INTERNATIONAL STANDARD

ISO 26262-9

First edition
2011-11-15

Road vehicles — Functional safety —

Part 9: 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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 26262-9:2011
https://standards.iteh.ai/catalog/standards/sist/4fc5b142-8936-43a6-a8be-372b0faa517a/iso-26262-9-2011

Reference number
ISO 26262-9:2011(E)

© ISO 2011

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 26262-9:2011
https://standards.iteh.ai/catalog/standards/sist/4fc5b142-8936-43a6-a8be-372b0faa517a/iso-26262-9-2011

COPYRIGHT PROTECTED DOCUMENT

© ISO 2011

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

Published in Switzerland

© ISO 2011 – All rights reserved

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 26262-9:2011
https://standards.iteh.ai/catalog/standards/sist/4fc5b142-8936-43a6-a8be-372b0faa517a/iso-26262-9-2011

© ISO 2011 – All rights reserved

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*.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

ISO 26262-9:2011
https://standards.iteh.ai/catalog/standards/sist/4fc5b142-8936-43a6-a8be-372b0faa517a/iso-26262-9-2011

— *Part 1: Vocabulary*

— *Part 2: Management of functional safety*

— *Part 3: Concept phase*

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

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

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

— *Part 7: Production and operation*

— *Part 8: Supporting processes*

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

— *Part 10: Guideline on ISO 26262*

© ISO 2011 – All rights reserved

Introduction

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

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

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

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

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

ISO 26262-9:2011
https://standards.iteh.ai/catalog/standards/sist/4fc5b142-8936-43a6-a8be-372b08a517a/iso-26262-9-2011

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

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

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

e) provides requirements for relations with suppliers.

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

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

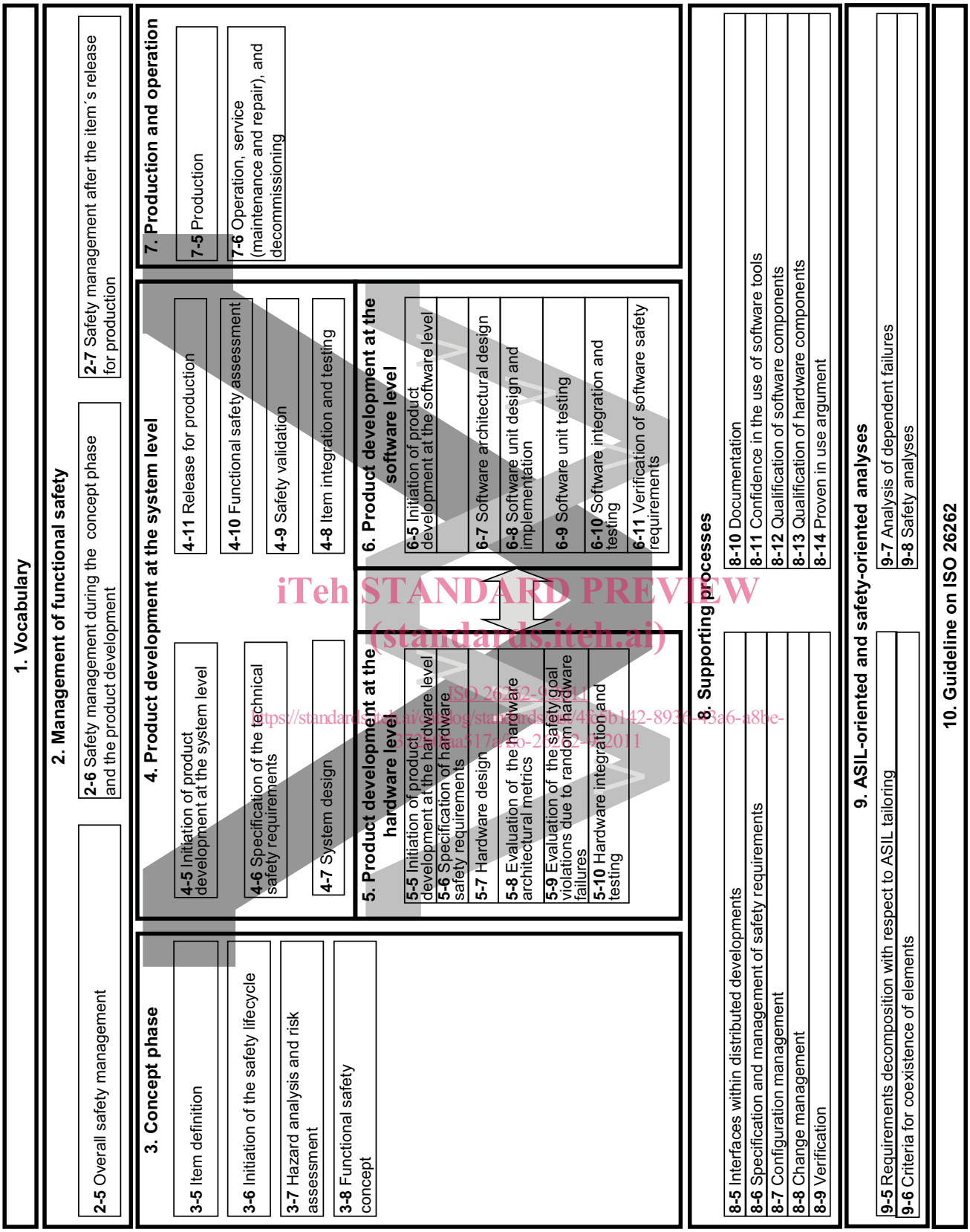
Figure 1 shows the overall structure of this edition of ISO 26262. ISO 26262 is based upon a V-model as a reference process model for the different phases of product development. Within the figure:

