DRAFT INTERNATIONAL STANDARD ISO/DIS 26262-9

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

Voting begins on:
2009-07-08

Voting terminates on:
2009-12-08

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

Road vehicles — Functional safety —

Part 9:
ASIL-oriented and safety-oriented analyses

Véhicules routiers — Sécurité fonctionnelle —

Partie 9: Analyses liées aux ASIL et à la sécurité

ICS 43.040.10

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

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

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

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

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

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

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

PDF disclaimer

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

Adobe is a trademark of Adobe Systems Incorporated.

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

Contents

Page

Foreword iv
Introduction v
1 Scope 1
2 Normative references 1
3 Terms, definitions, abbreviated terms 2
4 Requirements for compliance 2
4.1 General requirements 2
4.2 Interpretations of tables 2
4.3 ASIL dependent requirements and recommendations 2
5 Requirements decomposition with respect to ASIL tailoring 3
5.1 Objectives 3
5.2 General 3
5.3 Inputs to this clause 4
5.4 Requirements and recommendations 4
5.5 Work products 8
6 Criteria for coexistence of elements 8
6.1 Objectives 8
6.2 General 8
6.3 Inputs to this clause 8
6.4 Requirements and recommendations 9
6.5 Work products 9
7 Analysis of dependent failures 9
7.1 Objectives 9
7.2 General 10
7.3 Inputs to this clause 10
7.4 Requirements and recommendations 10
7.5 Work products 12
8 Safety analyses 12
8.1 Objectives 12
8.2 General 12
8.3 Inputs to this clause 13
8.4 Requirements and recommendations 14
8.5 Work products 15
Annex A (informative) Overview on and document flow of ASIL-oriented and safety-oriented analyses 16
Bibliography 17

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 26262-9 was prepared by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee SC 3, *Electrical and electronic equipment*.

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

- *Part 1: Vocabulary*
- *Part 2: Management of functional safety*
- *Part 3: Concept phase*
- *Part 4: Product development: system level*
- *Part 5: Product development: hardware level*
- *Part 6: Product development: software level*
- *Part 7: Production and operation*
- *Part 8: Supporting processes*
- *Part 9: ASIL-oriented and safety-oriented analyses*
- *Part 10: Guideline for ISO 26262*

Introduction

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

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

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

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

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

ISO 26262:

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

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

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

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

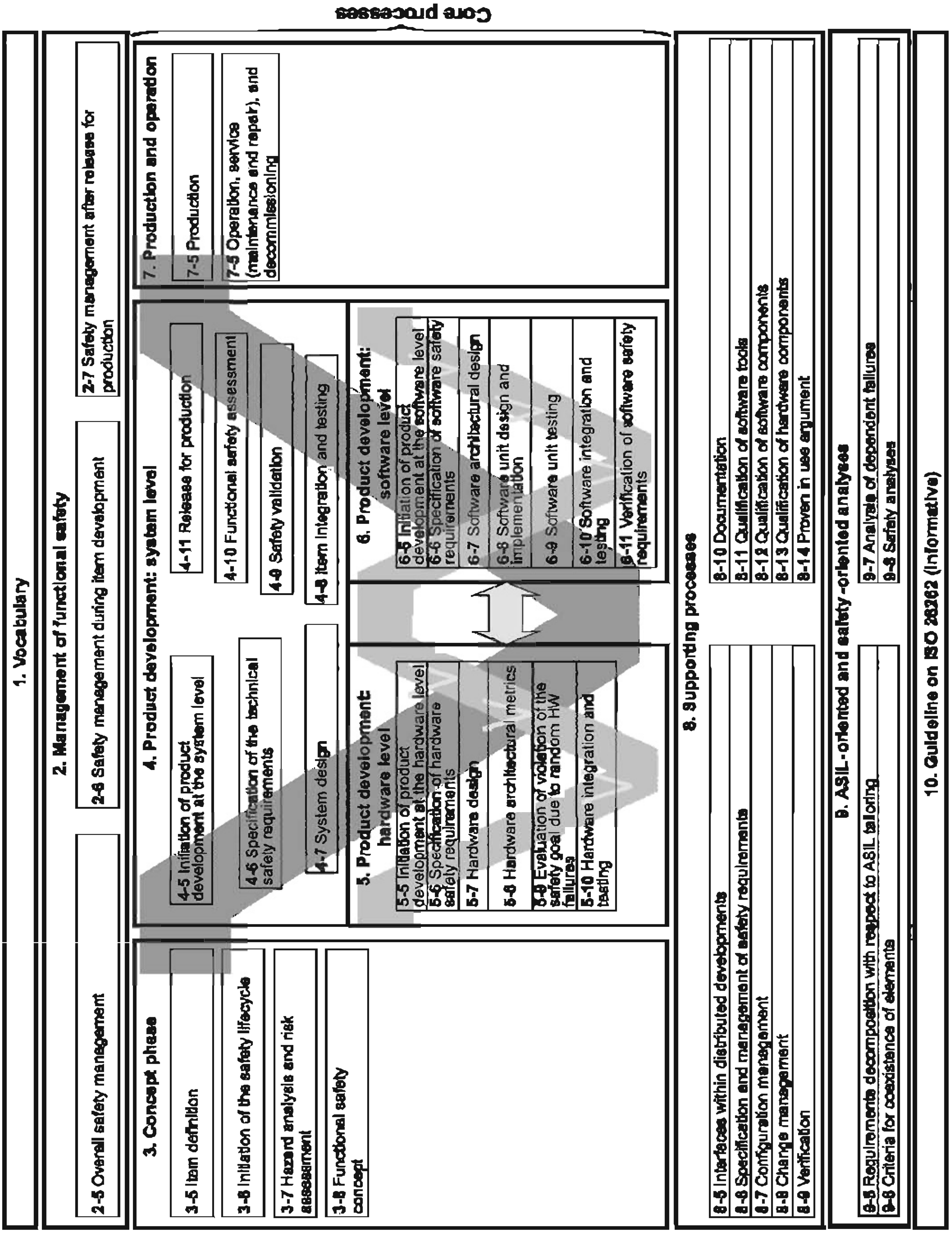
1. Vocabulary
2. Management of functional safety
2-5 Overall safety management
2-6 Safety management during item development
2-7 Safety management after release for production
3. Concept phase
3-5 Item definition
3-6 Initiation of the safety lifecycle
3-7 Hazard analysis and risk assessment
3-8 Functional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

