INTERNATIONAL STANDARD

ISO 26262-9

Second edition
2018-12

Road vehicles — Functional safety —

Part 9: https://www.kekaoxing.com Automotive safety integrity level (ASIL)-oriented and safety-oriented analyses

Véhicules routiers — Sécurité fonctionnelle —

Partie 9: Analyses liées aux niveaux d'intégrité de sécurité automobile (ASIL) et à la sécurité

Reference number
ISO 26262-9:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: 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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html .

This document was prepared by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee SC 32, *Electrical and electronic components and general system aspects*.

This edition of ISO 26262 series of standards cancels and replaces the edition ISO 26262:2011 series of standards, which has been technically revised and includes the following main changes:

— requirements for trucks, buses, trailers and semi-trailers;

— extension of the vocabulary;

— more detailed objectives;

— objective oriented confirmation measures;

— management of safety anomalies;

— references to cyber security;

— updated target values for hardware architecture metrics;

— guidance on model based development and software safety analysis;

— evaluation of hardware elements;

— additional guidance on dependent failure analysis;

— guidance on fault tolerance, safety related special characteristics and software tools;

— guidance for semiconductors;

— requirements for motorcycles; and

— general restructuring of all parts for improved clarity.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

A list of all parts in the ISO 26262 series can be found on the ISO website.

Introduction

The ISO 26262 series of standards is the adaptation of IEC 61508 series of standards to address the sector specific needs 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 in the development of road vehicles. Development and integration of automotive functionalities strengthen the need for functional safety and the need to provide evidence that functional 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, these being considered within the scope of functional safety. ISO 26262 series of standards includes guidance to mitigate these risks by providing appropriate requirements and processes.

To achieve functional safety, the ISO 26262 series of standards:

a) provides a reference for the automotive safety lifecycle and supports the tailoring of the activities to be performed during the lifecycle phases, i.e., development, production, operation, service and decommissioning;

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

c) uses ASILs to specify which of the requirements of ISO 26262 are applicable to avoid unreasonable residual risk;

d) provides requirements for functional safety management, design, implementation, verification, validation and confirmation measures; and

e) provides requirements for relations between customers and suppliers.

The ISO 26262 series of standards is concerned with functional safety of E/E systems that is achieved through safety measures including safety mechanisms. It also provides a framework within which safety-related systems based on other technologies (e.g. mechanical, hydraulic and pneumatic) can be considered.

The achievement of 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 the management processes.

Safety is intertwined with common function-oriented and quality-oriented activities and work products. The ISO 26262 series of standards addresses the safety-related aspects of these activities and work products.

Figure 1 shows the overall structure of the ISO 26262 series of standards. The ISO 26262 series of standards 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 among ISO 26262-3, ISO 26262-4, ISO 26262-5, ISO 26262-6 and ISO 26262-7;

— for motorcycles:

  — ISO 26262-12:2018, Clause 8 supports ISO 26262-3;

  — ISO 26262-12:2018, Clauses 9 and 10 support ISO 26262-4;

— 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 ISO 26262-2:2018, Clause 6.

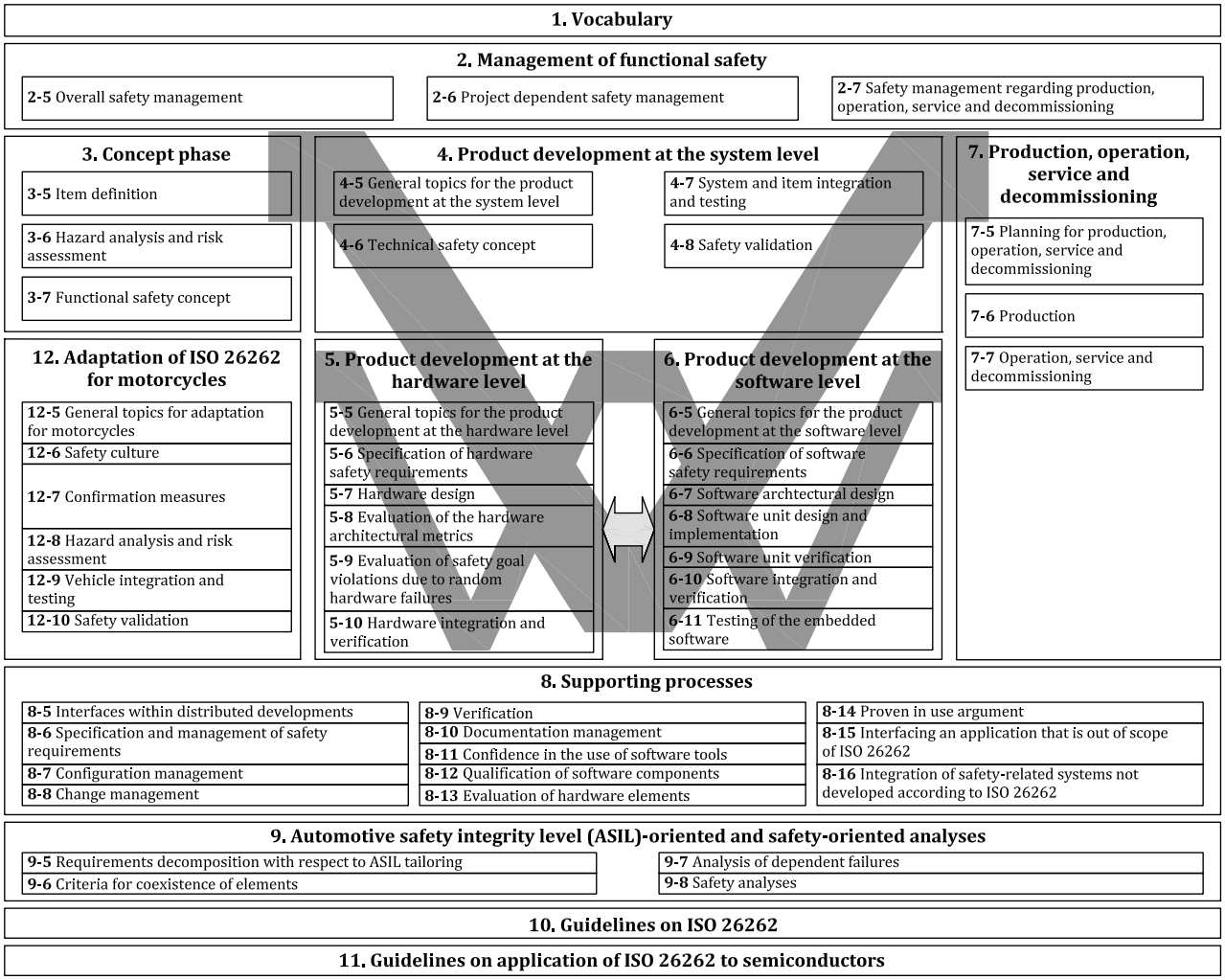

Figure 1 — Overview of the ISO 26262 series of standards

Road vehicles — Functional safety —

Part 9: Automotive safety integrity level (ASIL)-oriented and safety-oriented analyses

1 Scope

This document 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 road vehicles, excluding mopeds. This document does not address unique E/E systems in special vehicles such as E/E systems designed for drivers with disabilities.

NOTE Other dedicated application-specific safety standards exist and can complement the ISO 26262 series of standards or vice versa.

