BS ISO 26262-9:2011

BSI Standards Publication

Road vehicles — Functional safety

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

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of ISO 26262-9:2011.

The UK participation in its preparation was entrusted to Technical Committee AUE/16, Electrical and electronic equipment.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 62311 0

ICS 43.040.10

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2011.

Amendments issued since publication

Date	Text affected

BS ISO 26262-9:2011

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

Reference number
ISO 26262-9:2011(E)

COPYRIGHT PROTECTED DOCUMENT

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

Published in Switzerland

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms, definitions and 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 3

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 7

6 Criteria for coexistence of elements 7
6.1 Objectives 7
6.2 General 7
6.3 Inputs to this clause 8
6.4 Requirements and recommendations 8
6.5 Work products 9

7 Analysis of dependent failures 9
7.1 Objectives 9
7.2 General 9
7.3 Inputs to this clause 9
7.4 Requirements and recommendations 10
7.5 Work products 11

8 Safety analyses 11
8.1 Objectives 11
8.2 General 11
8.3 Inputs to this clause 13
8.4 Requirements and recommendations 13
8.5 Work products 14

Annex A (informative) **Overview of and document flow of Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses** 15

Bibliography 16

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 at the system level*

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

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

— *Part 7: Production and operation*

— *Part 8: Supporting processes*

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

— *Part 10: Guideline on ISO 26262*

Introduction

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

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

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

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

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

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

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

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

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

e) provides requirements for relations with suppliers.

