INTERNATIONAL STANDARD

ISO 26262-3

Second edition
2018-12

Road vehicles — Functional safety —

Part 3: Concept phase

Véhicules routiers — Sécurité fonctionnelle —

Partie 3: Phase de projet

Reference number
ISO 26262-3:2018(E)

COPYRIGHT PROTECTED DOCUMENT

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.

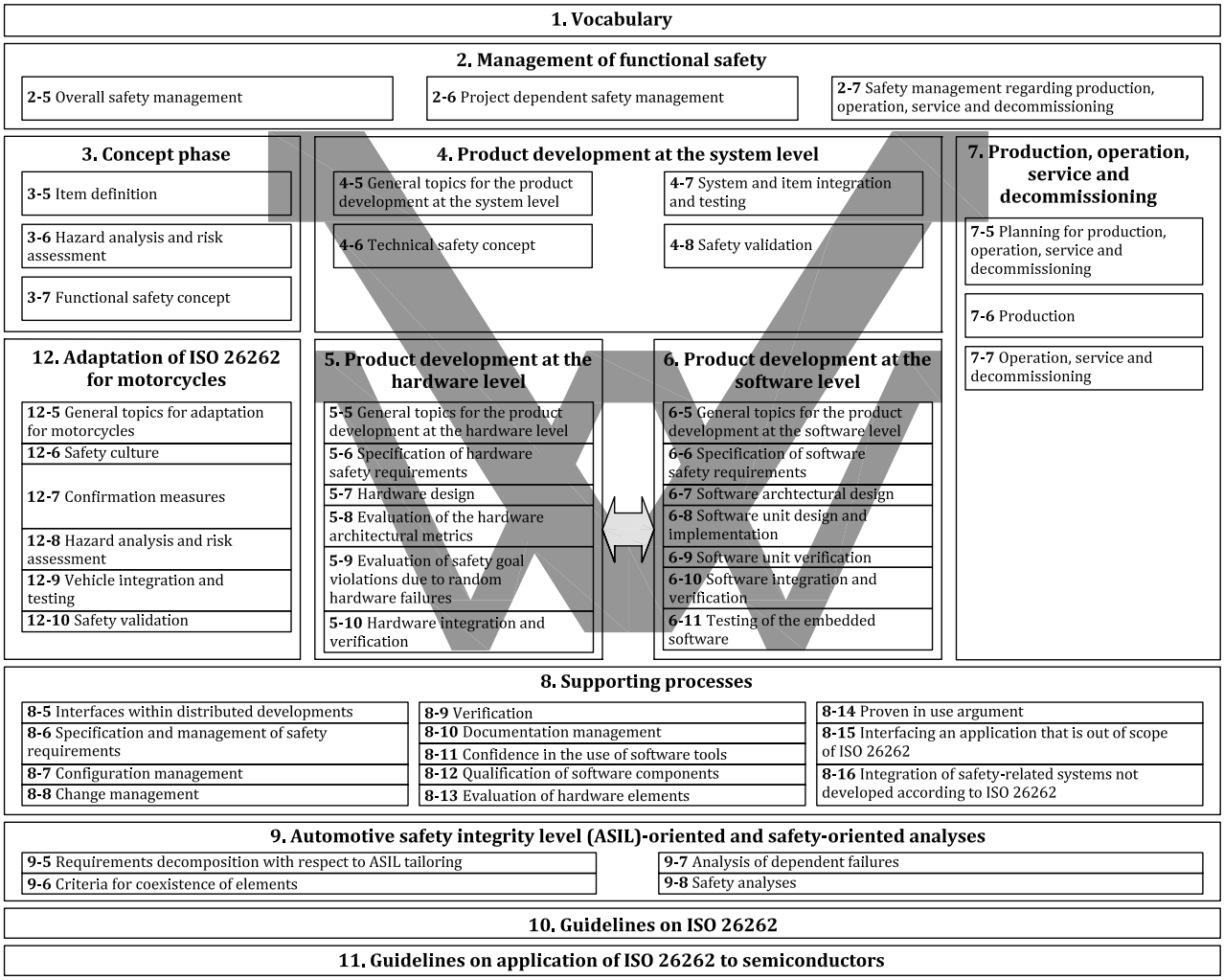


Figure 1 — Overview of the ISO 26262 series of standards

Road vehicles — Functional safety —

Part 3: Concept phase

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 the concept phase for automotive applications, including the following:

— item definition;

— hazard analysis and risk assessment; and

— functional safety concept.

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, *Road Vehicles — Functional Safety — Part 1: Vocabulary*

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

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

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

ISO 26262-9:2018, *Road vehicles — Functional safety — Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses*

3 Terms and definitions

For the purposes of this document, the terms, definitions and abbreviated terms given in ISO 26262-1 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 ISO 26262-9:2018, 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 Item definition

5.1 Objectives

The objectives of this clause are:

a) to define and describe the item, its functionality, dependencies on, and interaction with, the driver, the environment and other items at the vehicle level; and

b) to support an adequate understanding of the item so that the activities in subsequent phases can be performed.

5.2 General

This clause lists the requirements and recommendations for establishing the definition of the item, including its functionality, interfaces, environmental conditions, legal requirements and hazards. This definition serves to provide sufficient information about the item to the persons who conduct the subsequent sub-phases: "Hazard analysis and risk assessment" (see Clause 6) and "Functional safety concept" (see Clause 7).

NOTE Table A.1 provides an overview of objectives, prerequisites and work products of the concept phase.

5.3 Inputs to this clause

5.3.1 Prerequisites

None.

5.3.2 Further supporting information

The following information can be considered:

— any information that already exists concerning the item, e.g. a product idea, a project sketch, relevant patents, the results of pre-trials, the documentation from predecessor items, relevant information on other items.

5.4 Requirements and recommendations

5.4.1 The requirements of the item shall be made available, including:

NOTE 1 Requirements can be classified as safety-related after safety goals and their respective ASIL have been defined.

NOTE 2 If the functional and non-functional requirements are not already available, their generation can be triggered by the requirements of this clause.

a) legal requirements, national and international standards;

b) the functional behaviour at the vehicle level, including the operating modes or states;

c) the required quality, performance and availability of the functionality, if applicable;

d) constraints regarding the item such as functional dependencies, dependencies on other items, and the operating environment;

e) potential consequences of behavioural shortfalls including known failure modes and hazards, if any; and

NOTE 3 This can include known safety-related incidents including similar items.

f) the capabilities of the actuators, or their assumed capabilities.

NOTE 4 These values (e.g. torque output, force exerted, speed of operation, brightness, loudness), or their estimates, are necessary to determine the magnitude of the effect when performing the hazard analysis and risk assessment. The magnitude of the effect is taken into account when deciding the values of severity and controllability.

5.4.2 The boundary of the item, its interfaces, and the assumptions concerning its interaction with other items and elements, shall be defined considering:

a) the elements of the item;

NOTE 1 The elements can also be based on other technology.

b) the assumptions concerning the effects of the item's behaviour on the vehicle;

c) the functionality of the item under consideration required by other items and elements;

d) the functionality of other items and elements required by the item under consideration;

e) the allocation and distribution of functions among the involved systems and elements; and

f) the operational scenarios which impact the functionality of the item.