Figure 1 — Overview of ISO 26262

DRAFT INTERNATIONAL STANDARD ISO/DIS 26262-9

Road vehicles — Functional safety — Part 9: ASIL-oriented and safety-oriented analyses

1 Scope

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

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

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

This Part of the International Standard specifies the requirements for ASIL-oriented and safety-oriented analyses. These include ASIL decomposition, criteria for coexistence of elements of different ASIL, analysis of dependent failures, and safety analyses.

2 Normative references

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

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

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

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

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

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

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

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

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

[1] To be published

3 Terms, definitions, abbreviated terms

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

4 Requirements for compliance

4.1 General requirements

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

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

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

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

4.2 Interpretations of tables

Tables may be normative or informative depending on their context.

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

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

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

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

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

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

“+“ The method is recommended for this ASIL.

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

4.3 ASIL dependent requirements and recommendations

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

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

5 Requirements decomposition with respect to ASIL tailoring

5.1 Objectives

The objective of this clause is to provide rules and guidance for decomposing safety requirements into redundant safety requirements to allow ASIL tailoring at the next level of detail.

5.2 General

The ASIL of the safety goals of an item under development is assured throughout the item's development process. Starting from safety goals, the safety requirements are derived and detailed during the development phases. The ASIL, as an attribute of the safety goal, is inherited by each subsequent safety requirement. The functional and technical safety requirements are allocated to architectural elements, starting with preliminary architectural assumptions and ending with the hardware and software elements.

The method of ASIL tailoring during the design process given in ISO 26262 is called "ASIL decomposition". During the allocation process, benefit can be obtained from architectural decisions and the existence of independent architectural elements. This offers the opportunity:

— to implement safety requirements redundantly by these independent architectural elements; and

— to assign a potentially lower ASIL to these redundant safety requirements.

If there is no independence between the elements, the ASIL of the safety goal is inherited by each requirement and element.

NOTE 1 ASIL decomposition is an ASIL tailoring measure that can be applied to the functional, technical, hardware or software safety requirements of the item or system.

NOTE 2 As a basic rule, the application of ASIL decomposition requires redundancy of safety requirements allocated to architectural elements that are sufficiently independent.

NOTE 3 In the case of use of homogenous redundancy (e.g. by duplicated device or duplicated software) the ASIL with respect to systematic failures of hardware and software cannot be reduced unless an analysis of dependent failures shows sufficient independence or that the potential common causes lead to a safe state. Therefore, homogenous redundancy is in general not sufficient for reducing the ASIL due to the lack of independence between the elements.

In general ASIL decomposition allows apportioning of the ASIL of a safety requirement between several elements that ensure compliance with the same safety requirement addressing the same safety goal. ASIL decomposition between an intended functionality and its corresponding safety requirements is allowed under certain conditions (see 5.4.4).

