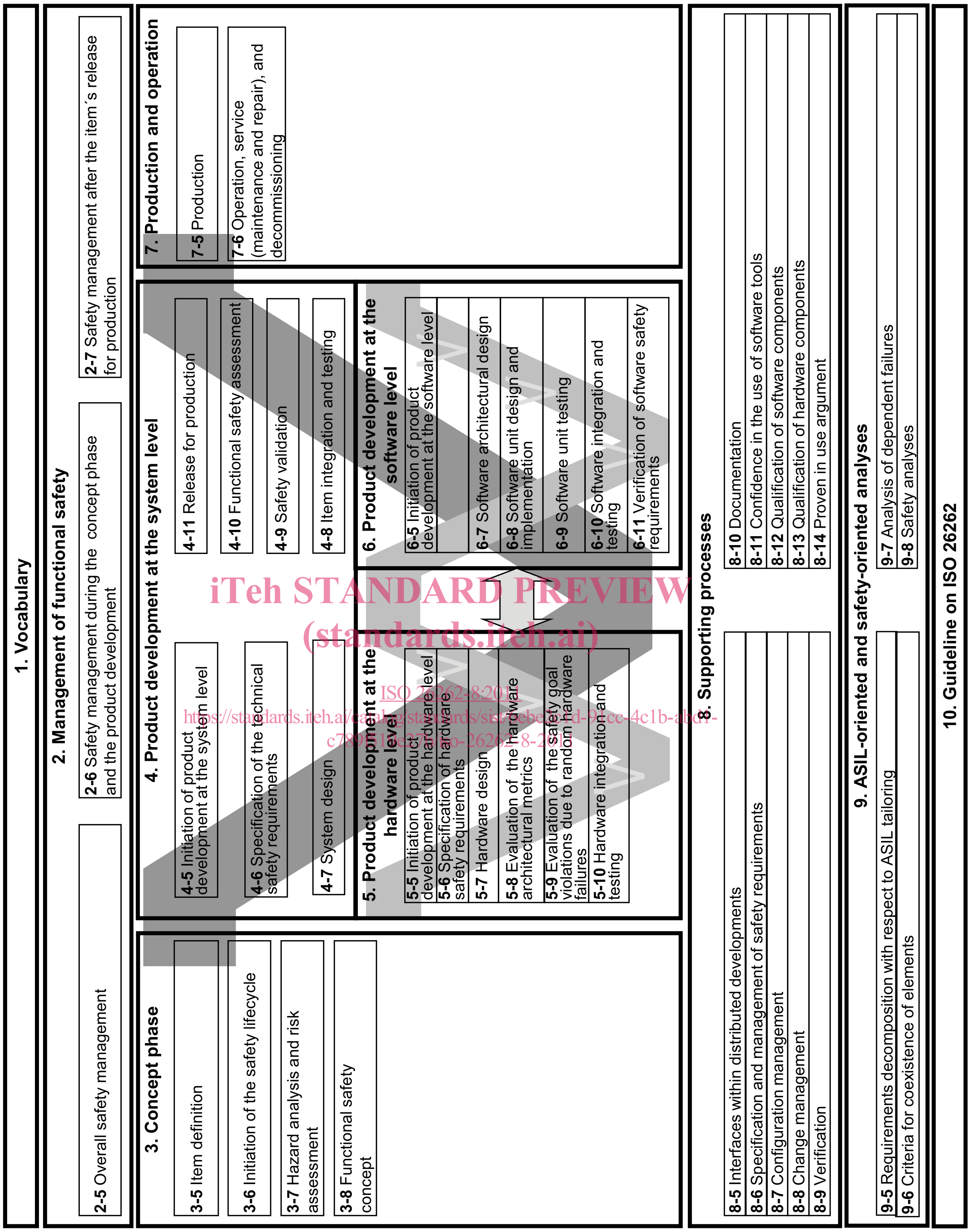

Figure 1 — Overview of ISO 26262

Road vehicles — Functional safety —

Part 8: **Supporting processes**

1 Scope

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

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

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

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

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

— interfaces within distributed developments,

— overall management of safety requirements,

— configuration management,

— change management,

— verification,

— documentation,

— confidence in the use of software tools,

— qualification of software components,

— qualification of hardware components, and

— proven in use argument.

2 Normative references

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

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

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

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

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

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

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

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

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

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

3 Terms, definitions and abbreviated terms

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

4 Requirements for compliance

4.1 General requirements

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

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

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

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

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

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

4.2 Interpretations of tables

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

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

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

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

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

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

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

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

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

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

4.3 ASIL-dependent requirements and recommendations

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

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

5 Interfaces within distributed developments

5.1 Objectives

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

5.2 General

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

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

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

5.3 Inputs to this clause

5.3.1 Prerequisites

See applicable prerequisites of the relevant phases of the safety lifecycle for which a distributed development is planned and carried out.

5.3.2 Further supporting information

The following information can be considered:

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

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

5.4 Requirements and recommendations

5.4.1 Application of requirements

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

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

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

5.4.1.2 Requirements on the customer-supplier relationship (interfaces and interactions) shall apply to each level of the customer-supplier relationship.

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

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

5.4.2 Supplier selection criteria

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

NOTE Supplier selection criteria includes:

— evidence of the supplier's quality management system;

— the supplier's past performance and quality;

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

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

— recommendations from the development, production, quality and logistics departments of the vehicle manufacturer as far as they impact functional safety.

5.4.2.2 The RFQ from the customer to the supplier candidates shall include:

a) a formal request to comply with ISO 26262,

b) the item definition or functional specification of the element, and

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

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

5.4.3 Initiation and planning of distributed development

5.4.3.1 The customer and the supplier shall specify a DIA including the following:

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

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

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

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

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

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

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

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

e) the parties or persons responsible for the activities,

f) the communication of the target values, derived from the system level targets, to each relevant party in order for them to meet the target values for single-point faults metric and latent faults metric in accordance with the evaluation of the hardware architectural metrics and the evaluation of safety goal violations due to random hardware failures (see ISO 26262-5), and

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

5.4.3.2 If the supplier conducts the hazard analysis and risk assessment, then the hazard analysis and risk assessment shall be provided to the customer for verification.

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

5.4.4 Execution of distributed development

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

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

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

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

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

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

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

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

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

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

5.4.5 Functional safety assessment at supplier's premises

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

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

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

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

NOTE This can be done by the supplier itself.

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

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

5.4.6 After release for production

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

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

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

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

5.5 Work products

5.5.1 **Supplier selection report** resulting from requirements 5.4.2.1 and 5.4.2.2.

5.5.2 **Development interface agreement (DIA)** resulting from requirement 5.4.3.

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

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

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

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

6 Specification and management of safety requirements

6.1 Objectives

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

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

6.2 General

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

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