NOTE 2 With increasing complexity of vehicle functions, there are dependencies between items. One item can be realized by an array of systems that themselves implement other vehicle level functions, i.e. can be considered as items in their own right.

EXAMPLE A combined adaptive cruise control and lane keeping assist function is implemented in a braking system, a steering system and a propulsion system. In this example the braking system implements the service braking function, which can be considered an item in its own right.

NOTE 3 If the scope of the development is an element and not an item, then refer to ISO 26262-2:2018, 6.4.5.7.

5.5 Work products

5.5.1 **Item definition** resulting from requirements in 5.4.

6 Hazard analysis and risk assessment

6.1 Objectives

The objectives of this clause are:

a) to identify and to classify the hazardous events caused by malfunctioning behaviour of the item; and

b) to formulate the safety goals with their corresponding ASILs related to the prevention or mitigation of the hazardous events, in order to avoid unreasonable risk.

6.2 General

Hazard analysis, risk assessment and ASIL determination are used to determine the safety goals for the item. For this, the item is evaluated with regard to its potential hazardous events. Safety goals and their assigned ASIL are determined by a systematic evaluation of hazardous events. The ASIL is determined by considering severity, probability of exposure and controllability. It is based on the item's functional behaviour; therefore, the detailed design of the item does not need to be known.

6.3 Inputs to this clause

6.3.1 Prerequisites

The following information shall be available:

— item definition in accordance with 5.5.1.

6.3.2 Further supporting information

The following information can be considered:

— relevant information on other items (from an external source).

6.4 Requirements and recommendations

6.4.1 Initiation of the hazard analysis and risk assessment

6.4.1.1 The hazard analysis and risk assessment shall be based on the item definition.

6.4.1.2 The item without internal safety mechanisms shall be evaluated during the hazard analysis and risk assessment, i.e. safety mechanisms intended to be implemented or that have already been implemented in predecessor items shall not be considered in the hazard analysis and risk assessment.

NOTE 1 In the evaluation of an item, available and sufficiently independent external measures can be beneficial.

EXAMPLE Electronic stability control can mitigate the effect of failures in chassis systems by increasing the controllability for the driver if it is shown to be available and independent from the item under evaluation.

NOTE 2 Safety mechanisms of the item that are intended to be implemented or that have already been implemented are incorporated as part of the functional safety concept.

6.4.2 Situation analysis and hazard identification

6.4.2.1 The operational situations and operating modes in which an item's malfunctioning behaviour will result in a hazardous event shall be described; both when the vehicle is correctly used and when it is incorrectly used in a reasonably foreseeable way.

NOTE 1 Operational situations describe conditions within which the item is assumed to behave in a safe manner.

NOTE 2 Hazards resulting only from the item behaviour, in the absence of any item failure, are outside the scope of this document.

6.4.2.2 The hazards shall be determined systematically based on possible malfunctioning behaviour of the item.

NOTE 1 FMEA approaches and HAZOP are suitable to support hazard identification at the item level. These can be supported by brainstorming, checklists, quality history, and field studies.

NOTE 2 The responsibility to establish external measures to mitigate the additional risks from transporting goods is outside of the scope of ISO 26262. Therefore, the additional risks related to the transport of goods are not part of the hazard analysis and risk assessment.

6.4.2.3 Hazards caused by malfunctioning behaviour of the item shall be defined at the vehicle level.

NOTE 1 In general, each hazard will have a variety of potential causes related to the item's implementation, but these causes do not need to be considered in the hazard analysis and risk assessment for the analysis of the malfunctioning behaviour.

NOTE 2 Only hazards associated with malfunctioning behaviour of the item are considered; every other system (external measure) is presumed to be functioning correctly provided it is sufficiently independent.

6.4.2.4 If there are hazards identified in this clause that are outside of the scope of ISO 26262 (see Clause 1), then these hazards shall be addressed according to organization specific procedures.

NOTE As these hazards are outside the scope of ISO 26262, this document does not provide guidance for ASIL compliance of these hazards. Such hazards are classified according to the procedures of the applicable safety discipline.

6.4.2.5 Relevant hazardous events shall be determined.

6.4.2.6 The consequences of hazardous events shall be identified.

NOTE If malfunctioning behaviour induces the loss of several functions of the item, then the situation analysis and hazard identification consider the combined effects.

EXAMPLE 1 Loss of the functionality of a braking system (ESC) can lead to the simultaneous unavailability of driver assistance functions.

EXAMPLE 2 Failure of the vehicle's electrical power supply system can lead to a simultaneous loss of a number of functions including "engine torque", "power assisted steering" and "forward illumination".

6.4.2.7 It shall be ensured that the chosen level of detail of the list of operational situations does not lead to an inappropriate lowering of the ASIL.

NOTE A very detailed list of operational situations (see 6.4.2.1) for one hazard, with regard to the vehicle state, road conditions and environmental conditions, can lead to a fine granularity of situations for the classification of hazardous events. This can make it easier to rate controllability and severity. However, a larger number of different operational situations can lead to a consequential reduction of the respective classes of exposure, and thus to an inappropriate lowering of the ASIL. This can be avoided by aggregating similar situations.

6.4.3 Classification of hazardous events

6.4.3.1 All hazardous events identified in 6.4.2 shall be classified, except those that are outside the scope of ISO 26262.

NOTE If classification of a given hazard with respect to severity (S), probability of exposure (E) or controllability (C) is difficult to make, it is classified conservatively, i.e. whenever there is a reasonable doubt, a higher S, E or C classification is chosen.

6.4.3.2 The severity of potential harm shall be estimated based on a defined rationale for each hazardous event. The severity shall be assigned to one of the severity classes S0, S1, S2 or S3 in accordance with Table 1.

NOTE 1 The risk assessment of hazardous events focuses on the harm to each person potentially at risk – including the driver or the passengers of the vehicle causing the hazardous event, and other persons potentially at risk such as cyclists, pedestrians or occupants of other vehicles. The description of the Abbreviated Injury Scale (AIS) can be used for characterising the severity and can be found in Annex B, along with informative examples of different types of severity and accidents.

NOTE 2 The severity class can be based on a combination of injuries, and this can lead to a higher classification of the severity than would result from just looking at a single injury.

NOTE 3 The estimate considers reasonable sequences of events for the operational situation being evaluated.

NOTE 4 The severity classification is based on a representative sample of persons at risk.

Table 1 — Classes of severity

	Class			
	S0	**S1**	**S2**	**S3**
Description	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

6.4.3.3 There are operational situations that result in harm (e.g. an accident). A subsequent malfunctioning behaviour of the item in such an operational situation can increase, or fail to decrease, the resulting harm. In this case the classification of the severity may be limited to the difference between the severity caused by the initial operational situation (e.g. the accident) and the malfunctioning behaviour of the item.

EXAMPLE 1 If an accident occurs which is not caused by the malfunctioning behaviour of an item, the resulting harm from the accident is not considered for the classification of the severity.

EXAMPLE 2 The item under consideration includes an airbag functionality to reduce harm caused by the crash. For an accident in which the airbag fails to deploy, the harm caused by the crash can be determined. If a correctly operating airbag would have reduced the harm of the same accident to a lower severity class, then only the difference is considered for the severity classification.