The requirements on the hardware architecture metrics and on the probability of violation of safety goals due to random hardware failures remain unchanged by ASIL decomposition (see ISO 26262-5:—, Clauses 8 and 9).

ASIL decomposition may be performed in the following subphases: ISO 26262-3:—, Clause 8 "Functional safety concept", ISO 26262-4:—, Clause 7 "System design", ISO 26262-5:—, Clause 7 "Hardware design", and ISO 26262-6:—, Clause 7 "Software architectural design". If a need for decomposition arises during the software or the hardware design, it is recommended to ensure the correct application of decomposition at the system level.

ASIL decomposition addresses systematic failures related to system, hardware, or software elements.

5.3 Inputs to this clause

5.3.1 Prerequisites

The following information shall be available:

- safety requirements at the applied system, hardware or software level (see ISO 26262-3:— 8.5.1, ISO 26262-4:— 6.5.1, ISO 26262-5:— 6.5.1, or ISO 26262-6:— 6.5.1);

- architectural information at the applied system, hardware or software level (see ISO 26262-4:— 7.5.2, ISO 26262-5:— 7.5.1, or ISO 26262-6:— 7.5.1).

5.3.2 Further supporting information

The following information may be considered:

- item definition (see ISO 26262-3:— 5.5);

- safety goals (see ISO 26262-3:— 7.5.2).

5.4 Requirements and recommendations

5.4.1 ASIL decomposition shall be performed considering each allocated safety requirement of the element.

NOTE If several requirements with identical ASIL are allocated to the same independent elements, the results of several ASIL decompositions can be combined. However, the ASIL decomposition described in this clause applies to each individual safety requirement.

5.4.2 Initial safety requirements shall be implemented by sufficiently independent elements and redundant safety requirements shall be derived for each of these elements.

NOTE 1 The derived safety requirements, allocated to each independent element, are able to comply with the initial safety requirement by themselves. This provides a sufficient argument for redundancy.

NOTE 2 Redundancy can be applied as information redundancy, time redundancy, hardware redundancy or software redundancy. Moreover, Diverse redundancy is distinguished from homogeneous redundancy where:

- diverse redundancy is used to cope with both systematic failures and random hardware failures; and

- homogeneous redundancy is used to cope with random hardware failures only.

5.4.3 If ASIL decomposition is applied at the software level, appropriate measures shall be taken at the system and the hardware level to show sufficient independence.

5.4.4 If ASIL decomposition is applied by apportioning the intended functionality and its associated safety mechanism the following shall be complied with:

a) the associated safety mechanism should be assigned the highest decomposed ASIL;

b) the intended functionality shall become a safety requirement and implemented applying its decomposed ASIL;

c) the effectiveness of the safety mechanism for its purpose shall be shown.

NOTE If the decomposition scheme ASIL x + QM(x) is chosen; QM(x) means that the quality management system used for the development of the corresponding element is able to support the demonstration of independence. Application of ISO 26262-8:—, Clause 6 is not required in this case.

5.4.5 If functions are used that do not result in a safe state by switching them off, sufficient availability of the decomposed item or element shall be shown.

5.4.6 ASIL decomposition of each safety requirement shall apply:

a) one of the decomposition schemes given in 5.4.7;

b) each step from one level of the selected decomposition scheme to the lower next level defines one decomposition of the ASIL;

c) the decompositions resulting in lower ASILs than those given in 5.4.7 shall not be applied; the decompositions resulting in higher ASILs may be applied;

NOTE 1 The methods and measures given in ISO 26262-4:— "Product development: system level", ISO 26262-5:— "Product development: hardware level" and ISO 26262-6:— "Product development: software level" only support the given or higher decompositions, not the lower ones.

d) ASIL decomposition may be applied more than once provided that the decomposition schemes given in 5.4.7 or higher decompositions are used;

e) each decomposed ASIL shall be marked by giving the ASIL of the safety goal in parenthesis.

EXAMPLE If an ASIL D is decomposed into one ASIL C and one ASIL A, then these are marked as "ASIL C(D)" and "ASIL A(D)". If the resulting ASIL C(D) is decomposed into one ASIL B and one ASIL A, then these are also marked with the ASIL of the safety goal as "ASIL B(D)" and "ASIL A(D)".

NOTE 2 This notation does not imply hidden requirements.