Systems and their components released for production, or systems and their components already under development prior to the publication date of this document, are exempted from the scope of this edition. This document addresses alterations to existing systems and their components released for production prior to the publication of this document by tailoring the safety lifecycle depending on the alteration. This document addresses integration of existing systems not developed according to this document and systems developed according to this document by tailoring the safety lifecycle.

This document addresses possible hazards caused by malfunctioning behaviour of safety-related E/E 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 safety-related E/E systems.

This document describes a framework for functional safety to assist the development of safety-related E/E systems. This framework is intended to be used to integrate functional safety activities into a company-specific development framework. Some requirements have a clear technical focus to implement functional safety into a product; others address the development process and can therefore be seen as process requirements in order to demonstrate the capability of an organization with respect to functional safety.

This document does not address the nominal performance of E/E systems.

This document specifies the requirements for Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses, including the following:

— requirements decomposition with respect to ASIL tailoring;

— criteria for coexistence of elements;

— analysis of dependent failures; and

— safety analyses.

Annex A provides an overview on objectives, prerequisites and work products of this document.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 26262-1:2018, *Road vehicles — Functional safety — Part 1: Vocabulary*

ISO 26262-2:2018, *Road vehicles — Functional safety — Part 2: Management of Functional Safety*

ISO 26262-3:2018, *Road vehicles — Functional safety — Part 3: Concept phase*

ISO 26262-4:2018, *Road vehicles — Functional safety — Part 4: Product development at the system level*

ISO 26262-5:2018, *Road vehicles — Functional safety — Part 5: Product development at the hardware level*

ISO 26262-6:2018, *Road vehicles — Functional safety — Part 6: Product development at the software level*

ISO 26262-7:2018, *Road vehicles — Functional safety — Part 7: Production, operation, service and decommissioning*

ISO 26262-8:2018, *Road vehicles — Functional safety — Part 8: Supporting processes*

3 Terms and definitions

For the purposes of this document, the terms, definitions and abbreviated terms given in ISO 26262-1:2018 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at https://www.iso.org/obp

4 Requirements for compliance

4.1 Purpose

This clause describes how:

a) to achieve compliance with the ISO 26262 series of standards;

b) to interpret the tables used in the ISO 26262 series of standards; and

c) to interpret the applicability of each clause, depending on the relevant ASIL(s).

4.2 General requirements

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

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

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

Informative content, including notes and examples, 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 the ISO 26262 series of standards 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.

4.3 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 listed highly recommended and recommended methods in accordance with the ASIL apply. It is allowed to substitute a highly recommended or recommended method by others not listed in the table, in this case, a rationale shall be given describing why these comply with the corresponding requirement. If a rationale can be given to comply with the corresponding requirement without choosing all entries, a further rationale for omitted methods is not necessary.

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 or even a selected single method 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; and

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

4.4 ASIL-dependent requirements and recommendations

The requirements or recommendations of each sub-clause shall be met 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 Clause 5, the ASIL resulting from the decomposition shall be met.

If an ASIL is given in parentheses in the ISO 26262 series of standards, the corresponding sub-clause 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.

4.5 Adaptation for motorcycles

For items or elements of motorcycles for which requirements of ISO 26262-12 are applicable, the requirements of ISO 26262-12 supersede the corresponding requirements in this document. Requirements of ISO 26262-2 that are superseded by ISO 26262-12 are defined in Part 12.

4.6 Adaptation for trucks, buses, trailers and semi-trailers

Content that is intended to be unique for trucks, buses, trailers and semi-trailers (T&B) is indicated as such.

5 Requirements decomposition with respect to ASIL tailoring

5.1 Objectives

If ASIL decomposition is applied, the objectives of this clause are:

a) to ensure that a safety requirement is decomposed into redundant safety requirements at the next level of detail, and that these are allocated to sufficiently independent design elements; and

b) to apply ASIL decomposition according to permitted ASIL decomposition schemas.

NOTE The independence mentioned in this clause is technical independence and not organizational independence (see ISO 26262-1:2018, 3.78)

5.2 General

The ASIL of the safety goals of an item under development is propagated throughout the item's development. Starting from safety goals, the safety requirements are derived and refined during the development phases. The ASIL, as an attribute of the safety goal, is inherited by each subsequent safety requirement. The safety requirements are allocated to architectural elements, starting with functional safety requirements allocated to elements of system architectural design and finally resulting in safety requirements allocated to the hardware and/or software elements.

ASIL decomposition is a method of ASIL tailoring during the concept and development phases. During the safety requirements allocation process, benefit can be obtained from architectural decisions including the existence of sufficiently 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 (some of) these decomposed safety requirements.

If the architectural elements are not sufficiently independent, then the redundant requirements and the architectural elements inherit the initial ASIL.

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

In general, ASIL decomposition allows the 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 mechanism is allowed under certain conditions (see 5.4.7).

The requirements specific to the random hardware failures, including the evaluation of the hardware architectural metrics and the evaluation of safety goal violations due to random hardware failures (see ISO 26262-5:2018, Clause 8 and Clause 9) remain unchanged by ASIL decomposition.

An example architecture decomposition is given in Annex B.

5.3 Inputs to this clause

5.3.1 Prerequisites

The following information shall be available:

— the safety requirements at the level at which the ASIL decomposition is to be applied: vehicle, system, hardware, or software in accordance with ISO 26262-3:2018, 7.5.1, or ISO 26262-4:2018, 6.5.1, or ISO 26262-5:2018, 6.5.1 or ISO 26262-6:2018, 6.5.1; and

— the architectural information at the level at which the ASIL decomposition is to be applied: vehicle, system, hardware, or software in accordance with ISO 26262-3:2018, 7.5.1, or ISO 26262-4:2018, 6.5.3, or ISO 26262-5:2018, 7.5.1, or ISO 26262-6:2018, 7.5.1.

5.3.2 Further supporting information

The following information can be considered:

— item definition (see ISO 26262-3:2018, 5.5.1); and

— safety goals included in the hazard analysis and risk assessment report (see ISO 26262-3:2018, 6.5.1).

5.4 Requirements and recommendations

5.4.1 If ASIL decomposition is applied, all the requirements within this clause shall be complied with.

5.4.2 ASIL decomposition shall be performed by considering each initial safety requirement individually.

NOTE 1 Several safety requirements can be allocated to the same independent elements as the result of ASIL decompositions of different initial safety requirements.

5.4.3 The initial safety requirement shall be decomposed to redundant safety requirements, that shall be implemented by sufficiently independent elements. These elements are sufficiently independent if the analysis of dependent failures (see Clause 7) does not find a plausible cause of dependent failures that can lead to the violation of an initial safety requirement, or if each identified cause of dependent failures is controlled by an adequate safety measure according to the ASIL of the initial safety requirement.

NOTE 1 A given decomposed requirement can be the result of the decomposition of several initial safety requirements.

NOTE 2 The use of homogenous redundancy to implement the decomposed requirements (e.g. by duplicated device or duplicated software) does not address the systematic failures of hardware and software. This prevents the ASIL from being reduced, unless an analysis of dependent failures (see Clause 7) provides evidence that sufficient independence (see ISO 26262-1:2018, 3.78) exists or that the potential common causes lead to a safe state. Therefore, homogenous redundancy alone is, in general, not sufficient for reducing the ASIL without the support of the analysis of dependent failures for the specific system context.

NOTE 3 In general, ASIL decomposition does not apply to elements ensuring the channel selection or switching in multi-channel architectural designs.