6.4.3.4 The severity class S0 may be assigned if the hazard analysis and risk assessment determines that the consequences of a malfunctioning behaviour of the item are clearly limited to material damage. If a hazardous event is assigned severity class S0, no ASIL assignment is required.

6.4.3.5 The probability of exposure of each operational situation shall be estimated based on a defined rationale for each hazardous event. The probability of exposure shall be assigned to one of the probability classes, E0, E1, E2, E3 or E4 in accordance with Table 2.

NOTE 1 For classes E1 to E4, the difference in probability from one E class to the next is an order of magnitude.

NOTE 2 The exposure determination is based on a representative sample of operational situations for the target markets.

NOTE 3 For further information and examples related to the probability of exposure see Annex B.

Table 2 — Classes of probability of exposure regarding operational situations

	Class				
	E0	**E1**	**E2**	**E3**	**E4**
Description	Incredible	Very low probability	Low probability	Medium probability	High probability

6.4.3.6 The number of vehicles equipped with the item shall not be considered when estimating the probability of exposure.

NOTE The evaluation of the probability of exposure is performed assuming each vehicle is equipped with the item. This means that the argument “the probability of exposure can be reduced, because the item is not present in every vehicle (as only some vehicles are equipped with the item)” is not valid.

6.4.3.7 Class E0 may be used for those operational situations that are suggested during hazard analysis and risk assessment, but that are considered incredible, and therefore not explored further. A rationale shall be recorded for the exclusion of these situations. If a hazardous event is assigned exposure class E0, no ASIL assignment is required.

EXAMPLE E0 can be used in the case of “force majeure” risk (see B.3).

6.4.3.8 The controllability of each hazardous event, by the driver or other persons involved in the operational situation shall be estimated based on a defined rationale for each hazardous event. The controllability shall be assigned to one of the controllability classes C0, C1, C2 or C3 in accordance with Table 3.

NOTE 1 For classes C1 to C3, the difference in probability from one C class to the next is an order of magnitude.

NOTE 2 The evaluation of the controllability is an estimate of the probability that someone is able to gain sufficient control of the hazardous event, such that they are able to avoid the specific harm. For this purpose, the parameter C is used, with the classes C0, C1, C2 and C3, to classify the potential of avoiding harm. It is assumed that the driver is in an appropriate condition to drive (e.g. they are not tired), has the appropriate driver training (they have a driver's licence) and is complying with the applicable legal regulations, including due care requirements to avoid risks to other traffic participants. Some examples, which serve as an interpretation of these classes, are listed in Table B.6.

NOTE 3 Reasonably foreseeable misuse is considered, e.g. “not keeping the required distance to the vehicle in front as a common behaviour”.

NOTE 4 Where the hazardous event is not related to the control of the vehicle direction and speed, e.g. potential limb entrapment in moving parts, the controllability can be an estimate of the probability that the person at risk is able to remove themselves, or to be removed by others from the hazardous situation. When considering controllability, note that the person at risk might not be familiar with the operation of the item or may not be aware that a potentially hazardous situation evolves.

NOTE 5 When controllability involves the actions of multiple traffic participants, the controllability assessment can be based on the controllability of the vehicle with the malfunctioning item and the assumed action of other participants.

Table 3 — Classes of controllability

	Class			
	C0	**C1**	**C2**	**C3**
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

6.4.3.9 Class C0 may be used for hazards addressing the unavailability of the item if they do not affect the safe operation of the vehicle (e.g. some driver assistance systems) or if an accident can be avoided by routine driver actions. If a hazardous event is assigned controllability class C0, no ASIL assignment is required.

EXAMPLE 1 If loss of propulsion occurs in the garage when attempting to drive away from the house, C0 can be chosen as any driver can put the car back in park.

NOTE Dedicated regulations that specify a functional performance with regard to the applicable hazardous event can be used as part of a rationale when selecting a suitable controllability class, if applicable, and supported by evidence, e.g. real usage experience.

EXAMPLE 2 A dedicated regulation that covers the requirements for the certification of a vehicle system with a precise definition of forces or acceleration values in the case of a failure.

6.4.3.10 An ASIL shall be determined for each hazardous event based on the classification of severity, probability of exposure and controllability, in accordance with Table 4.

NOTE 1 Four ASILs are defined: ASIL A, ASIL B, ASIL C and ASIL D, where ASIL A is the lowest safety integrity level and ASIL D the highest one.

NOTE 2 In addition to these four ASILs, the class QM (quality management) denotes no requirement to comply with ISO 26262. Nevertheless, the corresponding hazardous event can have consequences with regards to safety and safety requirements can be formulated in this case. The classification QM indicates that quality processes are sufficient to manage the identified risk.

Table 4 — ASIL determination

Severity class	Exposure class	Controllability class		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A[a]
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

[a] See 6.4.3.11.

6.4.3.11 If several unlikely situations are combined that result in a lower probability of exposure than E1, QM may be argued for S3, C3 based on this combination.

EXAMPLE 1 For the malfunction of a high voltage system erroneously supplying power. The combined operational situations are:

— a crash which deploys the airbag;

— with the vehicle lying partly in the water; and

— the high voltage system partially exposed without causing an internal short circuit.

EXAMPLE 2 For the malfunction of a fuel pump supplying petrol erroneously. The combined operational situations are:

— a crash which deploys the airbag;

— the tank system behind the pump remains fully functional;

— the fuel line from the pump is broken, such that petrol can drip on hot parts; and

— the energy supply of the pump is fully functional.

6.4.4 Determination of safety goals

6.4.4.1 A safety goal shall be determined for each hazardous event with an ASIL evaluated in the hazard analysis and risk assessment. If similar safety goals are determined, these may be combined into one safety goal.

NOTE Safety goals are top-level safety requirements for the item. They lead to the functional safety requirements needed to avoid an unreasonable risk for each hazardous event. Safety goals are not expressed in terms of technological solutions, but in terms of functional objectives.

6.4.4.2 The ASIL determined for the hazardous event shall be assigned to the corresponding safety goal. If similar safety goals are combined into a single one, in accordance with 6.4.4.1, the highest ASIL shall be assigned to the combined safety goal.

6.4.4.3 The safety goals together with their ASIL shall be specified in accordance with ISO 26262-8:2018, Clause 6.

NOTE The safety goal can specify the fault tolerant time interval, or physical characteristics (e.g. a maximum level of unwanted steering-wheel torque, maximum level of unwanted acceleration) if they were relevant to the ASIL determination.

6.4.4.4 Assumptions used for, or resulting from the hazard analysis and risk assessment which are relevant for ASIL determination (if applicable, including hazardous events classified QM or with no ASIL assigned) shall be identified. These assumptions shall be validated in accordance with ISO 26262-4:2018, Clause 8 for the integrated item.

NOTE Assumptions, if any, that are considered during the HARA include assumed actions of the driver or persons at risk and assumptions regarding external measures.

6.4.5 Management of variances of T&B in hazard analysis and risk assessment

6.4.5.1 The requirements in 6.4.5 shall only be applied to T&B.

6.4.5.2 The following variances shall be considered when conducting a hazard analysis and risk assessment for a T&B vehicle:

a) type of base vehicle;

b) the T&B vehicle configuration; and

c) the T&B vehicle operation.

NOTE Engineering judgement is appropriate when selecting variance types for the analysis.