5.4.7 One of the decomposition schemes given in Figure 2 shall be chosen in accordance with the ASIL before decomposition:

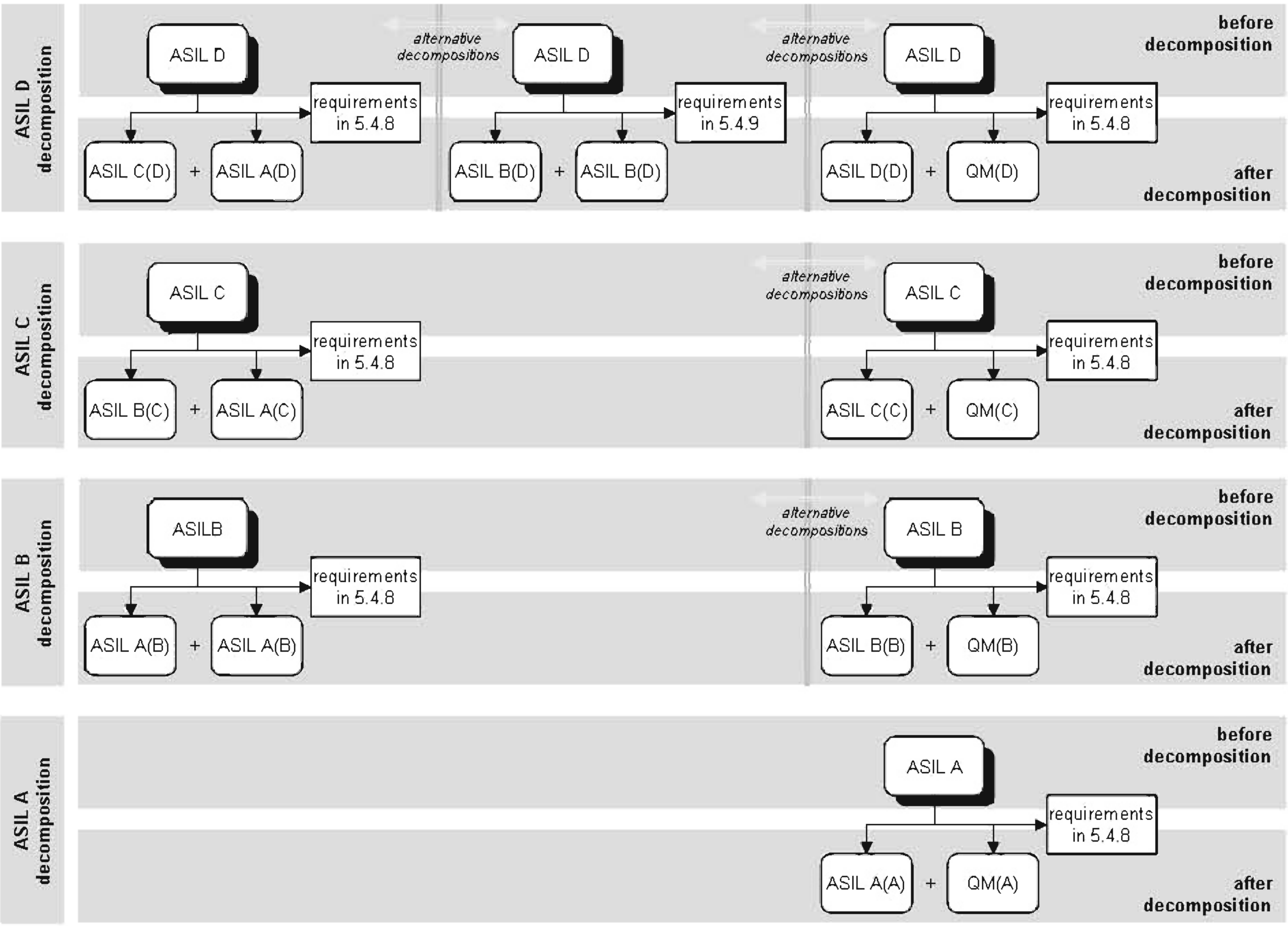

Figure 2 — Classification scheme of ASILs when decomposing safety requirements

NOTE 1 The uppermost box of each decomposition step in Figure 2 (shadowed box "before decomposition") represents the ASIL before decomposition

NOTE 2 The case where a safety requirement is apportioned into an intended functionality (QM) and its associated safety mechanism (ASIL) is shown in the rightmost column in Figure 2

a) ASIL D shall be decomposed either as

1) one ASIL C(D) and one ASIL A(D); or as

2) one ASIL B(D) and one ASIL B(D); or as

3) one ASIL D(D) and one QM(D);

b) ASIL C shall be decomposed either as

1) one ASIL B(C) and one ASIL A(C); or as

2) one ASIL C(C) and one QM(C);

c) ASIL B shall be decomposed either as

1) one ASIL A(B) and one ASIL A(B); or as

2) one ASIL B(B) and one QM(B);

d) ASIL A shall not be further decomposed, except, if needed, as one ASIL A(A) and one QM(A).