5.4.4 Each decomposed safety requirement shall comply with the initial safety requirement by itself.

NOTE 1 This provides redundancy by definition.

NOTE 2 If a decomposed safety requirement is allocated to a safety mechanism, the effectiveness of this safety mechanism is considered in the evaluation of the compliance of the decomposed requirement with the initial safety requirement.

EXAMPLE An ASIL D requirement allocated to a given ECU might naively be decomposed between an ASIL D requirement allocated to a simple watchdog in this ECU and a QM safety requirement allocated to the microprocessor of the ECU. However, this simple watchdog is insufficient to cover the failure modes of a microprocessor with regard to an ASIL D requirement. In this case, this watchdog does not effectively comply with the initial safety requirement.

5.4.5 The requirements on the evaluation of the hardware architectural metrics and the evaluation of safety goal violations due to random hardware failures in accordance with ISO 26262-5 shall remain unchanged by ASIL decomposition.

5.4.6 If ASIL decomposition is applied at the software level, sufficient independence between the elements implementing the decomposed requirements shall be verified at the system level. If necessary, additional measures shall be taken at the software level, hardware level, or system level to achieve sufficient independence.

5.4.7 If ASIL decomposition of an initial safety requirement results in the allocation of decomposed requirements to the intended functionality and an associated safety mechanism, then:

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

NOTE 1 In general, the safety mechanisms have a lower complexity and lower size than the intended functionality.

b) a safety requirement shall be allocated to the intended functionality and implemented applying the corresponding decomposed ASIL.

NOTE 2 If the decomposition schema ASIL x(x) + QM(x) is chosen, then QM(x) means that the quality management system is sufficient to develop element(s) that implement the safety requirement allocated to the intended functionality.

5.4.8 When applying ASIL decomposition to a safety requirement:

a) ASIL decomposition shall be applied in accordance with 5.4.9;

b) ASIL decomposition may be applied more than once (in this case, the intermediate requirement allocation step may be omitted); and

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

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

5.4.9 One of the following decomposition schemas outlined below shall be chosen in accordance with the ASIL before decomposition (as shown in Figure 2). A decomposition schema resulting in higher ASILs may also be used.

NOTE 1 The step from one level of the selected decomposition schema to the lower next level defines one decomposition of the ASIL.

a) An ASIL D requirement shall be decomposed as one of the following:

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

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

3) one ASIL D(D) requirement and one QM(D) requirement.

b) An ASIL C requirement shall be decomposed as one of the following:

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

2) one ASIL C(C) requirement and one QM(C) requirement.

c) An ASIL B requirement shall be decomposed as one of the following:

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

2) one ASIL B(B) requirement and one QM(B) requirement.

d) An ASIL A shall only be decomposed, if needed, as one ASIL A(A) requirement and one QM(A) requirement.

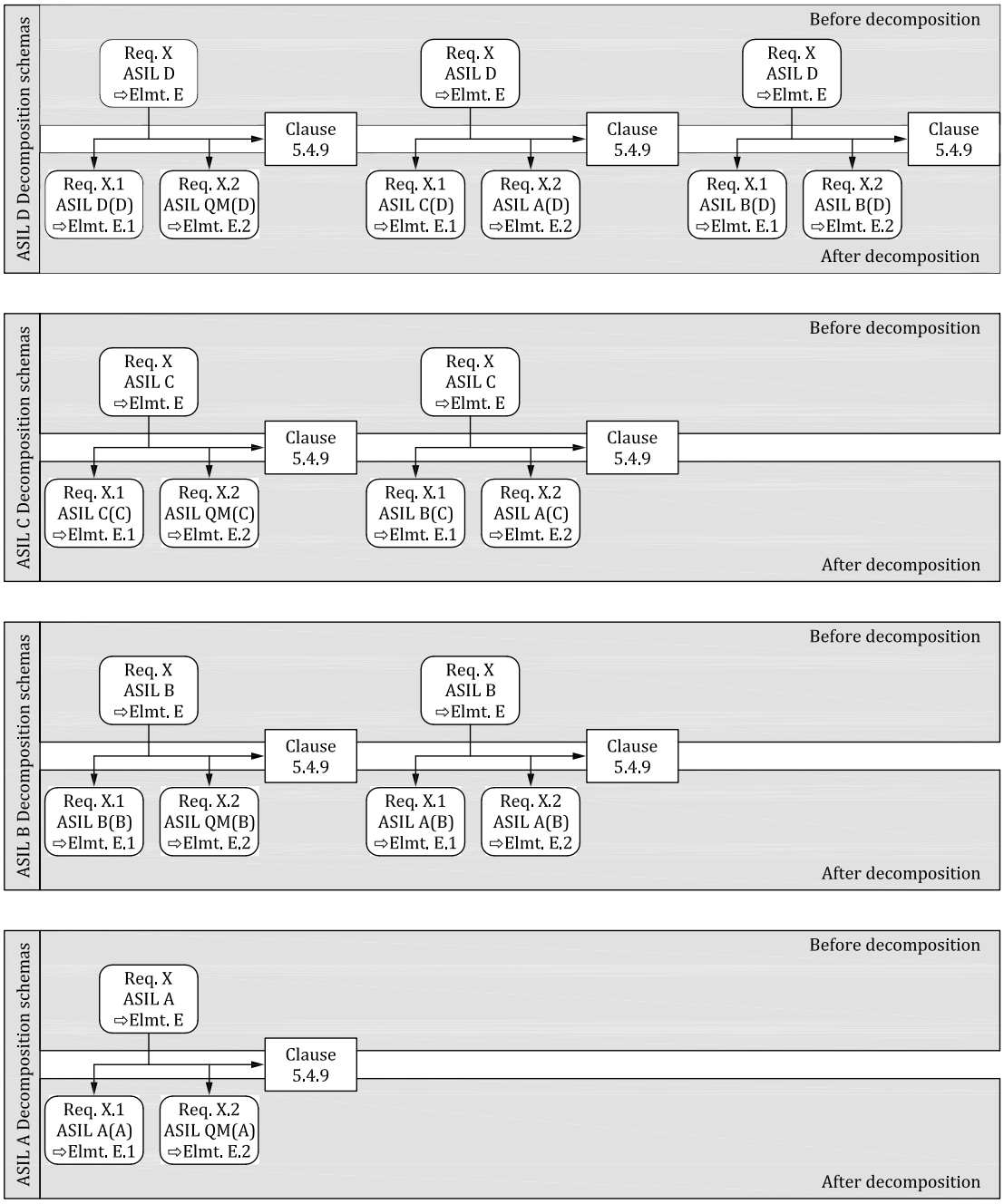

Figure 2 — ASIL decomposition schemas

Key

Req. X ASIL D → Elmt.E means that the requirement X with the ASIL D attribute is allocated to the element E

EXAMPLE The cases described in 5.4.7, where QM is assigned to the intended functionality and an ASIL equal to the initial ASIL is assigned to its associated safety mechanism, are shown in the leftmost column.

NOTE 2 The uppermost box of each decomposition step represents the ASIL before decomposition.

NOTE 3 Architectural elements E.1 and E.2 are sufficiently independent to comply with 5.4.3

5.4.10 When using any of the decomposition schemas given in 5.4.9, evidence for sufficient independence of the elements after decomposition shall be made available (see 5.4.3).