EXAMPLE 1 Wheel spin may only be relevant for unloaded trucks which is not as common as loaded trucks, thereby affecting probability of exposure.

EXAMPLE 2 An attached trailer may reduce driver's controllability of the vehicle when compared to no trailer attached for certain hazards, thereby affecting controllability.

EXAMPLE 3 Different T&B bodies may have different safety properties, thereby affecting severity.

6.4.5.3 When conducting a hazard analysis and risk assessment each relevant type of base vehicle shall be considered.

6.4.5.4 The number of vehicles of a given type of base vehicle shall not be considered when estimating the probability of exposure.

6.4.5.5 The number of vehicles equipped with a specific configuration shall not be considered when estimating the probability of exposure.

6.4.5.6 When conducting a hazard analysis and risk assessment the variances in operational situations that have impact on technical parameters shall be considered.

NOTE 1 The use of the vehicle is part of the considered operational situation and is considered when estimating the probability of exposure.

EXAMPLE 1 Driving a tractor without a semi-trailer attached results in a low load on the drive axle (technical parameter) which leads to a reduction of vehicle dynamics stability. When estimating the probability of exposure, the operational situation would be for example: "Driving a tractor on public roads without a semi-trailer". With reference to Table B.4, this scenario could be classified as E2.

NOTE 2 When conducting a hazard analysis and risk assessment, the body application can be considered as cargo. Variations in the cargo can be considered.

EXAMPLE 2 Variations in loading condition (full, partial, empty) and position of centre of gravity.

NOTE 3 Functions of body builder equipment, especially machinery functions, can be in scope of other safety standards. Hazard analysis and risk assessment for these functions is done following the specific applicable safety standards.

NOTE 4 For functions of the vehicle that are designed to support dedicated body applications the operational situations of the body can be considered during the hazard analysis and risk assessment.

6.4.5.7 When classifying the parameters Severity, Exposure and Controllability, an appropriate combination of the variance types for an item shall be considered.

NOTE The appropriate combination can be determined based on engineering judgement.

6.4.6 Verification

6.4.6.1 The hazard analysis and risk assessment including the safety goals shall be verified in accordance with ISO 26262-8:2018, Clause 9, to provide evidence for the:

a) appropriate selection with regard to operational situations and hazard identification (and T&B vehicle configuration);

b) compliance with the item definition;

c) consistency with related hazard analyses and risk assessments of other items;

d) completeness of the coverage of the hazardous events; and

e) consistency of the safety goals with the assigned ASILs and the corresponding hazardous events.

6.5 Work products

6.5.1 Hazard analysis and risk assessment report resulting from requirements in 6.4.1 to 6.4.5.

6.5.2 Verification report of the hazard analysis and risk assessment resulting from requirement 6.4.6.

7 Functional safety concept

7.1 Objectives

The objectives of this clause are:

a) to specify the functional or degraded functional behaviour of the item in accordance with its safety goals;

b) to specify the constraints regarding suitable and timely detection and control of relevant faults in accordance with its safety goals;

c) to specify the item level strategies or measures to achieve the required fault tolerance or adequately mitigate the effects of relevant faults by the item itself, by the driver or by external measures;

d) to allocate the functional safety requirements to the system architectural design, or to external measures; and

e) to verify the functional safety concept and specify the safety validation criteria.

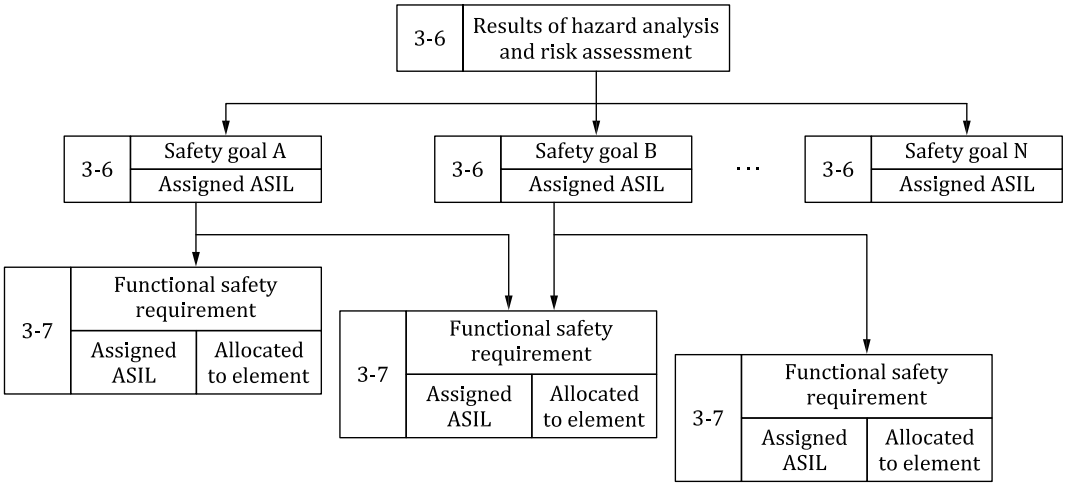
7.2 General

To comply with the safety goals, the functional safety concept contains safety measures, including the safety mechanisms, to be implemented in the item's architectural elements and specified in the functional safety requirements.

Figure 2 illustrates the hierarchical approach by which the safety goals are determined as a result of the hazard analysis and risk assessment. The functional safety requirements are then derived from the safety goals and are allocated to the system architectural design.

Using preliminary architectural assumptions provides a means to handle immature architectural information in early development phases.

For the structure and distribution of safety requirements within the corresponding Parts of ISO 26262, see ISO 26262-8:2018, Figure 2.



NOTE Within the figure, the specific clauses of each part of ISO 26262 are indicated in the following manner: "m-n", where "m" represents the number of the part and "n" indicates the number of the clause, e.g. "3-6" represents ISO 26262-3:2018, Clause 6.

Figure 2 — Hierarchy of safety goals and functional safety requirements

7.3 Inputs to this clause

7.3.1 Prerequisites

The following information shall be available:

— item definition in accordance with 5.5.1;

— hazard analysis and risk assessment report in accordance with 6.5.1; and

— system architectural design (from an external source).

7.3.2 Further supporting information

The following information can be considered:

None.

7.4 Requirements and recommendations

7.4.1 General

The functional safety requirements shall be specified in accordance with ISO 26262-8:2018, Clause 6.

7.4.2 Derivation of functional safety requirements

7.4.2.1 The functional safety requirements shall be derived from the safety goals, considering the system architectural design.

7.4.2.2 At least one functional safety requirement shall be derived from each safety goal.

NOTE The same functional safety requirement can be derived from several safety goals (see Figure 2).

7.4.2.3 The functional safety requirements shall specify, if applicable, strategies for:

a) fault avoidance;

b) fault detection and control of faults or the resulting malfunctioning behaviour;

c) transitioning to a safe state, and if applicable, from a safe state;

d) fault tolerance;

e) the degradation of the functionality in the presence of a fault and its interaction with f) or g);

EXAMPLE Maintaining the vehicle in a limp-home mode until the ignition has been switched from "on" to "off".

f) driver warnings needed to reduce the risk exposure time to an acceptable duration;

g) driver warnings needed to increase the controllability by the driver (e.g. engine malfunction indicator lamp, ABS fault warning lamp);

h) how timing requirements at the vehicle level are met, i.e. how the fault tolerant time interval shall be met by defining a fault handling time interval; and

i) avoidance or mitigation of a hazardous event due to improper arbitration of multiple control requests generated simultaneously by different functions.