5.4.8 When using the decomposition schemes given in 5.4.7, with the exception of the scheme in 5.4.7 a) 2), the following methods and processes shall be applied:

a) confirmation measures (see ISO 26262-2:—, 6.4.6) shall be applied in compliance with the ASIL of the safety goal;

b) independence of the elements after decomposition shall be justified;

NOTE 1 The elements are justified as independent if the analysis of dependent failures (see Clause 7) does not find a cause of dependent failures that can lead to the violation of a safety requirement before decomposition, or if each identified cause of dependent failures is controlled by an adequate safety measure at the ASIL of the safety goal.

NOTE 2 Special attention is to be paid to elements ensuring the channel selection or switching if ASIL decomposition is applied to multi-channel architectural designs.

c) if the ASIL of the safety goal is either ASIL C or ASIL D, quantitative evaluation in accordance with ISO 26262-5:—, Clauses 8 and 9 shall be performed.

5.4.9 When using the decomposition scheme for ASIL D given in 5.4.7 a) 2), the following methods and processes shall be applied:

a) confirmation measures (see ISO 26262-2:—, 6.4.6) shall be applied in compliance with ASIL D;

b) independence of the elements after decomposition shall be justified;

NOTE 1 The elements are justified as independent if the analysis of dependent failures (see Clause 7) does not find a cause of dependent failures that can lead to the violation of a safety requirement before decomposition, or if each identified cause of dependent failures is controlled by an adequate safety measure at the ASIL of the safety goal.

c) overall management of the derived safety requirements (see ISO 26262-8:—, Clause 6) allocated to the independent elements shall be implemented in compliance with ASIL C;

NOTE 2 The rigour in requirements management is more important for ASIL C than for ASIL B.

d) test and integration of each decomposed elements shall be implemented in compliance with ASIL C;

NOTE 3 The recommended measures for avoidance of systematic failures in bullets c) and d) are more effective for ASIL C than for ASIL B, and redundancy alone is not sufficient if the applied measures are not effective enough.

e) if credit is taken from the use of software tools and if the same tools are used for the development of the decomposed elements (see ISO 26262-8:—, Clause 11), then these software tools shall be qualified in compliance with ASIL D;

f) quantitative evaluation given in ISO 26262-5:—, Clauses 8 and 9 shall be performed in compliance with ASIL D.

5.4.10 Product development of the decomposed elements at the system level (see ISO 26262-4:—), at the hardware level (see ISO 26262-5:—) and at the software level (see ISO 26262-6:—) may be performed in compliance with the ASIL after decomposition.

5.4.11 At each level of the design process at which decomposition is applied, the corresponding integration activities of the decomposed elements and subsequent activities shall be applied at the ASIL before decomposition.

5.5 Work products

5.5.1 Update of architectural information, resulting from subclause 5.4.2 (see ISO 26262-4:— 7.5.2, ISO 26262-5:— 7.5.1, or ISO 26262-6:— 7.5.1)

5.5.2 Update of ASIL as attribute of safety requirements and elements, resulting from subclauses 5.4.6 and 5.4.7.

6 Criteria for coexistence of elements

6.1 Objectives

This clause is intended to provide criteria for coexistence within the same element of:

- safety-related sub-elements with non-safety-related ones; and
- safety-related sub-elements assigned different ASILs.

6.2 General

By default, when an element is composed of several sub-elements, each of those sub-elements is developed in accordance with the measures corresponding to the highest ASIL applicable to this element.

In the case of coexistence of sub-elements with different ASILs or safety-related sub-element(s) with non-safety-related one(s), it can be beneficial to avoid raising the ASIL for some of them to the ASIL of the parent element.

For this purpose, this clause provides guidance for determining the potential of each of its sub-elements for violating any safety requirement that is allocated to it. It is based on demonstration of freedom from interference: the coexistence of a sub-element with the rest of an element is allowed or not allowed, depending on its degree of interference with the rest of this element.

This clause may be applied at any step of refinement of the design process, in parallel with the progress of allocation of the safety requirements to the elements and sub-elements of an architecture; typically during sub phases "System design" (see ISO°26262-4:—, Clause 7), "Hardware design" (see ISO°26262-5:—, Clause 7) or "Software architectural design" (see ISO°26262-6:—, Clause 7).

