INTERNATIONAL STANDARD

ISO 26262-3

First edition
2011-11-15

Road vehicles — Functional safety —

Part 3: Concept phase

Véhicules routiers — Sécurité fonctionnelle —

Partie 3: Phase de projet

Reference number
ISO 26262-3:2011(E)

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

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 26262-3 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.

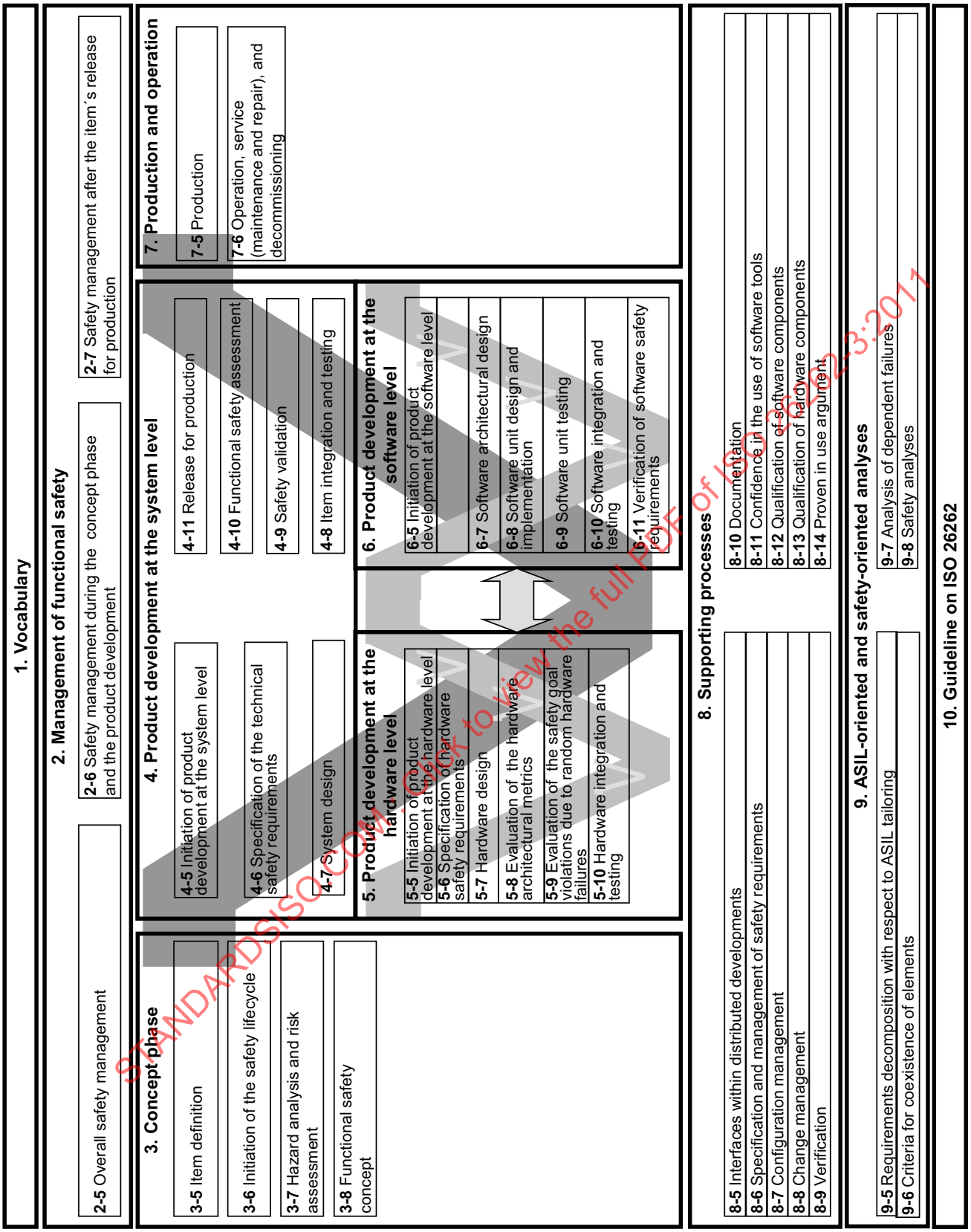


Figure 1 — Overview of ISO 26262

Road vehicles — Functional safety —

Part 3:
Concept phase

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 the concept phase for automotive applications, including the following:

— item definition,

— initiation of the safety lifecycle,

— hazard analysis and risk assessment, and

— functional safety concept.