5.4.11 The development of the decomposed elements at the system level and at the software level shall be performed, as a minimum, in accordance with the ASIL requirements (after decomposition) of ISO 26262-4 and ISO 26262-6. The development of the decomposed elements at the hardware level shall be performed, as a minimum, in accordance with the ASIL requirements (after decomposition) of ISO 26262-5, except for the evaluation of the hardware architectural metrics and the evaluation of safety goal violations due to random hardware failures (see 5.4.5).

5.4.12 At each level of the design process at which decomposition is applied, the corresponding integration activities of the decomposed elements and subsequent activities, including verification and confirmation measures, shall be applied in accordance with the requirements of the ASIL before decomposition.

5.5 Work products

5.5.1 Update of architectural information, resulting from 5.4.

5.5.2 Update of ASIL as attribute of safety requirements and elements, resulting from 5.4.

6 Criteria for coexistence of elements

6.1 Objectives

This clause provides criteria for the coexistence within the same element of:

a) safety-related sub-elements with non-safety-related sub-elements; and

b) safety-related sub-elements that have different ASILs assigned.

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 the element, i.e. the highest ASIL of the safety requirements allocated to the element.

In the case of the coexistence of sub-elements that have different or no ASILs assigned, or the coexistence of non-safety-related sub-elements with safety-related ones, it can be beneficial to avoid assigning the ASIL of the element to all the sub-elements. For this purpose, this clause provides guidance for determining if sub-elements with different ASILs can coexist within the same element. This clause is based on the analysis of interference of each sub-element with the other sub-elements of an element.

In the context of this clause, interference is the presence of cascading failures from a sub-element with no ASIL assigned, or a lower ASIL assigned, to a sub-element with a higher ASIL assigned which leads to the violation of a safety requirement of the element (see ISO 26262-1:2018, 3.65).

When determining the ASIL of sub-elements of an element, the rationale for freedom from interference is supported by analyses of dependent failures (see Clause 7), focused on cascading failures.

6.3 Inputs to this clause

6.3.1 Prerequisites

The following information shall be available:

— the safety requirements at the level at which the analysis is to be performed: system, or hardware, or software in accordance with ISO 26262-3:2018, 7.5.1, or ISO 26262-4:2018, 6.5.1, or ISO 26262-5:2018, 6.5.1, or ISO 26262-6:2018, 6.5.1;

— the architectural information of the element at the level at which the analysis is to be performed: system, or hardware, or software, in accordance with ISO 26262-3:2018, 7.5.1, ISO 26262-4:2018, 6.5.3, or ISO 26262-5:2018, 7.5.1, or ISO 26262-6:2018, 7.5.1; and

— the allocation of the safety requirements to the element and sub-elements under consideration.

6.3.2 Further supporting information

None.

6.4 Requirements and recommendations

6.4.1 This clause may be applied at any refinement step during the design process, in parallel with the allocation of the safety requirements to the elements and sub-elements of an architecture.

NOTE Criteria of coexistence are typically considered during system design, hardware design, or software architectural design, in accordance with ISO 26262-4, or ISO 26262-5, or ISO 26262-6.

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

a) each safety requirement allocated to the element; and

b) each sub-element that is part of the element.

6.4.3 If a non-safety-related sub-element and safety-related sub-elements coexist in the same element, then the non-safety-related sub-element shall only be treated as a non-safety-related sub-element if evidence is made available that this non-safety-related sub-element cannot, directly or indirectly, violate any safety requirement allocated to the element. That is, this non-safety-related sub-element cannot interfere with any safety-related sub-element of the element.

NOTE 1 This means that there are no cascading failures from this sub-element to the safety-related sub-elements.

NOTE 2 This can be achieved by design measures, such as those concerning the data flow and control flow for software, or the input/output signals and control lines for hardware.

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

6.4.4 If safety-related sub-elements implementing requirements with different ASILs, including QM(X) (see 5.4.9), coexist in the same element, then a considered sub-element shall only be treated as a sub-element with a lower ASIL if evidence is available that, for each safety requirement allocated to the element, the considered sub-element cannot, directly or indirectly, violate any safety requirement allocated to the sub-elements implementing higher ASIL requirements. Otherwise, the considered sub-element shall be assigned the highest ASIL of the coexisting safety-related sub-elements for which evidence of freedom from interference is not available.

NOTE The evaluation of the freedom from interference is commensurate with the highest ASIL requirements allocated to the coexisting sub-elements (see 7.4.8).

6.5 Work products

6.5.1 Update of the ASIL attribute of the sub-elements of the element, resulting from 6.4.

7 Analysis of dependent failures

7.1 Objectives

The objectives of this clause are:

a) to confirm that a required independence or freedom from interference is sufficiently achieved in the design by analysing their potential causes or initiators; and

b) to define safety measures to mitigate plausible dependent failures, if necessary.

7.2 General

The scope of the analysis of dependent failures can be influenced by the technology of the given elements (e.g. software elements, hardware elements, or a mix of hardware and software elements), and by the safety requirements involved.

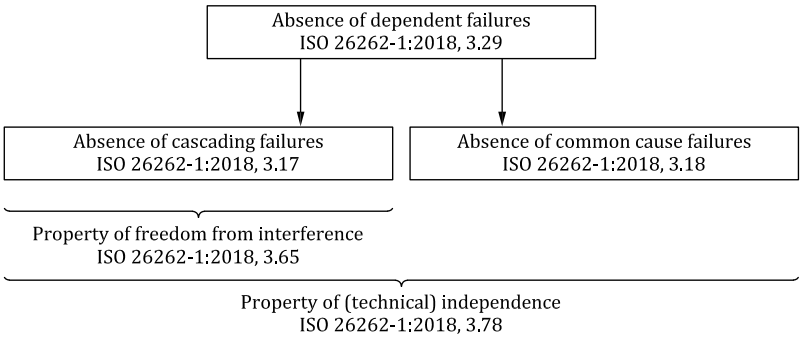

Figure 3 — Relationship between the different classes of dependent failures

Figure 3 describes the relationship between dependent failures, freedom from interference, and technical independence.

Freedom from interference is used to justify the coexistence of elements with different, or no, assigned ASIL (See Clause 6).

Freedom from interference and absence of common cause failures are used to justify independence when performing ASIL decomposition (See Clause 5).

NOTE 1 Other system properties can also require independence and, thus, absence of dependent failures. For instance, the analysis of dependent failures can be used to support the demonstration of effectiveness of the safety mechanisms to avoid single-point faults and latent faults (e.g. see ISO 26262-5:2018, Clause 8).

NOTE 2 The analysis of dependent failures can be applied at various design levels of the system or the item.

The analysis of dependent failures considers architectural features such as:

— similar and dissimilar redundant elements;

— different functions implemented with identical software or hardware elements;

— functions and their respective safety mechanisms;

— partitions of functions or software elements;

— physical distance between hardware elements, with or without a barrier; and

— common external resources.

Independence is threatened by common cause failures and cascading failures, while freedom from interference is only threatened by cascading failures.

EXAMPLE 1 A high intensity electromagnetic field that causes different electronic devices to fail in a way that depends on design and use, is a common cause failure.

EXAMPLE 2 Erroneous vehicle speed information transmitted to other vehicle functions and thus, affecting their behaviour, is a cascading failure.

EXAMPLE 3 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, which is a common cause failure.

An example framework for identifying dependent failures is given in Annex C.