6.3 Inputs to this clause

6.3.1 Prerequisites

The following information shall be available:

- safety requirements at the applied element level;
- architectural information at the applied element level.

6.3.2 Further supporting information

The following information may be considered:

— none

6.4 Requirements and recommendations

6.4.1 The requirements of this clause shall be applied after the assignment of ASIL to the sub-elements of the element being analysed.

NOTE ASIL assignment results from allocation of safety requirements to the elements either by default inheritance or by ASIL decomposition,

6.4.2 The following shall be considered during analysis of an element:

a) each of the safety requirements allocated to the element;

b) each of the sub-elements that are part of the element.

6.4.3 Coexistence of non-safety-related sub-elements within an element

A non-safety-related sub-element coexisting in the same element with safety-related sub-element(s) shall only be treated as a QM sub-element, if:

a) this sub-element has no functional dependency with any of the safety requirements allocated to the element; and

b) it does not interfere with any other safety-related sub-elements of the element.

Otherwise, this non-safety-related sub-element shall be assigned the highest ASIL of the coexisting safety-related sub-elements for which freedom from interference is not shown.

6.4.4 Coexistence of safety-related sub-elements with different ASILs within an element

In the case of coexistence in the same element of safety-related sub-elements with different ASILs, a sub-element shall only be treated as a lower ASIL sub-element if it is shown that it does not interfere with any other sub-element assigned a higher ASIL, for each of the safety requirements allocated to the element.

Otherwise, it shall be assigned the highest ASIL of the coexisting safety-related sub-elements for which freedom from interference is not shown.

6.5 Work products

6.5.1 Results of application of coexistence criteria, resulting from subclauses 6.4.3 and 6.4.4.

7 Analysis of dependent failures

7.1 Objectives

The analysis of dependent failures aims to identify any single event or single cause that could bypass or invalidate the independence or freedom from interference between elements of an item required to comply with its safety goals.

7.2 General

The scope of analysis of dependent failures is architectural features such as:

a) similar and dissimilar redundant elements;

b) different functions implemented with identical software or hardware elements;

c) functions and their respective safety mechanisms;

d) partitions of functions or software elements;

e) physical distance between hardware elements, with or without barrier.

According to the definitions given in ISO 26262-1:—, independence is threatened by common cause failures and cascading failures, while freedom from interference is only threatened by cascading failures.

EXAMPLE A high intensity electromagnetic field that causes different electronic devices to fail in a way that depends on design and use is an example of a common cause failure. Biased vehicle speed information that affects the behaviour of one or more vehicle functions is an example of cascading failures.

Dependent failures can manifest themselves simultaneously, or within a sufficiently short time interval, to have the effect of simultaneous failures. For example, a monitor designed to detect anomalous behaviour of a function can be rendered inoperative some time before the monitored function fails if both the monitor and the monitored function are subjected to the same event or cause.

7.3 Inputs to this clause

7.3.1 Prerequisites

The following information shall be available:

- requirements for independence at the applied level;
- requirements for freedom from interference at the applied level;
- architectural information at the applied level;
- boundaries of the analyses of dependent failures.

7.3.2 Further supporting information

The following information may be considered:

- none

7.4 Requirements and recommendations

7.4.1 Identification of potential for dependent failures

The potential for dependent failures shall be identified from the results of safety analyses (see Clause 8).

NOTE 1 The identification can be based on deductive safety analyses: examination of cut sets or repeated identical events of an FTA or an equivalent method provide useful information about the potential for dependent failures.

NOTE 2 The identification of potential for dependent failures can also be supported by inductive safety analyses: similar parts or components with analogous failure modes that appear several times in an FMEA, or equivalent method, give additional information about the potential for dependent failures.

7.4.2 Evaluation of potential for dependent failures

7.4.2.1 Each identified potential for dependent failures shall be evaluated to determine if a reasonably foreseeable cause exists which will cause the dependent failures to occur and violate a safety goal or a safety requirement.

NOTE 1 The potential for dependent failures relates to systematic faults. This evaluation of potential is based on qualitative analysis methods.

NOTE 2 When a quantitative evaluation of hardware random failures is required, as in ISO 26262-5:—, Clause 9, the contribution of common cause failures needs to be estimated on a case by case basis because no general and sufficiently reliable method exists for quantifying such failures.

7.4.2.2 This evaluation shall consider the operational situations as well as the different operating modes of the item or element under consideration.