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

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

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

© ISO 2011 – All rights reserved



iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 26262-9:2011
https://standards.iteh.ai/catalog/standards/sist/4f6cb142-8936-43a6-a8be-3...aa517a...-26262-9-2011

Figure 1 — Overview of ISO 26262

© ISO 2011 – All rights reserved

Road vehicles — Functional safety —

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

1 Scope

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

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

ISO 26262-9:2011
https://standards.iteh.ai/catalog/standards/sist/4fc5b142-8936-43a6-a8be-372b0faa517a/iso-26262-9-2011

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

This part of ISO 26262 specifies the requirements for 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.

2 Normative references

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

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

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

© ISO 2011 – All rights reserved

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

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

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

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

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

3 Terms, definitions and abbreviated terms

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

4 Requirements for compliance

4.1 General requirements

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

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

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 26262-9:2011
https://standards.iteh.ai/catalog/standards/sist/4fc5b142-8936-43a6-a8be-5f2b01aa5f7b/iso-26262-9-2011

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

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

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

4.2 Interpretations of tables

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

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

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

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

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

© ISO 2011 – All rights reserved

rationale shall be given that the selected combination of methods complies with the corresponding requirement.

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

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

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

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

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

4.3 ASIL-dependent requirements and recommendations

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

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

5 Requirements decomposition with respect to ASIL tailoring

ISO 26262-9:2011
https://standards.iteh.ai/catalog/standards/sist/4fc5b142-8936-43a6-a8be-372b0faa517a/iso-26262-9-2011

5.1 Objectives

This clause provides 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 propagated throughout the item's development process. 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 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 is called "ASIL decomposition". During the 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 these decomposed safety requirements.

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

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 element.

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

© ISO 2011 – All rights reserved

NOTE 3 In the case of use of homogenous redundancy (e.g. by duplicated device or duplicated software) and with respect to systematic failures of hardware and software, the ASIL cannot be reduced unless an analysis of dependent failures provides evidence that sufficient independence exists 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.

NOTE 4 In general, ASIL decomposition does not apply to elements ensuring the channel selection or switching in multi-channel architectural designs.

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) remain unchanged by ASIL decomposition.

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: system, or hardware, or software in accordance with ISO 26262-3:2011, 8.5.1, or ISO 26262-4:2011, 6.5.1, or ISO 26262-5:2011, 6.5.1 or ISO 26262-6:2011, 6.5.1; and

— the architectural information at the level at which the ASIL decomposition is to be applied: system, or hardware, or software in accordance with ISO 26262-4:2011, 7.5.2, or ISO 26262-5:2011, 7.5.1, or ISO 26262-6:2011, 7.5.1.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 26262-9:2011
https://standards.iteh.ai/catalog/standards/sist/4fc5b142-8936-43a6-a8be-372b0faa517a/iso-26262-9-2011

5.3.2 Further supporting information

The following information can be considered:

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

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

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 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 implemented by sufficiently independent elements.

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

NOTE This requirement provides redundancy by definition.

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 shall remain unchanged by ASIL decomposition in accordance with ISO 26262-5.

 © ISO 2011 – All rights reserved

5.4.6 If ASIL decomposition is applied at the software level, sufficient independence between the elements implementing the decomposed requirements shall be checked at the system level and appropriate measures shall be taken at the software level, or 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 highest decomposed ASIL;

NOTE 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 If the decomposition scheme ASIL x(x) + QM(x) is chosen, then QM(x) means that the quality management system can be sufficient to develop element(s) that implement the safety requirement allocated to the intended functionality. QM(x) also means that the quality management system can support the rationale for the independence between the intended functionality and the safety mechanism.

5.4.8 If the violation of an initial safety requirement cannot be prevented by switching off the element, then adequate availability of the sufficiently independent elements implementing the decomposed safety requirements shall be shown.

5.4.9 When applying ASIL decomposition to a safety requirement, then:

a) ASIL decomposition shall be applied in accordance with 5.4.10;

b) ASIL decomposition may be applied more than once;

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 26262-9:2011

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)”.

5.4.10 One of the following decomposition schemes outlined below shall be chosen in accordance with the ASIL before decomposition (as shown in Figure 2), or a scheme resulting in higher ASILs may be used.

NOTE The step from one level of the selected decomposition scheme 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

© ISO 2011 – All rights reserved