7.3 Inputs to this clause

7.3.1 Prerequisites

The following information shall be available:

— the independence requirements at the level at which the analysis of dependent failures is applied: system, hardware, or software in accordance with ISO 26262-3:2018, 7.5.1, ISO 26262-4:2018, 6.5.1, ISO 26262-5:2018, 6.5.1, or ISO 26262-6:2018, 6.5.1;

— the freedom from interference requirements at the level at which the analysis of dependent failures is applied: system, hardware, or software in accordance with ISO 26262-3:2018, 7.5.1, ISO 26262-4:2018, 6.5.1, ISO 26262-5:2018, 6.5.1, or ISO 26262-6:2018, 6.5.1;

— the architectural information at the level at which the analysis of dependent failures is applied: system, hardware, or software in accordance with ISO 26262-3:2018, 7.5.1, ISO 26262-4:2018, 6.5.3, ISO 26262-5:2018, 7.5.1, or ISO 26262-6:2018, 7.5.1; and

NOTE 1 The architectural information is used to determine the boundary of the analysis of dependent failures.

— the safety plan in accordance with ISO 26262-2:2018, 6.5.3.

NOTE 2 The objectives and scope of a dependent failure analysis depend on the sub-phase and the level of abstraction at which the analysis is performed. This information is defined prior to conducting the analysis, for instance in the safety plan.

7.3.2 Further supporting information

None.

7.4 Requirements and recommendations

7.4.1 The potential for dependent failures shall be identified from the results of safety analyses in accordance with Clause 8.

NOTE 1 Both systematic failures and random hardware failures have the potential to be dependent failures.

NOTE 2 The identification of the potential for dependent failures can be based on deductive analyses, e.g. examination of cut sets or repeated identical events of an FTA.

NOTE 3 The identification of the potential for dependent failures can also be supported by inductive analyses, e.g. similar parts or components with similar failure modes that appear several times in an FMEA.

NOTE 4 Examples of analyses of dependent failures applied on semiconductors can be found in ISO 26262-11:2018, 4.7.

7.4.2 Each identified potential for dependent failures shall be evaluated to determine its plausibility, i.e. if a reasonably foreseeable cause exists which leads to the dependent failure and consequently violates a required independence, or freedom from interference, between given elements.

NOTE When quantification of random hardware failures is required, as for the evaluation of the safety goal violations due to random hardware failures (see ISO 26262-5), the contribution of common cause failures and cascading failures is estimated on a qualitative basis because no general and sufficiently reliable method exists for quantifying such failures.

7.4.3 This evaluation shall consider the operational situations as well as the different operating modes of the item or element being analysed.

7.4.4 This evaluation shall consider the following topics, as applicable:

NOTE 1 The evaluation of the plausibility of the potential dependent failures can be supported by appropriate checklists, e.g. checklists based on field experience. The checklists provide the analysts with representative examples of root causes and coupling factors such as same design, same process, same component, same interface, proximity. Annex C can be used as a basis to establish such checklists.

NOTE 2 This evaluation can also be supported by the adherence to process guidelines which are intended to prevent the introduction of root causes and coupling factors that could lead to dependent failures.

a) random hardware failures;

EXAMPLE 1 Failures of common blocks such as clock, test logic and internal voltage regulators in large scale integrated circuits (microcontrollers, ASICs, etc.).

b) development faults;

EXAMPLE 2 Requirement faults, design faults, implementation faults, faults resulting from the use of new technologies and faults introduced when making modifications.

c) manufacturing faults;

EXAMPLE 3 Faults related to processes, procedures and training; faults in control plans and in monitoring special characteristics; faults related to software flashing and end-of-line programming.

d) installation faults;

EXAMPLE 4 Faults related to wiring harness routing; faults related to the interchangeability of parts; failures of adjacent items or elements.

e) service faults;

EXAMPLE 5 Faults related to processes, procedures and training; faults related to trouble-shooting; faults related to the interchangeability of parts and faults due to backward incompatibility.

f) environmental factors;

EXAMPLE 6 Temperature, vibration, pressure, humidity/condensation, pollution, corrosion, contamination, EMC.

g) failures of common external resources or information;

EXAMPLE 7 Power supply, input data, inter-system data bus and communication.

h) stress due to specific situations; and

EXAMPLE 8 High operational loads, extreme user inputs or requests from other systems, thermal impact, and mechanical shocks.

i) ageing and wear.

7.4.5 Rationale for the plausibility of dependent failures and their impact shall be made available.

NOTE Plausible dependent failures are those for which the evaluation performed according to 7.4.2 has revealed a reasonably foreseeable cause.

7.4.6 Measures for the resolution of plausible dependent failures shall be specified during the development phase, in accordance with the change management in ISO 26262-8:2018, Clause 8.

7.4.7 Measures for the resolution of plausible dependent failures shall include the measures for preventing their root causes, or for controlling their effects, or for reducing the coupling factors.

EXAMPLE Diversity is a measure that can be used to prevent, reduce or detect common cause failures.

7.4.8 The analysis of dependent failures shall have a level of detail and rigor suitable to demonstrate the achievement of the required level of independence or freedom from interference.

NOTE Criteria that can be used to justify the suitability with respect to depth and rigor of a performed analysis of dependent failures include:

— the ASIL;

— the degree of independence between elements required in the safety concept;

— the product complexity;

— the technology; and

— the number and degree of adverse environmental and other stress factors

7.4.9 The analysis of dependent failures shall be verified in accordance with ISO 26262-8:2018, Clause 9.

7.5 Work products

7.5.1 **Dependent Failures Analysis**, resulting from 7.4.

7.5.2 **Dependent Failures Analysis Verification Report** resulting from 7.4.9.

8 Safety analyses

8.1 Objectives

The objective of safety analyses is to ensure that the risk of a safety goal violation due to systematic faults or random hardware faults is sufficiently low. Depending on the application, this is achieved by:

— identifying new hazards not previously identified during the hazard analysis and risk assessment;

— identifying faults, or failures, that can lead to the violation of a safety goal, or a safety requirement, respectively;

— identifying their potential causes;

— supporting the definition of safety measures for fault prevention, or fault control, respectively;

— providing evidence for the suitability of safety concepts; and

— supporting the verification of safety concepts, safety requirements, and the identification of design requirements and test requirements.

NOTE In the ISO 26262 series of standards, systematic faults are not analysed with a probability of occurrence. However, the measures against systematic faults contribute to the reduction of the overall risk of safety goal or safety requirement violation.

8.2 General

The scope of the safety analyses includes:

— the validation of safety goals and safety concepts;

— the verification of safety concepts and safety requirements;

— the identification of conditions and causes, including faults and failures, that could lead to the violation of a safety goal or safety requirement;

— the identification of additional safety requirements for detection of faults or failures;

— the determination of the required responses (actions/measures) to detected faults or failures; and

— the identification of additional measures for verifying that the safety goals or safety requirements are complied with, 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 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 a knowledge of the relevant fault types and fault models.

Qualitative analysis methods include:

— qualitative FMEA at system, design or process level;

— qualitative FTA;

— HAZOP; and

— qualitative ETA.

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

Quantitative safety analyses complement qualitative safety analyses. They are used to verify a hardware design against defined targets for the evaluation of the hardware architectural metrics and the evaluation of safety goal violations due to random hardware failures (see ISO 26262-5:2018, Clause 8 and Clause 9). Quantitative safety analyses require additional knowledge of the quantitative failure rates of the hardware elements.