NOTE List items c), e), f) and g) can be part of the warning and degradation strategy.

7.4.2.4 Each functional safety requirement shall be specified by considering the following, as applicable:

a) operating modes;

b) fault tolerant time interval;

c) safe states;

d) emergency operation time interval; and

e) functional redundancies (e.g. fault tolerance).

NOTE This activity can be supported by safety analyses (e.g. FMEA, FTA, HAZOP) in order to develop a complete set of effective functional safety requirements.

7.4.2.5 If a safety goal violation can be prevented by transitioning to, or by maintaining, one or more safe states, then the corresponding safe state(s) shall be specified.

EXAMPLE A safe state could be "switched off", "locked", "vehicle stationary and maintained", or "reduced functionality" in the case of a failure over a defined time.

7.4.2.6 If a safe state cannot be reached by a transition within an acceptable time interval, an emergency operation shall be specified.

7.4.2.7 If assumptions are made about the necessary actions of the driver, or other persons, in order to prevent the violation of a safety goal, then the following shall apply:

NOTE 1 The actions include those for which credit was taken during controllability estimation, and any further necessary actions taken to comply with the safety goals after the implementation of the safety requirements.

EXAMPLE Adaptive cruise control: the ACC generated brake activation being overridden when the driver presses the accelerator pedal.

a) these actions shall be specified in the functional safety concept; and

b) the adequate means and controls available to the driver or other persons shall be specified in the functional safety concept.

NOTE 2 Driver task analysis can be helpful to consider prevention of driver overload, prevention of driver surprise or panic (loss of capability to control vehicle), and mode confusion (an incorrect assumption about the operating mode).

NOTE 3 The specification of the warning and degradation strategy and the necessary actions of the driver and other persons potentially at risk are a potential input for the user's manual (see ISO 26262-7:2018, Clause 5).

7.4.2.8 The functional safety requirements shall be allocated to the elements of the system architectural design:

a) During requirement allocation, the ASIL and information given in 7.4.2.4 shall be inherited from the associated safety goal. If ASIL decomposition is applied then the requirements of ISO 26262-9:2018, Clause 5 are also applicable.

b) If freedom from interference in accordance with ISO 26262-9:2018, Clause 6 between elements implementing safety requirements cannot be argued in the system architectural design, then the architectural elements shall be developed in accordance with the highest ASIL for those safety requirements.

c) If the item comprises more than one E/E system, then the functional safety requirements for the individual E/E systems and their interfaces shall be specified, considering the system architectural design. These functional safety requirements shall be allocated to the E/E systems.

d) If the item comprises more than one E/E system then the corresponding target values for random hardware fault metrics (see ISO 26262-5:2018, Clauses 8 and 9) can be specified and allocated to each individual E/E system in accordance with ISO 26262-4:2018, 6.4.5.2.

   NOTE 1 The specification of E/E system target values is done according to the system architectural design and further refined during the development phases.

e) If ASIL decomposition is applied during the allocation of the functional safety requirements, then it shall be applied in accordance with ISO 26262-9:2018, Clause 5.

NOTE 2 Independence can be verified by an analysis of dependent failures (see ISO 26262-9:2018, Clause 7).

7.4.2.9 If the functional safety concept relies on elements of other technologies, then the following shall apply:

a) the functional safety requirements implemented by elements of other technologies shall be derived and allocated to the corresponding elements of the architecture;

b) the functional safety requirements relating to the interfaces with elements of other technologies shall be specified;

c) the implementation of functional safety requirements by elements of other technologies shall be ensured through specific measures that are outside the scope of ISO 26262; and

d) no ASIL should be assigned to safety requirements allocated to these elements.

NOTE 1 A proper safety attribute can be assigned to safety requirements allocated to elements of other technologies; and the concept of ASIL decomposition, described in ISO 26262-9:2018 Clause 5, could be extrapolated to the allocation of functional safety requirements to these elements. In this case, the appropriate implementation and verification rules are defined in addition to ISO 26262.

NOTE 2 Evidence for the adequacy of elements of other technologies is provided during safety validation activities (see ISO 26262-4:2018, Clause 8).

7.4.2.10 If the functional safety concept relies on external measures, then the following shall apply:

a) the functional safety requirements implemented by external measures shall be derived and communicated;

b) the functional safety requirements of interfaces with external measures shall be specified; and

c) if the external measures are implemented by one or more E/E systems, the functional safety requirements shall be addressed using ISO 26262.

NOTE Evidence for the adequacy of external measures is provided during safety validation activities (see ISO 26262-4:2018, Clause 8).

7.4.3 Safety validation criteria

7.4.3.1 The acceptance criteria for safety validation of the item shall be specified based on the functional safety requirements and the safety goals.

NOTE 1 For further requirements on detailing the criteria and a list of characteristics to be validated (see ISO 26262-4:2018, Clause 8).

NOTE 2 Safety validation of the safety goals is addressed on the upper right of the V cycle but is included in the activities during development and not only performed at the end of development.

7.4.4 Verification of the functional safety concept

7.4.4.1 The functional safety concept shall be verified in accordance with ISO 26262-8:2018, Clause 9, to provide evidence for:

a) its consistency and compliance with the safety goals; and

b) its ability to mitigate or avoid the hazards.

NOTE 1 Verification of the ability to mitigate or avoid a hazard can be carried out during the concept phase to evaluate the safety concept and indicate where concept improvements are needed. This verification can be based on the same methods that are used for safety validation. However, the safety validation undertaken (to fulfil ISO 26262-4:2018, Clause 8) cannot be based on concept studies alone (e.g. prototypes).

EXAMPLE The ability to mitigate or to avoid a hazard can be evaluated by tests, trials or expert judgement; with prototypes, studies, subject tests, or simulations.

NOTE 2 The verification of the ability to mitigate or to avoid a hazard addresses the characteristics of the fault (e.g. being transient or permanent).

NOTE 3 For verification, a traceability based argument can be used, i.e. the item complies with the safety goals if the item complies with the functional safety requirements.

7.5 Work products

7.5.1 **Functional safety concept** resulting from requirements in 7.4.1 to 7.4.3.

7.5.2 **Verification report of the functional safety concept** resulting from requirements in 7.4.4.

Annex A
(informative)

Overview of and workflow of concept phase

Table A.1 provides an overview of objectives, prerequisites and work products of the concept phase.