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

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

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

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

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

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

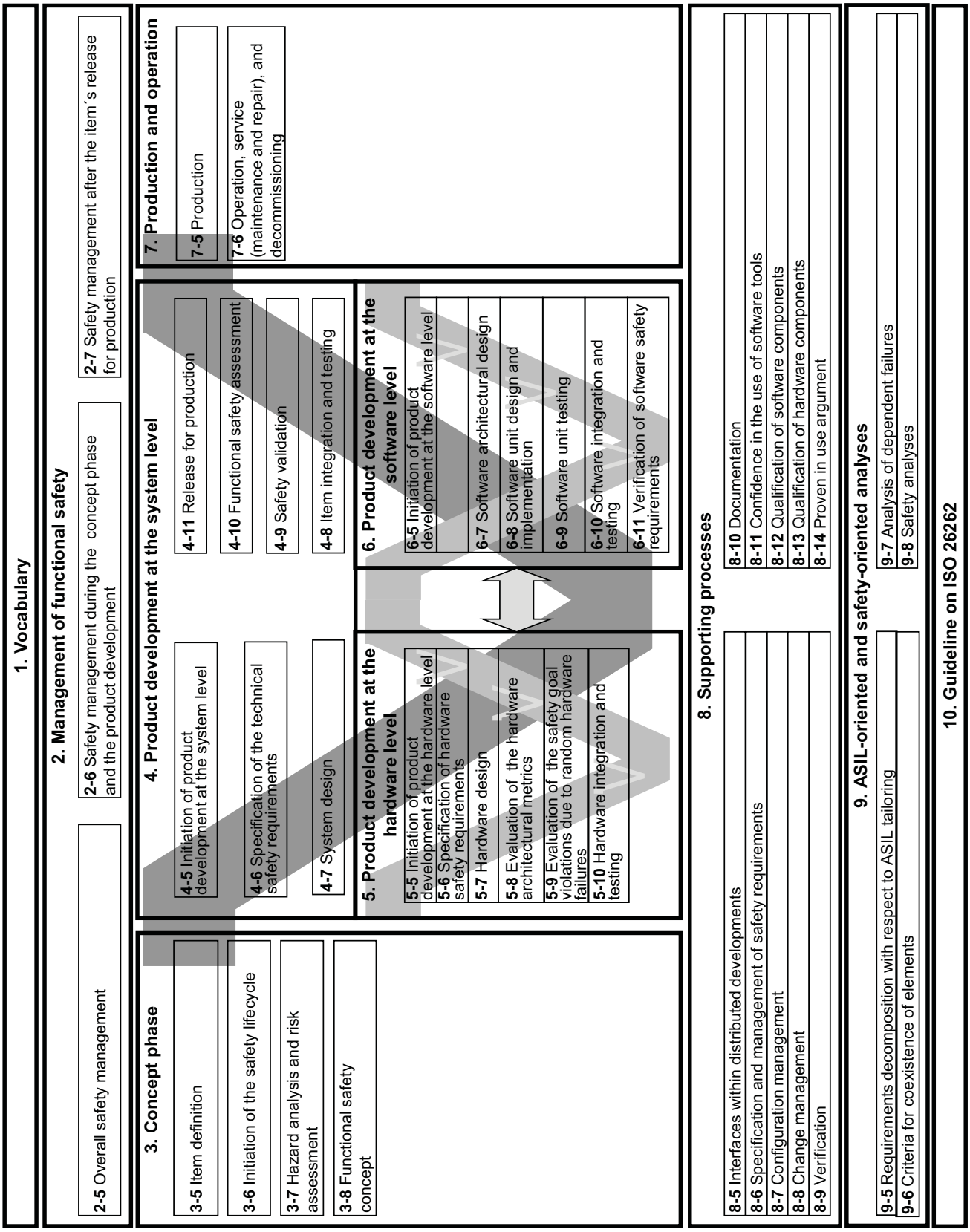


Figure 1 — Overview of ISO 26262

INTERNATIONAL STANDARD **ISO 26262-9:2011(E)**

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.

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

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

This part of ISO 26262 specifies the requirements for 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 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.

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

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

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

4.2 Interpretations of tables

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

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

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

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

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

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

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

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

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

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

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

4.3 ASIL-dependent requirements and recommendations

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

5 Requirements decomposition with respect to ASIL tailoring

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.

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.

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.

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.

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

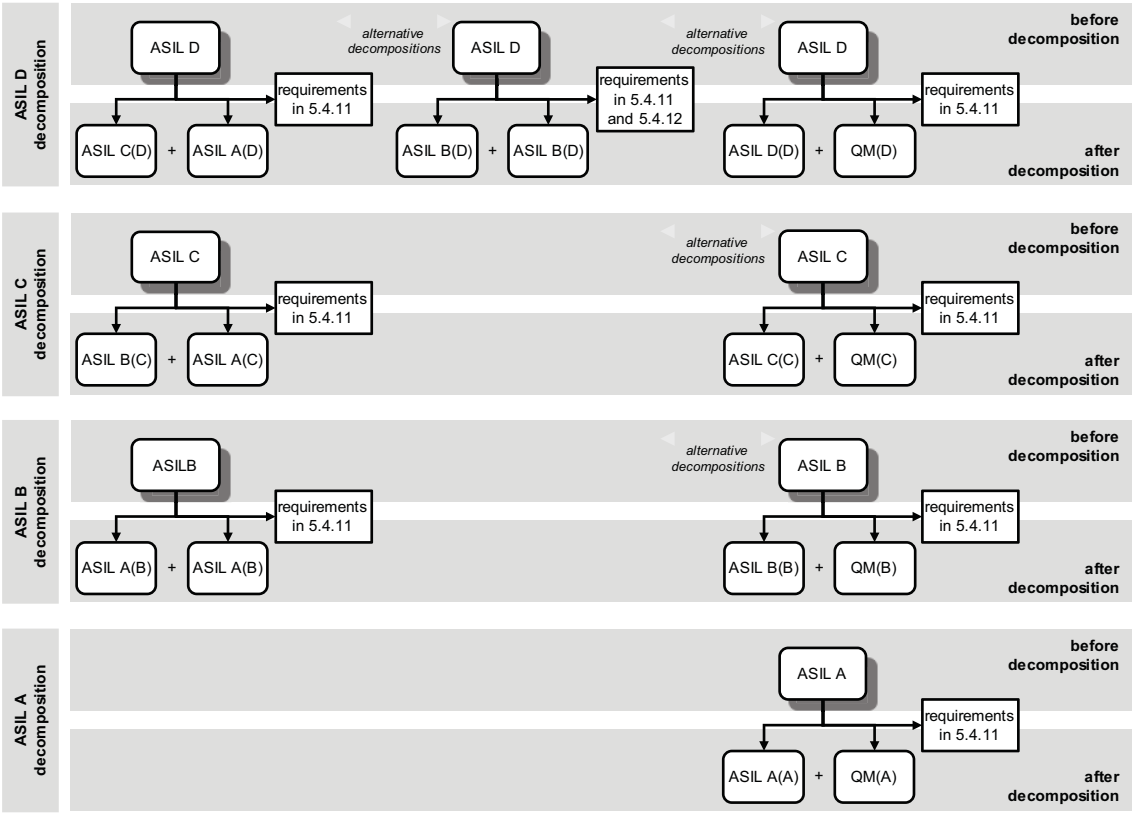
   2) one ASIL C(C) requirement and one QM(C) requirement.