7.4.2.3 This evaluation shall consider the following topics:

a) hardware failures;

b) development faults, e.g. those related to item or element requirements, software design and implementation, hardware design and implementation, in relation to new technology and change application;

c) manufacturing faults, e.g. those related to processes, procedures, training, control plans, monitoring of special characteristics, including flashing, end-of-line programming;

d) installation faults, e.g. those related to wiring routing, inter-changeability of parts, failures of adjacent items or elements;

e) repair faults, e.g. those related to processes, procedures, training, trouble shooting, inter-changeability of parts, backward compatibility;

f) environmental factors, e.g. temperature, vibration, pressure, humidity / condensation, pollution, corrosion, contamination, EMC;

g) failures of common external resources, e.g. power supply, input data, intersystem data bus and communication;

h) stress due to specific situations, e.g. wear, ageing.

NOTE 1 This evaluation can be supported by appropriate checklists, i.e. checklists based on field experience. Those checklists aim to provide the analysts with representative examples of root causes and coupling factors such as: same design, same process, same component, same interface, proximity.

NOTE 2 The evaluation of the potential for dependent failures can also be supported by demonstration of adherence to process guidelines when those are intended to prevent the introduction of root causes and coupling factors that could lead to dependent failures.

7.4.3 Resolution of dependent failures

7.4.3.1 Measures for resolution of relevant dependent failures shall be specified during the development phase using a change request, as described in ISO°26262-8:—, Clause 8.

NOTE Relevant dependent failures are those for which the evaluation in accordance with 7.4.2 has revealed a reasonably foreseeable cause.

7.4.3.2 Measures for resolution shall include assumptions and rationale regarding the dependent failures, their impact and suggested measures for preventing their root causes, reducing the coupling factors or controlling their effects.

7.4.3.3 Change requests, resulting from analysis of dependent failures, shall be sent back as input to the sub-phases of the safety lifecycle for which analysis of dependent failures is applied.

7.5 Work products

7.5.1 Results of analyses of dependent failures, resulting from subclauses 7.4.1 and 7.4.2

7.5.2 Change requests for confirmed dependent failures, resulting from subclause 7.4.3

8 Safety analyses

8.1 Objectives

The objective of safety analyses is to examine the consequences of faults and failures on items and elements considering their functions, behaviour and design. Safety analyses also provide information on conditions and causes that could lead to violation of a safety goal or safety requirement.

Additionally, the safety analyses also contribute to the identification of new functional or non-functional hazards not previously considered during hazard analysis and risk assessment.

8.2 General

The scope of the safety analyses includes:

- verification of safety concepts and safety requirements;
- identification of conditions and causes, including faults and failures, that could lead to violation of a safety goal or safety requirement;
- identification of additional requirements for detection of those faults or failures;
- determination of the required responses (actions/measures) to those detected faults or failures;
- identification of additional requirements for verifying that the safety goals or safety requirements are satisfied, including safety-related vehicle testing.

Safety analyses are performed at the appropriate level of abstraction during the concept and product development phases. Quantitative analysis methods are used to predict the frequency of failures while qualitative analysis methods identify failures but do not predict the frequency of failures. Both types of analysis methods depend upon the knowledge of fault types and fault models.

The methods available for qualitative analyses include:

- qualitative FMEA: system, design or process;
- qualitative FTA;
- ETA.

NOTE 1 The qualitative analysis methods listed above can be applied to software where no more appropriate software-specific analysis methods exist.

Quantitative analyses usually complement qualitative analyses. They are useful in estimating the likelihood of violation of a safety goal due to hardware random failures, and require additional knowledge of quantitative failure rates of hardware elements and their combinations.

The methods available for quantitative analyses include:

- quantitative FMEA;
- quantitative FTA;
- ETA;
- Markov models;
- reliability block diagrams.

NOTE 2 The quantitative analyses only address random failures of hardware. These are not applicable to systematic failures.

Another criteria for classification of safety analysis methods is given by the way they are conducted:

- inductive safety analysis methods are bottom-up methods that start from known causes to forecast unknown effects;
- deductive safety analysis methods are top-down methods that start from known effects to seek unknown causes.

EXAMPLE System, design and process FMEA, ETA, Markov modelling are inductive methods. FTA and reliability block diagrams are deductive methods.

8.3 Inputs to this clause

8.3.1 Prerequisites

The following information shall be available:

- safety requirements at the applied level;
- architectural information at the applied level;
- boundaries of the safety analyses.

8.3.2 Further supporting information

The following information may be considered:

- purpose of the safety analyses;
- fault models.

8.4 Requirements and recommendations

8.4.1 The safety analyses shall be performed in accordance with appropriate standards or guidelines.

8.4.2 The results of the safety analyses shall indicate if the respective safety goals or safety requirements are complied with or not.