Table A.1 — Overview of concept phase

Clause	Objectives	Prerequisites	Work products
5 Item definition	The objectives of this Clause are: a) to define and describe the item, its functionality, dependencies on, and interaction with, the driver, the environment and other items at the vehicle level; and b) to support an adequate understanding of the item so that the activities in subsequent phases can be performed.	None	5.5.1 Item definition resulting from requirements in 5.4.
6 Hazard analysis and risk assessment	The objectives of this Clause are: a) to identify and to classify the hazardous events caused by malfunctioning behaviour of the item; and b) to formulate the safety goals with their corresponding ASILs related to the prevention or mitigation of the hazardous events, in order to avoid unreasonable risk.	Item definition (see 5.5.1)	6.5.1 Hazard analysis and risk assessment report resulting from requirements 6.4.1 to 6.4.5. 6.5.2 Verification report of the hazard analysis and risk assessment resulting from requirement 6.4.6.
7 Functional safety concept	The objectives of this Clause are: a) to specify the functional or degraded functional behaviour of the item in accordance with its safety goals; b) to specify the constraints regarding suitable and timely detection and control of relevant faults in accordance with its safety goals; c) to specify the item level strategies or measures to achieve the required fault tolerance or adequately mitigate the effects of relevant faults by the item itself, by the driver or by external measures; d) to allocate the functional safety requirements to the system architectural design, or to external measures; and e) to verify the functional safety concept and specify the safety validation criteria.	Item definition (see 5.5.1) Hazard analysis and risk assessment report (see 6.5.1) System architectural design (from external source)	7.5.1 Functional safety concept resulting from requirements 7.4.1 to 7.4.3. 7.5.2 Verification report of the functional safety concept resulting from requirements in 7.4.4.

Annex B
(informative)

Hazard analysis and risk assessment

B.1 General

This annex gives a general explanation of the hazard analysis and risk assessment. The examples in B.2 (severity), B.3 (probability of exposure) and B.4 (controllability) are for information only and are not exhaustive.

For this analytical approach, a risk (R) can be described as a function (F), having three parameters: The frequency of occurrence (f) of a hazardous event, the controllability (C), i.e. the ability to avoid the specific harm or damage through timely reactions of the persons involved, and the potential severity (S) of the resulting harm or damage:

$$R = F(f, C, S) \tag{B.1}$$

The frequency of occurrence f is, in turn, influenced by two factors. One factor to consider is how frequently and for how long individuals find themselves in a situation where the aforementioned hazardous event can occur. In ISO 26262 this is simplified to be a measure of the probability of the operational situation taking place in which the hazardous event can occur (exposure, E). Another factor is the occurrence rate of faults in the item. This is not considered during hazard analysis and risk assessment. Instead, the ASILs that result from the classification of E, S, C during hazard analysis and risk assessment determine the minimum set of requirements on the item in order to control or reduce the probability of random hardware failures and to avoid systematic faults. The failure rate of the item is not considered a priori (in the risk assessment) because an unreasonable residual risk is avoided through the implementation of the resulting safety requirements.

The hazard analysis and risk assessment sub-phase comprises three steps, as described below.

a) Situation analysis and hazard identification (see 6.4.2): the goal of the situation analysis and hazard identification is to identify the potential unintended behaviours of the item that could lead to a hazardous event. The situation analysis and hazard identification activity requires a clear definition of the item, its functionality and its boundaries. It is based on the item's behaviour; therefore, the detailed design of the item does not necessarily need to be known.

   EXAMPLE Factors to be considered for situation analysis and hazard identification can include:

   — vehicle usage scenarios, for example high speed driving, urban driving, parking, off-road;

   — environmental conditions, for example road surface friction, side winds;

   — reasonably foreseeable driver use and misuse;

   — interaction between operational systems; and

   — T&B base vehicle, vehicle configuration and vehicle operation.

b) Classification of hazardous events (see 6.4.3): the hazard classification scheme comprises the determination of the severity, the probability of exposure, and the controllability associated with the hazardous events of the item. The severity represents an estimate of the potential harm in a particular driving situation, while the probability of exposure is determined by the corresponding situation. The controllability rates how easy or difficult it is for the driver or other road traffic participant to avoid the considered accident type in the considered operational situation. For each

hazard, depending on the number of related hazardous events, the classification will result in one or more combinations of severity, probability of exposure, and controllability.

c) ASIL determination (see 6.4.3): determining the required automotive safety integrity level.

B.2 Examples of severity

B.2.1 General

The potential injuries that result from a hazard are evaluated for the driver, passengers and people around the vehicle, or in surrounding vehicles to determine the severity class for a given hazard. From this evaluation, the corresponding severity class is then determined, for example, as shown in Table B.1.

Table B.1 presents examples of consequences which can occur for a given hazard, and the corresponding severity class for each consequence.

Given the complexity of accidents and the many possible variations of accident situations, the examples provided in Table B.1 represent only an approximate estimate of accident effects. They represent expected values based on previous accident analyses. Therefore, no generally valid conclusions can be derived from these individual descriptions.

Accident statistics can be used to determine the distribution of injuries that can be expected to occur in different types of accidents.

In Table B.1, AIS represents a categorisation of injury classes, but only for single injuries. Instead of AIS, other categorisations such as Maximum AIS (MAIS) and Injury Severity Score (ISS) can be used.

The use of a specific injury scale depends on the state of medical research at the time the analysis is performed. Therefore, the appropriateness of the different injury scales, such as AIS, ISS, and NISS, can vary over time (see References [3],[5],[6]).

B.2.2 Description of the AIS stages

To describe the severity, the AIS classification is used. The AIS represents a classification of the severity of injuries and is issued by the Association for the Advancement of Automotive Medicine (AAAM). The guidelines were created to enable an international comparison of severity. The scale is divided into seven classes:

— AIS 0: no injuries;

— AIS 1: light injuries such as skin-deep wounds, muscle pains, whiplash, etc.;

— AIS 2: moderate injuries such as deep flesh wounds, concussion with up to 15 minutes of unconsciousness, uncomplicated long bone fractures, uncomplicated rib fractures, etc.;

— AIS 3: severe but not life-threatening injuries such as skull fractures without brain injury, spinal dislocations below the fourth cervical vertebra without damage to the spinal cord, more than one fractured rib without paradoxical breathing, etc.;

— AIS 4: severe injuries (life-threatening, survival probable) such as concussion with or without skull fractures with up to 12 hours of unconsciousness, paradoxical breathing;

— AIS 5: critical injuries (life-threatening, survival uncertain) such as spinal fractures below the fourth cervical vertebra with damage to the spinal cord, intestinal tears, cardiac tears, more than 12 hours of unconsciousness including intracranial bleeding;

— AIS 6: extremely critical or fatal injuries such as fractures of the cervical vertebrae above the third cervical vertebra with damage to the spinal cord, extremely critical open wounds of body cavities (thoracic and abdominal cavities), etc.

Table B.1 — Examples of severity classification

	Class of severity (see Table 1)			
	S0	**S1**	**S2**	**S3**
Description	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries
Reference for single injuries (from AIS scale)	AIS 0 and less than 10 % probability of AIS 1-6; or damage that cannot be classified safety-related	More than 10 % probability of AIS 1-6 (and not S2 or S3)	More than 10 % probability of AIS 3-6 (and not S3)	More than 10 % probability of AIS 5-6
Examples	— Bumps with roadside infrastructure — Pushing over roadside post, fence, etc. — Light grazing damage — Damage entering/ exiting parking space — Leaving the road without collision or rollover	— Side impact with a narrow stationary object, e.g. passenger car crashing into a tree (impact to passenger cell) with very low speed — Rear/front collision with another passenger car with very low speed — Front collision (e.g. rear-ending another vehicle, semi-trailer, etc.) without passenger compartment deformation	— Side impact with a narrow stationary object, e.g. passenger car crashing into a tree (impact to passenger cell) with low speed — Rear/front collision with another passenger car with low speed — Pedestrian/ bicycle accident with low speed	— Side impact with a narrow stationary object, e.g. passenger car crashing into a tree (impact to passenger cell) with medium speed — Rear/front collision with another vehicle with medium speed — Front collision (e.g. rear-ending another vehicle, semi-trailer, etc.) with passenger compartment deformation
NOTE The informative examples in Table B.1 can be applied to passenger cars and T&B, but are considered on a case by case basis.				