Quantitative analysis methods include:

— quantitative FMEA;

— quantitative FTA;

— quantitative ETA;

— Markov models; and

— reliability block diagrams.

NOTE 2 The quantitative analysis methods only address random hardware failures. These analysis methods are not applied to systematic failures in the ISO 26262 series of standards.

Another way to classify the safety analyses is by the way they are conducted:

— inductive analysis methods are bottom-up methods that start from known causes and identify possible effects;

— deductive analysis methods are top-down methods that start from known effects and seek possible causes.

Inductive analyses and deductive analyses complement each other and therefore increase the coverage of their result.

NOTE FMEA and ETA are typically performed inductively, whereas FTA and reliability block diagram analyses are typically performed deductively.

A further classification of safety analyses is whether the chosen method is capable of identifying single-point or multiple-point faults in order to address latent faults according to ISO 26262-4:2018, 6.4.2, and ISO 26262-5:2018, 7.4.3.

8.3 Inputs to this clause

8.3.1 Prerequisites

The following information shall be available:

— the safety requirements at the level at which the safety analysis is to be performed: system, hardware, or software in accordance with ISO 26262-3:2018, 7.5.1, ISO 26262-4:2018, 6.5.1, ISO 26262-5:2018, 6.5.1, or ISO 26262-6:2018, 6.5.1; and

— the architectural information of the element at the level at which the safety analysis is to be performed: system, hardware, or software in accordance with ISO 26262-4:2018, 7.5.2, ISO 26262-5:2018, 7.5.1, or ISO 26262-6:2018, 7.5.1.

NOTE The architectural information is used to determine the boundaries of the safety analyses.

8.3.2 Further supporting information

The following information can be considered:

— fault models (from external sources).

8.4 Requirements and recommendations

8.4.1 The safety analyses shall be performed in accordance with appropriate standards or guidelines and the defined objectives, for instance in the safety plan.

NOTE 1 The level of detail of the analysis is appropriate to the level of detail of the design. The fault models depend on the description level of the design on which the analysis is based (System, Hardware, Software), and on the safety requirements being implemented. For semiconductor failure modes, ISO 26262-11:2018, 4.3.2 can be considered.

NOTE 2 Such standards and guidelines can include criteria for defining the depth and rigor of a safety analysis. These criteria can depend on the ASIL, complexity or experiences with a specific item, and its field of application.

NOTE 3 The objectives and scope of the safety analyses depend on the sub-phase and the level of granularity at which it is applied.

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 the 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, in accordance with ISO 26262-4, or ISO 26262-5, or ISO 26262-6 respectively.

8.4.5 Hazards newly identified by safety analyses during product development which are not already covered shall be included in an updated hazard analysis and risk assessment according to ISO 26262-3:2018, Clause 6. The corresponding changes shall be managed in accordance with ISO 26262-8:2018, Clause 8.

8.4.6 The fault models used for the safety analyses shall be suitable for the level of detail being analysed in a given development sub-phase and shall be used consistently within that sub-phase.

NOTE 1 Sub-phases include hardware design, evaluation of the hardware architectural metrics and evaluation of safety goal violations due to random hardware failures in ISO 26262-5, or software architectural design in accordance with ISO 26262-6.

NOTE 2 For the safety analyses at software architectural level, see ISO 26262-6:2018, Annex E.

8.4.7 Additional safety-related test cases shall be determined by using the fault models and the results of the safety analyses, if necessary.

8.4.8 The safety analyses and their outcomes shall be verified in accordance with ISO 26262-8:2018, Clause 9.

8.4.9 The qualitative safety analyses shall include:

a) a systematic identification of faults or failures that could lead to the 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 elements; and

   — the usage of the item or element.

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

c) the identification of the causes of each identified fault; and

d) the identification, or the support for the identification, of potential safety concept weaknesses, including the ineffectiveness of safety mechanisms in handling anomalies such as latent faults, multiple-point faults, common cause failures and cascading failures.

NOTE The interactions with other items or elements, internal and external to the item, are examined to assess the degree of independence and interference.

8.4.10 If quantitative safety analyses are used to complement the qualitative safety analyses, then they shall include:

a) the quantitative data to support the evaluation of the hardware architectural metrics and the evaluation of safety goal violations due to random hardware failures (see ISO 26262-5:2018, Clause 8 and Clause 9);

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

c) the evaluation and ranking of the potential safety concept weaknesses, including the ineffectiveness of safety mechanisms; and

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

8.5 Work products

8.5.1 Safety analyses, resulting from 8.4.

8.5.2 Safety analyses verification report, resulting from 8.4.8.

Annex A
(informative)

Overview of and document flow of Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses

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

Table A.1 — Overview of and document flow of ASIL-oriented and safety-oriented analyses

Clause	Objectives	Prerequisites	Work products
5 Requirements decomposition with respect to ASIL tailoring	If ASIL decomposition is applied, the objectives of this Clause are: a) to ensure that a safety requirement is decomposed into redundant safety requirements at the next level of detail, and that these are allocated to sufficiently independent design elements; and b) to apply ASIL decomposition according to permitted ASIL decomposition schemas.	— The safety requirements at the level at which the ASIL decomposition is to be applied: vehicle, system, hardware, or software in accordance with ISO 26262-3:2018, 7.5.1, or ISO 26262-4:2018, 6.5.1, or ISO 26262-5:2018, 6.5.1 or ISO 26262-6:2018, 6.5.1; and — The architectural information at the level at which the ASIL decomposition is to be applied: vehicle, system, hardware, or software in accordance with ISO 26262-3:2018, 7.5.1, or ISO 26262-4:2018, 6.5.3, or ISO 26262-5:2018, 7.5.1, or ISO 26262-6:2018, 7.5.1.	5.5.1 Update of architectural information, resulting from 5.4. 5.5.2 Update of ASIL as attribute of safety requirements and elements, resulting from 5.4.

Table A.1 *(continued)*

Clause	Objectives	Prerequisites	Work products
6 Criteria for coexistence of elements	This Clause provides criteria for the coexistence within the same element of: a) safety-related sub-elements with non-safety-related sub-elements; and b) safety-related sub-elements that have different ASILs assigned.	— the safety requirements at the level at which the analysis is to be performed: system, or hardware, or software in accordance with ISO 26262-3:2018, 7.5.1, or ISO 26262-4:2018, 6.5.1, or ISO 26262-5:2018, 6.5.1, or ISO 26262-6:2018, 6.5.1; — the architectural information of the element at the level at which the analysis is to be performed: system, or hardware, or software, in accordance with ISO 26262-3:2018, 7.5.1, ISO 26262-4:2018, 6.5.3, or ISO 26262-5:2018, 7.5.1, or ISO 26262-6:2018, 7.5.1; and — the allocation of the safety requirements to the element and sub-elements under consideration.	6.5.1 Update of the ASIL attribute of the sub-elements of the element, resulting from 6.4.