8.4.3 If a safety goal or a safety requirement is not complied with, the results of the safety analyses shall be used for deriving prevention, detection or effect mitigation measures regarding faults or failures causing the violation.

8.4.4 The measures derived from the safety analyses shall be implemented as part of the product development at the system level, at the hardware level or at the software level, respectively in accordance with ISO°26262-4:—, ISO°26262-5:— or ISO°26262-6:—.

8.4.5 If new hazards are identified by safety analyses during product development, the hazard analysis and risk assessment shall be updated, and applicable and subsequent activities shall be repeated as necessary. Such hazards and the resulting development activities shall be treated in accordance with the change management process in ISO°26262-8:—, Clause 8.

8.4.6 The fault models used for the safety analyses shall be consistent with the fault models used for ISO°26262-5:—, Clauses 7, 8 and 9, Moreover, the random or systematic nature of faults shall be considered.

8.4.7 The results of the safety analyses and fault models shall be used to determine the need for additional safety-related test cases.

8.4.8 The results of the safety analyses shall be documented and reviewed in accordance with ISO°26262-2:—, Table°1.

8.4.9 Qualitative analyses

The qualitative analyses shall include:

a) a systematic identification of faults or failures that could lead to violation of safety goals or safety requirements, originating in:

- the item or element itself;
- the interaction of the item or element with other items or element;
- the usage of the item or element;

b) the evaluation of the consequence(s) of each identified fault to determine the potential to violate safety goals or safety requirements;

c) the identification of the cause(s) of each identified fault;

d) the identification of potential weaknesses of safety mechanisms.

NOTE The examination of interactions with other items or elements, within and outside the item, is done in order to assess the degree of independence or interference.

8.4.10 Quantitative analyses

8.4.10.1 If applicable, the quantitative analyses shall include:

a) quantitative values to support the evaluation of quantitative targets assigned at the item level;

b) a systematic identification of faults or failures that could lead to violation of safety goals or safety requirements;

c) the identification of possible weaknesses of the redundancy concept (e.g. common cause failures, latent faults) and of the safety mechanisms;

d) the diagnostic interval, emergency operation time, and time between fault detection and repair.

8.4.10.2 If qualitative safety analyses are applied to prove the compliance with quantitative requirements, the level of detail within these analyses shall be chosen appropriately.

NOTE “Appropriately" means that the failure rate at the lowest level of detail still has to reflect the failure rate of the item, i.e. it does not affect the failure rate of the item more favourably than justifiable.

8.5 Work products

8.5.1 Results of safety analyses, resulting from 8.4.9 and 8.4.10.

Annex A
(informative)

Overview on and document flow of ASIL-oriented and safety-oriented analyses

Table A.1 provides an overview on objectives, prerequisites and work products of ASIL-oriented and safety-oriented analyses.

Table A.1 — ASIL-oriented and safety-oriented analyses: overview

Clause	Title	Objectives	Prerequisites	Work products
5	Requirements decomposition with respect to ASIL tailoring	The objective of this clause is to provide rules and guidance for decomposing safety requirements into redundant safety requirements to allow ASIL tailoring at the next level of detail.	- Safety requirements at the applied system, hardware or software level - Architectural information at the applied system, hardware or software level	5.5.1 Update of architectural information 5.5.2 Update of ASIL as attribute of safety requirements and elements
6	Criteria for coexistence of elements	This clause is intended to provide criteria for coexistence within the same element of: - safety-related sub-elements with non-safety-related ones; and - safety-related sub-elements assigned different ASILs.	- Safety requirements at the applied element level; - Architectural information at the applied element level.	6.5.1 Results of application of coexistence criteria
7	Analysis of dependent failures	The analysis of dependent failures aims to identify any single event or single cause that could bypass or invalidate the independence or freedom from interference between elements of an item required to comply with its safety goals.	- Requirements for independence at the applied level - Requirements for freedom from interference at the applied level - Architectural information at the applied level - Boundaries of the analyses of dependent failures	7.5.1 Results of analyses of dependent failures 7.5.2 Change requests for confirmed dependent failures
8	Safety analyses	The objective of safety analyses is to examine the consequences of faults and failures on items and elements considering their functions, behaviour and design. Safety analyses also provide information on conditions and causes that could lead to violation of a safety goal or safety requirement. Additionally, the safety analyses also contribute to the identification of new functional or non-functional hazards not previously considered during hazard analysis and risk assessment.	- Safety requirements at the applied level; - Architectural information at the applied level; - Boundaries of the safety analyses.	8.5.1 Results of safety analyses

Bibliography

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