B.3 Examples and explanations of the probability of exposure

An estimation of the probability of exposure requires the evaluation of the scenarios in which the relevant environmental factors that contribute to the occurrence of the hazard are present. The scenarios to be evaluated include a wide range of driving or operating situations.

These evaluations result in the designation of the hazard scenarios into one of five probability of exposure classifications, given the nomenclature E0 (lowest exposure level), E1, E2, E3 and E4 (highest exposure level).

The first of these, E0, is assigned to situations which, although identified during a hazard analysis and risk assessment, are considered to be unusual or incredible. Subsequent evaluation of the hazards associated exclusively with these E0 scenarios may be excluded from further analysis.

EXAMPLE 1 Typical examples of E0 include the following:

a) a very unusual, or infeasible, co-occurrence of circumstances, e.g. a vehicle involved in an incident which includes an aeroplane landing on a highway; and

b) natural disasters, e.g. earthquake, hurricane, forest fire.

The remaining E1, E2, E3 and E4 levels are assigned for situations that can become hazardous depending on either the duration of a situation (temporal overlap) or the frequency of occurrence of a situation.

NOTE 1 The classification can depend on, for example, geographical location or type of use (see 6.4.3.5).

The exposure (E) to a hazard can be estimated in two ways. The first is based on the duration of a situation and the second is based on the frequency in which a situation is encountered. For example, a hazard can be related to the duration of a given operational situation e.g. the average time spent negotiating traffic intersections, while another hazard can be related to the frequency of the same operational situation e.g. the rate of repetition with which a vehicle negotiates traffic intersections.

In the first case where the exposure is ranked based on the duration of a situation, the probability of exposure is typically estimated by the proportion of time spent in the considered situation compared to the total operating time e.g. ignition on. Note that in some cases the total operating time can be the vehicle life-time (including ignition off). In the second case, it is more appropriate that exposure estimates are determined using the frequency of occurrence of a related driving situation. An example where this is appropriate is where a pre-existing E/E system fault leads to the hazardous event within a short interval after the situation occurs.

Examples of driving situations classified by duration and typical exposure rankings are given in Tables B.2 and B.4 and examples of driving situations classified by frequency are given in Table B.3 and Table B.5.

In addition to these driving situations, the specific context of that operating situation is considered. This is necessary in order to determine the actual exposure in terms of exact time and exact location that leads to the hazardous event.

EXAMPLE 2 A child lock failure by itself does not necessarily lead to a hazardous event unless the child is old enough to unfasten the seatbelt and leave the car into traffic while another car is approaching in that very moment.

A driving situation may have both duration and a frequency, such as driving in a parking lot. In this case, the examples in Tables B.2/B.4 and Tables B.3/B.5 might not lead to the same exposure category, so the most appropriate exposure ranking is selected for the analysis of the considered operational situation.

If the time period in which a failure remains latent is comparable to the time period before the hazardous event can be expected to take place, then the estimation of the probability of exposure considers that time period. Typically this will concern devices that are expected to act on demand, e.g. airbags.

In this case, the probability of exposure is estimated by $\sigma \times T$ where σ is the rate of occurrence of the operational situation and T is the duration during which the failure is not perceived (possibly up to the lifetime of the vehicle). This approximation $\sigma \times T$ is valid when this resulting product is small.

NOTE 2 With regard to the duration of the considered failure, the hazard analysis and risk assessment does not consider safety mechanisms that are part of the item (see 6.4.1.2).

Table B.2 — Classes of probability of exposure regarding duration in operational situations

	Class of probability of exposure in operational situations (see Table 2)			
	E1	**E2**	**E3**	**E4**
Description	Very low probability	Low probability	Medium probability	High probability
Duration (% of average operating time)	Not specified	<1 % of average operating time	1 % to 10 % of average operating time	>10 % of average operating time
Examples for road layout	—	— Country road intersection — Highway exit ramp	— One-way street (city street)	— Highway — Country road

Table B.2 *(continued)*

	Class of probability of exposure in operational situations (see Table 2)			
	E1	**E2**	**E3**	**E4**
Examples for road surface	—	— Snow and ice on road — Slippery leaves on road	— Wet road	—
Examples for vehicle stationary state	— Vehicle during jump start — In repair garage	— Trailer attached — Roof rack attached — Vehicle being refuelled	— Vehicle on a hill (hill hold)	—
Examples for manoeuvre	— Driving downhill with engine off (mountain pass)	— Driving in reverse — Overtaking — Parking (with trailer attached)	— Heavy traffic (stop and go)	— Accelerating — Decelerating — Stopping at traffic light (city street) — Lane change (highway)

Table B.3 — Classes of probability of exposure regarding frequency in operational situations

	Class of probability of exposure in operational situations (see Table 2)			
	E1	**E2**	**E3**	**E4**
Description	Very low probability	Low probability	Medium probability	High probability
Frequency of situation	Occurs less often than once a year for the great majority of drivers	Occurs a few times a year for the great majority of drivers	Occurs once a month or more often for an average driver	Occurs during almost every drive on average
Examples for road layout	—	— Mountain pass with unsecured steep slope	—	—
Examples for road surface	—	— Snow and ice on road	— Wet road	—
Examples for vehicle stationary state	— Stopped, requiring engine restart (at railway crossing) — Vehicle being towed	— Roof rack attached	— Vehicle being refuelled — Vehicle on a hill (hill hold)	—
Examples for manoeuvre	—	— Evasive manoeuvre, deviating from desired path	— Overtaking	— Shifting transmission gears — Executing a turn (steering) — Using indicators — Driving in reverse

Table B.4 and B.5 provide examples for T&B. Different types of base vehicles are considered in the tables:

— long haul (LH), for long distance transporting goods;

— distribution (DI), for distributing goods;

— vocational (VO), for performing specific work functions, e.g. dumper truck, concrete mixer, dustcart;

— city bus (CB), for urban and suburban use;

— interurban bus (IB), for interurban transport; and

— coach (CO), for long distance journeys.

Table B.4 — Classes of probability of exposure regarding duration in operational situations for T&B

		Class of probability of exposure in operational situations (see Table 2)			
		E1	**E2**	**E3**	**E4**
Description		Very low probability	Low probability	Medium probability	High probability
Duration (% of average operating time)		Not specified	<1 % of average operating time	1 % to 10 % of average operating time	>10 % of average operating time
Examples for	driving in reverse	—	LH, CB, CO, IB	DI, VO	—
	overtaking another truck or bus with small speed difference (with lane change to oncoming lane)	LH, DI, VO, CO, IB	—	—	—
	driving with trailer attached	—	—	DI, CO, IB	LH, VO
	semi-trailer tractor without trailer attached (on public road)	—	LH, DI, VO	—	—
	driving on construction site (vehicle is driving directly on construction site, not only for delivering goods to construction site)	LH	DI	—	VO
	steep slope	LH, CB	DI, CO, IB	VO	—
	standing at a bus stop	—	—	CO	CB, IB
	entering/driving off from bus stop	—	CO	CB, IB	—
NOTE The informative examples in Table B.2 can be applied to T&B, but are considered on a case by case basis. For situations occurring in both, Table B.2 and Table B.4, Table B.4 is considered more appropriate for T&B.					