Table A.1 *(continued)*

Clause	Objectives	Prerequisites	Work products
7 Analysis of dependent failures	The objectives of this Clause are: a) to confirm that a required independence or freedom from interference is sufficiently achieved in the design by analysing their potential causes or initiators; and b) to define safety measures to mitigate plausible dependent failures, if necessary.	— The independence requirements at the level at which the analysis of dependent failures is applied: system, hardware, or software in accordance with ISO 26262-3:2018, 7.5.1, ISO 26262-4:2018, 6.5.1, ISO 26262-5:2018, 6.5.1, or ISO 26262-6:2018, 6.5.1; — The freedom from interference requirements at the level at which the analysis of dependent failures is applied: system, hardware, or software in accordance with ISO 26262-3:2018, 7.5.1, ISO 26262-4:2018, 6.5.1, ISO 26262-5:2018, 6.5.1, or ISO 26262-6:2018, 6.5.1; — The architectural information at the level at which the analysis of dependent failures is applied: system, hardware, or software in accordance with ISO 26262-3:2018, 7.5.1, ISO 26262-4:2018, 6.5.3, ISO 26262-5:2018, 7.5.1, or ISO 26262-6:2018, 7.5.1; and — The safety plan in accordance with ISO 26262-2:2018, 6.5.3.	7.5.1 Dependent Failures Analysis, resulting from 7.4. 7.5.2 Dependent Failures Analysis Verification Report resulting from 7.4.9.

Table A.1 *(continued)*

Clause	Objectives	Prerequisites	Work products
8 Safety analyses	The objective of safety analyses is to ensure that the risk of a safety goal violation due to systematic faults or random hardware faults is sufficiently low. Depending on the application, this is achieved by: — identifying new hazards not previously identified during the hazard analysis and risk assessment; — identifying faults, or failures, that can lead to the violation of a safety goal, or a safety requirement, respectively; — identifying their potential causes; — supporting the definition of safety measures for fault prevention, or fault control, respectively; — providing evidence for the suitability of safety concepts; and — supporting the verification of safety concepts, safety requirements, and the identification of design requirements and test requirements.	— The safety requirements at the level at which the safety analysis is to be performed: system, hardware, or software in accordance with ISO 26262-3:2018, 7.5.1, ISO 26262-4:2018, 6.5.1, ISO 26262-5:2018, 6.5.1, or ISO 26262-6:2018, 6.5.1; and — The architectural information of the element at the level at which the safety analysis is to be performed: system, hardware, or software in accordance with ISO 26262-4:2018, 7.5.2, ISO 26262-5:2018, 7.5.1, or ISO 26262-6:2018, 7.5.1.	8.5.1 Safety analyses, resulting from 8.4 8.5.2 Safety analyses verification report, resulting from 8.4.8

Annex B
(informative)

Example architectures for Coexistence of elements and Decomposition of requirements

B.1 Example architecture

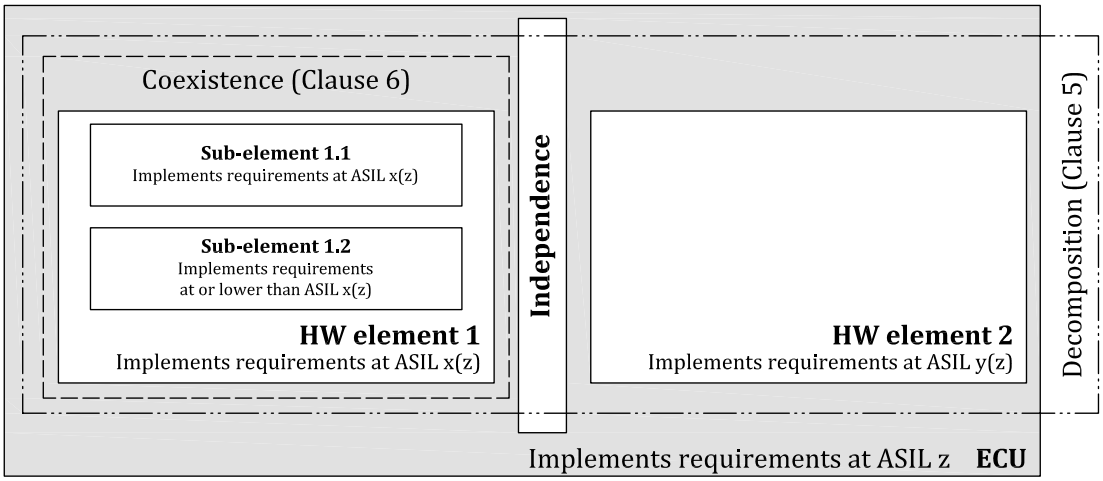

Figure B.1 — Coexistence and decomposition in an example architecture

NOTE Coexistence and decomposition are part of the system architectural design constraints addressed in ISO 26262-4:2018, Clause 6; hardware design in ISO 26262-5:2018, Clause 7; and software in ISO 26262-6:2018, Clause 7.

B.2 Coexistence (Clause 6):

— If an ASIL x requirement is allocated to Element 1, then Sub-element 1.1 and Sub-element 1.2 inherit ASIL x.

— Sub-element 1.2 is only developed at a lower ASIL if the following conditions are met:

  — At least one sub-element of Element 1 is able to fulfil Element 1 requirement at ASIL x (e.g. Sub-element 1.1);

  — Sub-element 1.2 cannot violate Element 1 safety requirement; and

  — Criteria for coexistence are met (see Clause 6): no cascading failures from Sub-element 1.2 to Sub-element 1.1 (Freedom From Interference).

B.3 Decomposition (Clause 5)

If an ASIL z requirement is allocated to the ECU in Figure B.1, it can be decomposed between independent AND redundant hardware elements.

This is equivalent to meeting all of the following conditions:

— A decomposition schema described in Clause 5 is used, i.e. ASIL z → ASIL x(z) + ASIL y(z);

— HW_Element_1 fulfils by itself the ECU safety requirement at ASIL x(z);

— HW_Element_2 fulfils by itself the ECU safety requirement at ASIL y(z); and

— HW_Element_1 and HW_Element_2 are independent, i.e. no cascading failures from HW_Element_1 to HW_Element_2 and no cascading failures from HW_Element_2 to HW_Element_1, no common cause failure, demonstrated at ASIL z.

Annex C
(informative)

Framework for Identifying Dependent Failures

Independence between two or more elements is determined by showing absence of dependent failures, i.e. absence of cascading failures and common cause failures. Independence can be required between elements according to the safety concept, e.g. to support ASIL decomposition.

In order to identify cascading and common cause failures, the following classes of coupling factors can be used to improve the completeness of the analysis.