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

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

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



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 rightmost column.

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

Figure 2 — ASIL decomposition schemes

5.4.11 When using any of the decomposition schemes given in 5.4.10, then:

a) confirmation measures in accordance with ISO 26262-2:2011, 6.4.7, shall be applied in compliance with the ASIL of the safety goal;

b) evidence for sufficient independence of the elements after decomposition shall be made available.

NOTE The elements are sufficiently independent if the analysis of dependent failures (see Clause 7 of this part of ISO 26262) 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 according to the ASIL of the safety goal.

5.4.12 When using the decomposition scheme for ASIL D given in 5.4.10 a) 2), then:

a) decomposed safety requirements shall be specified in accordance with ASIL C requirements of ISO 26262-8:2011, Clause 6;

NOTE The more formalized notation required for ASIL C compared to ASIL B increases the avoidance of systematic failures and decreases dependencies between the two ASIL B(D) implementations.

b) if the same software tools are used for the development of the decomposed elements, then these software tools shall be considered as software tools for developing ASIL D items or elements, in accordance with the confidence in the use of software tools in ISO 26262-8.

5.4.13 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. 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).

5.4.14 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 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:

— safety-related sub-elements with sub-elements that have no ASIL assigned; and

— 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 (see ISO 26262-4:2011, 7.4.2.3).

In the case of the coexistence of sub-elements that have different ASILs assigned or the coexistence of sub-elements that have no ASIL assigned with safety-related ones, it can be beneficial to avoid raising the ASIL for some of them to the ASIL of the element. For this purpose, this clause provides guidance for determining the ASIL of sub-elements of an element. This clause is based on the analysis of interference of a sub-element with the other sub-elements of an element.

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 leading to the violation of a safety requirement of the element (see ISO 26262-1:2011, definitions 1.13 and 1.49).

When determining the ASIL of sub-elements of an element, the rationale for freedom from interference is supported by analyses of dependent failures focused on cascading failures (see Clause 7 of this part of ISO 26262).

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 26262-3:2011, 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 of the element at the level at which the analysis is to be performed: 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.

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, typically during the subphases of system design, or hardware design, or software architectural design, in accordance with ISO 26262-4, or ISO 26262-5, or ISO 26262-6.

6.4.2 The safety requirements shall be allocated to the sub-elements of the element before applying this clause.

NOTE The allocation of safety requirements to the sub-elements results in safety-related sub-elements and sub-elements that have no ASIL assigned.

6.4.3 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.

6.4.4 If a sub-element with no ASIL assigned and safety-related sub-elements coexist in the same element, then the sub-element with no ASIL assigned shall only be treated as a QM sub-element if evidence is made available that it cannot violate, directly or indirectly, any safety requirement allocated to the element, i.e. it cannot interfere with any safety-related sub-element of the element.

NOTE 1 This means that cascading failures from this sub-element to the safety-related elements are absent.

NOTE 2 This can be achieved by design precautions such as those concerning the data flow and control flow for software, or the I/O 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 made available.

6.4.5 If safety-related sub-elements with different ASILs, including QM(x) (see 5.4.10), coexist in the same element, then a sub-element shall only be treated as a sub-element with a lower ASIL assigned if evidence is made available that, for each safety requirement allocated to the element, it cannot interfere with any sub-element with a higher ASIL assigned. 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 made available.

6.5 Work products

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

7 Analysis of dependent failures

7.1 Objectives

The analysis of dependent failures aims to identify the single events or single causes that could bypass or invalidate a required independence or freedom from interference between given elements and violate a safety requirement or a safety goal.

7.2 General

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 barrier;

— common external resources.

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 1 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.

EXAMPLE 2 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:

— the independence requirements at the level at which they are 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;

— the freedom from interference requirements at the level at which they are 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 independence or freedom from interference requirements are 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.

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

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 potential for dependent failures can be based on deductive analyses: examination of cut sets or repeated identical events of an FTA can indicate potential for dependent failures.