Table B.5 — Classes of probability of exposure regarding frequency in operational situations for T&B

		Class of probability of exposure in operational situations (see Table 2)			
		E1	E2	E3	E4
Description		Very low probability	Low probability	Medium probability	High probability
Frequency of situation		Occurs less often than once a year for the great majority of drivers	Occurs a few times a year for the great majority of drivers	Occurs once a month or more often for an average driver	Occurs during almost every drive on average
Examples for	driving in reverse	—	—	CB	LH, DI, VO, CO, IB
	overtaking another truck or bus with small speed difference (with lane change to oncoming lane)	—	—	LH, DI, VO, CO, IB	—
	driving with trailer attached	—	—	DI, CO, IB	LH, VO
	semi-trailer tractor without trailer attached (on public road)	—	DI, VO	LH	—
	driving on construction site (vehicle is driving directly on construction site, not only for delivering goods to construction site)	LH	DI	—	VO
	steep slope	LH, CB	DI, CO, IB	—	VO
	standing at/entering/driving off a bus stop	—	—	—	CB, CO, IB
NOTE The informative examples in Table B.3 can be applied to T&B, but are considered on a case by case basis. For situations occurring in both Table B.3 and Table B.5, Table B.5 is considered more appropriate for T&B.					

B.4 Examples of controllability

To determine the controllability class for a given hazard an estimation of the probability that the representative driver or other persons involved can influence the situation in order to avoid harm is made.

This probability estimation involves the consideration of the likelihood that representative drivers will be able to retain or regain control of the vehicle if the hazard were to occur, or that individuals in the vicinity will contribute to the avoidance of the hazard by their actions. This consideration is based on assumptions about the control actions, necessary by the individuals involved in the hazard scenario, to retain or regain control of the situation, as well as the representative driving behaviour of the drivers involved.

NOTE 1 Controllability estimations can be influenced by a number of factors including driver profiles for the target market, individuals' age, eye-hand coordination, driving experience, cultural background, etc.).

NOTE 2 Estimates can be made using either experimental or analytical procedures.

To aid in these evaluations, Table B.6 provides examples of driving situations in which a malfunction is introduced, and the assumptions about the corresponding control behaviours that would avoid harm. These situations are mapped to the controllability rankings, clarifying the 90 % and 99 % breakpoint levels for judging controllability.

Table B.6 — Examples of possibly controllable hazardous events by the driver or by the persons potentially at risk

	Class of controllability (see Table 3)			
	C0	**C1**	**C2**	**C3**
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable
Driving factors and scenarios	Controllable in general	More than 99 % of the average drivers or other traffic participants are able to avoid harm	Between 90 % an 99 % of the average drivers or other traffic participants are able to avoid harm	Less than 90 % of the average drivers or other traffic participants are able to avoid harm
Example situations that are considered distracting e.g. unexpected radio volume increase or warning message - fuel low	Maintain intended driving path	—	—	—
Example for unavailability of a driver assisting system that does not affect the safe operation of the vehicle	Maintain intended driving path	—	—	—
Example for unintended closing of window while driving	—	Remove arm from window	—	—
Example for blocked steering column when accelerating from standstill	—	Brake to slow/stop vehicle	—	—
Example for failure of ABS during emergency braking	—	—	Maintain intended driving path	
Example for propulsion failure at high lateral acceleration	—	—	Maintain intended driving path	—
Example for inadvertent opening bus door while driving with passenger standing in doorway	—	—	Passenger grabs hand rail to avoid falling out of bus	—
Example for failure of brakes	—	—	—	Steer away from objects in driving path

NOTE 1 For C2, a feasible test scenario in accordance with RESPONSE 3 (see Reference [4]) is accepted as adequate: "Practical testing experience revealed that a number of 20 valid data sets per scenario can supply a basic indication of validity". If each of the 20 data sets complies with the pass-criteria for the test, a level of controllability of 85 % (with a level of confidence of 95 % which is generally accepted for human factors tests) can be proven. This is appropriate evidence of the rationale for a C2-estimate.

NOTE 2 For C1 a test to provide a rationale that 99 % of the drivers "pass" the test in a certain traffic scenario might not be feasible because a large number of test subjects would be necessary as the appropriate evidence for such a rationale. Decision can be based on expert judgement.

NOTE 3 As no controllability is assumed for category C3, it is not relevant to have appropriate evidence of the rationale for such a classification.

NOTE 4 The informative examples in Table B.6 can be applied to passenger cars and T&B vehicles, but are considered on a case-by-case basis.

Table B.6 *(continued)*

	Class of controllability (see Table 3)			
	C0	**C1**	**C2**	**C3**
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable
Example for faulty driver airbag release when travelling at high speed	—	—	—	Maintain intended driving path, stay in lane, or brake to slow/stop vehicle
Example for excessive trailer swing during braking potential for jacknifing	—	—	—	Driver counter-steers and brakes in an attempt to maintain intended driving path
Example for function with high automation where driver is not in the loop	—	—	—	No attempt to maintain intended driving path

NOTE 1 For C2, a feasible test scenario in accordance with RESPONSE 3 (see Reference [4]) is accepted as adequate: "Practical testing experience revealed that a number of 20 valid data sets per scenario can supply a basic indication of validity". If each of the 20 data sets complies with the pass-criteria for the test, a level of controllability of 85 % (with a level of confidence of 95 % which is generally accepted for human factors tests) can be proven. This is appropriate evidence of the rationale for a C2-estimate.

NOTE 2 For C1 a test to provide a rationale that 99 % of the drivers "pass" the test in a certain traffic scenario might not be feasible because a large number of test subjects would be necessary as the appropriate evidence for such a rationale. Decision can be based on expert judgement.

NOTE 3 As no controllability is assumed for category C3, it is not relevant to have appropriate evidence of the rationale for such a classification.

NOTE 4 The informative examples in Table B.6 can be applied to passenger cars and T&B vehicles, but are considered on a case-by-case basis.

Bibliography

[1] ISO 26262-12:2018, *Road Vehicles — Functional Safety — Part 12: Adaptation of ISO 26262 for motorcycles*

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

[3] Abbreviated injury scale; Association of the advancement of Automotive medicine; Barrington, IL, USA Information is also available at www.aaam.org

[4] Code of Practice for the design and evaluation of ADAS, EU Project RESPONSE 3: Oct. 2006; https://www.acea.be/publications/article/code-of-practice-for-the-design-and-evaluation-of-adas

[5] Baker S.P. O'Neill, B., Haddon, W., Long, W.B., The injury severity score: a method for describing patients with multiple injuries and evaluating emergency care. *The Journal of Trauma*, Vol. **14**, No. 3, 1974

[6] Balogh Z., Offner P.J., Moore E.E., Biffl W.L. NISS predicts post injury multiple organ failure better than ISS, *The Journal of Trauma*, Vol. **48**, No. 4, 2000

ICS 43.040.10

Price based on 28 pages