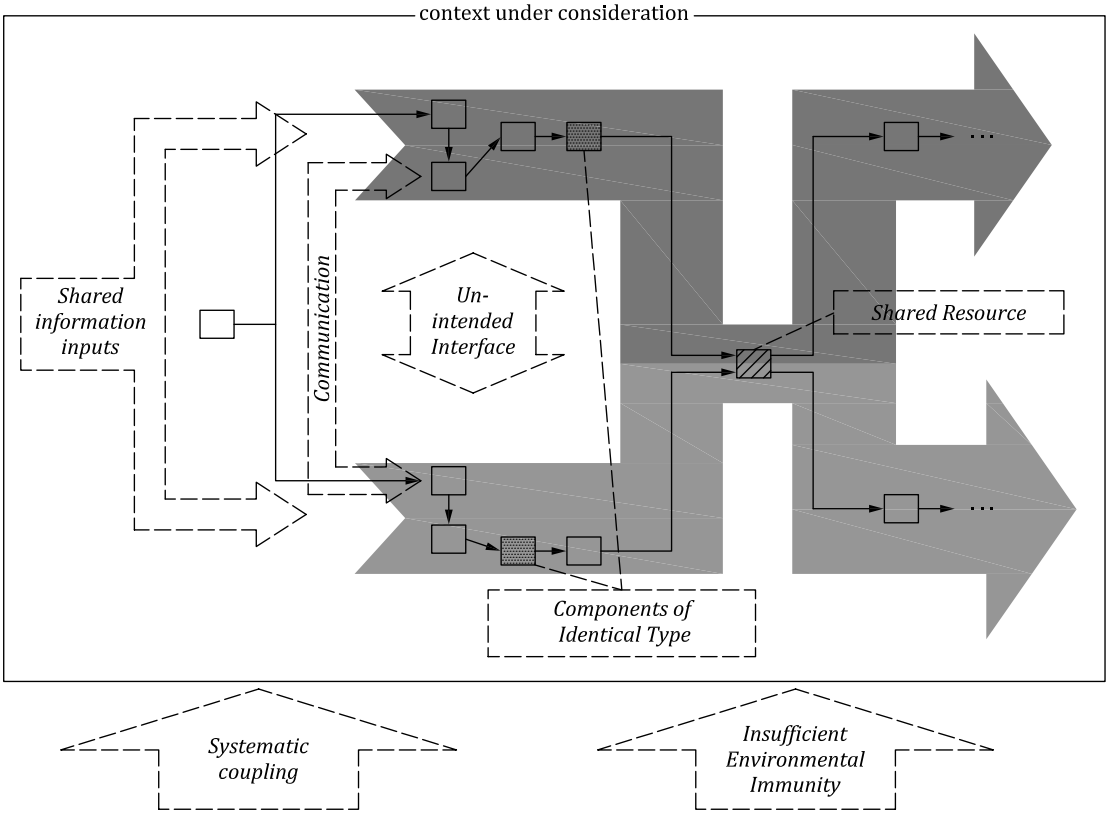

Figure C.1 — Coupling factor classes between elements

NOTE The grey arrows indicate the functional chain of events linking the elements thereby realizing the functionality affected by coupling factors. The dotted arrows indicate the classes of coupling factors potentially affecting the system and its elements.

These classes of coupling factors can be applied as checklists to any level of abstraction, including the system, software, hardware, and semiconductor levels, as illustrated in Table C.1. This table presents examples of coupling factors, which are mapped to the topics in 7.4.4. Some examples can belong to several coupling factor classes, e.g. software calibration parameters might be considered as Shared Resource or Shared Information Input.

Table C.1 — Examples at the system, software, hardware, and semiconductor levels

Coupling factor class	Mapping to the topics in ISO 26262-9:2018, 7.4.4	Examples at the system level	Examples at the hardware level	Examples at the software level	Examples at the semiconductor level
Shared Resource The same software, hardware, or system element instance is used by two elements, which are therefore affected by the failure or unavailability of that shared resource.	a) random hardware failures g) failures of common external resources or information	— Power supply (see also Insufficient Environmental Immunity) — Wiring harness — Data and communication busses — Powerstage	— Clock — Same H-Bridge used by two shut-down paths — Sockets, plug connectors	— SW component used by 2 other SW components, e.g. — maths or other libraries — I/O routines, drivers — Hardware resource used by more than one software element	"Failure of shared resources" and "single physical root cause" in ISO 26262-11
Shared Information Input Connection to the same information source by means of which the two functions consume the same information, even in absence of shared resources, i.e. from a functional perspective.	a) random hardware failures	— External messages (e.g. CAN, Flexray, or AUTOSAR RTE messages) — External physical signals (e.g. magnetic fields, remote/radio signals) — Readings detected by capacitive/radar/optical sensors	— Connection to sources of raw physical digital or analogous signals	— Constants, or variables, being global to the two software functions — Data/function parameter arguments/messages delivered by software function to more than one other function	"Failure of Shared resources" in ISO 26262-11
Insufficient Environmental Immunity Same or similar physical characteristics of elements, which can be affected by the same external environmental disturbance	f) environmental factors h) stress due to specific situation	— Mechanical coupling — Flammable material	— Grade of sensitivity to electrical effects (creating the potential of suffering from e.g. EMI, ESD) — Proximity of HW elements (creating the potential of suffering from e.g. dust, particles) — Same housing (creating the potential of suffering from e.g. water entry, humidity)	Not directly applicable to SW alone. Environmental influences that affect behaviour of software can be considered at the system and hardware levels	"Environmental faults" in ISO 26262-11

Table C.1 *(continued)*

Coupling factor class	Mapping to the topics in ISO 26262-9:2018, 7.4.4	Examples at the system level	Examples at the hardware level	Examples at the software level	Examples at the semiconductor level
Systematic Coupling Failure of elements due to a common systematic human error or tool error.	b) development faults c) manufacturing faults d) installation faults e) service faults h) stress due to specific situation	— Identical production processes used for multiple elements — Identical repair processes used for multiple elements.		— Same software tools e.g. IDE, compiler, linker, software configurator — Same programming and/or modelling language — Same compiler/linker	"Development faults", "Manufacturing faults", "Installation faults", and "Repair faults" in ISO 26262-11
Components of Identical Type Multiple instances of identical or very similar components can jointly fail due to a common cause failure.	a) random hardware failures b) development faults	— Same type of actuator/power stage e.g. motor — Same type of sensors	— Same type of HW parts and components — Same power supply ICs for different microcontrollers — Same microcontroller — Same ASICs	— The same source code expanded twice, e.g. by usage of C macros NOTE: the same library instance or the same standard SW module instance called from different locations is rather considered as a Shared Resource.	"Development faults" in ISO 26262-11
Communication An element receives information from another element by means of a communication channel	a) random hardware failures b) development faults d) installation faults e) repair faults i) ageing and wear	— CAN connection between two ECUs of the same system — Communication between two microcontrollers within the same ECU	— Electrical connection between two HW elements	— Data flow via global variables — Messaging — Function calls with arguments passed	"Failure of shared resources" and "single physical root cause" with semiconductors in ISO 26262-11

Table C.1 *(continued)*

Coupling factor class	Mapping to the topics in ISO 26262-9:2018, 7.4.4	Examples at the system level	Examples at the hardware level	Examples at the software level	Examples at the semiconductor level
Unintended Interface Two elements affecting each other directly via an unanticipated interface	a) random hardware failures b) development faults d) installation faults h) stress due to specific situation	— One functionality overruling the other because of missing synchronization	— Proximity of HW elements, creating the potential of crosstalk between signal lines, heat impact, interference etc.	— Same memory space which means a potential of wrong memory allocation or memory leaks	"Single physical root cause" originating from a semiconductor (see ISO 26262-11)

Bibliography

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

[2] Lovric T. (ZF TRW), Metz P. (Brose), Schnellbach A. (Magna), Dependent Failure Analysis in Practice, VDA Sys Conference, July 6th–8th 2016, Berlin

[3] Schnellbach, *Magna Powertrain, Dependent Failure Analysis, The MPT approach*, Safetronic. 2014 — Functional Safety in Automotive conference, 11th–12th Nov, 2014, Stuttgart

[4] ISO 26262-11:2018, *Road vehicles - Functional safety - Part 11: Guidelines on application of ISO 26262 to semiconductors*

[5] ISO 26262-12:2018, *Road vehicles - Functional safety - Part 12: Adaptation for motorcycles*

ICS 43.040.10

Price based on 29 pages