NOTE 3 The identification can also be supported by inductive analyses: similar parts or components with similar failure modes that appear several times in an FMEA can give additional information about the potential for dependent failures.

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 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 analyzed.

7.4.4 This evaluation shall consider the following topics as applicable:

NOTE 1 The evaluation of the potential dependent failures plausibility 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. IEC 61508 provides information that 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 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 Requirement faults, design faults, implementation faults, faults resulting from the use of new technologies and faults introduced when making modifications.

c) manufacturing faults;

EXAMPLE 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 Faults related to wiring harness routing; faults related to the inter-changeability of parts; failures of adjacent items or elements.

e) repair faults;

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

f) environmental factors;

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

g) failures of common external resources; and

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

h) stress due to specific situations.

EXAMPLE Wear, ageing.

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 as given in 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.

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.

7.5 Work products

7.5.1 **Analysis of dependent failures**, resulting from 7.4.

8 Safety analyses

8.1 Objectives

The objective of safety analyses is to examine the consequences of faults and failures on the functions, behaviour and design of items and elements. Safety analyses also provide information on conditions and causes that could lead to the 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 identified during the hazard analysis and risk assessment.

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 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 requirements 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;

— 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). 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;

— reliability block diagrams.

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

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

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

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

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

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, 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;

— the architectural information of the element at the level at which the safety analysis is to be performed: 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; and

NOTE 1 The architectural information is used to determine the boundaries of the safety analyses.

— the safety plan in accordance with ISO 26262-2:2011, 6.5.1

NOTE 2 The safety plan contains the objective 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.

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, or 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, or at the hardware level, or at the software level, respectively in accordance with ISO 26262-4, or ISO 26262-5, or ISO 26262-6.

8.4.5 Newly identified hazards by safety analyses during product development not covered in a safety goal shall be introduced and evaluated in the hazard analysis and risk assessment in accordance with the change management in ISO 26262-8.

8.4.6 The fault models used for the safety analyses shall be consistent with the appropriate development subphases, e.g. hardware design, evaluation of the hardware architectural metrics and evaluation of safety goal violations due to random hardware failures in ISO 26262-5.

8.4.7 The need for additional safety-related test cases shall be determined by using the fault models and the results of the safety analyses.

8.4.8 The results of the safety analyses shall be verified in accordance with ISO 26262-8.

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; or

— the interaction of the item or element with other items or elements; or

— 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 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 If quantitative safety analyses are applicable, 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);

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

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

8.5 Work products

8.5.1 **Safety analyses**, resulting from 8.4.

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 ASIL-oriented and safety-oriented analyses

Clause	Objectives	Prerequisites	Work products
5 Requirements decomposition with respect to ASIL tailoring	This clause provides rules and guidance for decomposing safety requirements into redundant safety requirements to allow ASIL tailoring at the next level of detail.	The safety requirements at the level at which the ASIL decomposition is to be applied: system, or hardware, or software level. The architectural information at the level at which the ASIL decomposition is to be applied: system, or 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 provides criteria for the coexistence within the same element of: — safety-related sub-elements with sub-elements that have no ASIL assigned; and — 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. The architectural information of the element at the level at which the analysis is to be performed: system, or hardware, or software.	6.5.1 Update of ASIL as attribute of sub-elements of elements
7 Analysis of dependent failures	The analysis of dependent failures aims to identify the single events or single causes that could bypass or invalidate a required independence or freedom from interference between given elements and violate a safety requirement or a safety goal.	The independence requirements at the level at which they are applied: system, or hardware, or software. The freedom from interference requirements at the level at which they are applied: system, or hardware, or software. The architectural information at the level at which the independence or freedom from interference requirements are to be applied: system, or hardware, or software.	7.5.1 Analysis of dependent failures
8 Safety analyses	The objective of safety analyses is to examine the consequences of faults and failures on the functions, behaviour and design of items and elements. Safety analyses also provide information on conditions and causes that could lead to the 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.	The safety requirements at the level at which the safety analysis is to be performed: system, or hardware, or software. The architectural information of the element at the level at which the safety analysis is to be performed: system, or hardware, or software. The safety plan.	8.5.1 Safety analyses

Bibliography

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

ICS 43.040.10
Price based on 16 pages

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™