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

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

ISO 26262-9:2011, *Road vehicles — Functional safety — Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses*

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 ISO 26262-9:2011, Clause 5, 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 Item definition

5.1 Objectives

The first objective is to define and describe the item, its dependencies on, and interaction with, the environment and other items.

The second objective is 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 with regard to its functionality, interfaces, environmental conditions, legal requirements, hazards, etc. This definition serves to provide sufficient information about the item to the persons who conduct the subsequent subphases: “Initiation of safety lifecycle” (see Clause 6), “Hazard analysis and risk assessment” (see Clause 7) and “Functional safety concept” (see Clause 8).

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 independent items.

5.4 Requirements and recommendations

5.4.1 The functional and non-functional requirements of the item as well as the dependencies between the item and its environment shall be made available.

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

NOTE 2 The required information is a necessary input for the item definition although it is not safety-related. If not already available, its generation can be triggered by the requirements of this clause.

This information includes:

a) the functional concept, describing the purpose and functionality, including the operating modes and states of the item;

b) the operational and environmental constraints;

c) legal requirements (especially laws and regulations), national and international standards;

d) behaviour achieved by similar functions, items or elements, if any;

e) assumptions on behaviour expected from the item; and

f) potential consequences of behaviour shortfalls including known failure modes and hazards.

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

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 The elements could also be based on other technology

b) the assumptions concerning the effects of the item's behaviour on other items or elements, that is the environment of the item;

c) interactions of the item with other items or elements;

d) functionality required by other items, elements and the environment;

e) functionality required from other items, elements and the environment;

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

g) the operating scenarios which impact the functionality of the item.

5.5 Work products

Item definition resulting from the requirements of 5.4.

6 Initiation of the safety lifecycle

6.1 Objectives

The first objective of the initiation of the safety lifecycle is to make the distinction between a new item development and a modification to an existing item (see ISO 26262-2:2011, Figure 2).

The second objective is to define the safety lifecycle activities (see ISO 26262-2:2011, Figure 2) that will be carried out in the case of a modification.

6.2 General

Based on the item definition, the safety lifecycle is initiated by distinguishing between either a new development, or a modification of an existing item. In the case of a modification, the tailoring of the safety-related activities takes place.

6.3 Inputs to this clause

6.3.1 Prerequisites

The following information shall be available:

— item definition in accordance with 5.5.

6.3.2 Further supporting information

The following information can be considered:

— any existing information, not already covered by the item definition, being useful for conducting the impact analysis.

EXAMPLE Product concept, requests for change, implementation planning, proven in use argument.

6.4 Requirements and recommendations

6.4.1 Determination of the development category

6.4.1.1 It shall be determined whether the item is either a new development, or if it is a modification of an existing item or its environment:

a) in the case of a new development, the development shall be continued with the hazard analysis and risk assessment in accordance with Clause 7;

b) in the case of a modification of the item or its environment the applicable lifecycle subphases and activities shall be determined in accordance with 6.4.2.

NOTE A proven in use argument can be applied to modification (see ISO 26262-8:2011, Clause 14).

6.4.2 Impact analysis and possible tailored safety lifecycle, in the case of modification

6.4.2.1 An impact analysis shall be carried out in order to identify and describe the intended modification applied to the item or its environment and to assess the impact of these modifications.

NOTE 1 Modifications to the item include design modifications and implementation modifications. Design modification can result from requirements modifications (e.g. functional or performance enhancement or cost optimisation). Implementation modifications do not affect the specification or performance of the item, but only the implementation features.

EXAMPLE Implementation modifications can result from corrections of software, or the use of new development or production tools.

NOTE 2 Modifications to configuration data or calibration data are considered as modifications to the item if they impact the functional behaviour of the item.

NOTE 3 Modifications to the environment of the item can result from the installation of the item in a new target environment (e.g. another vehicle variant) or by the upgrading of other items or elements interacting with (or in the vicinity of) the item.

6.4.2.2 The impact analysis shall identify and address areas affected by the modifications to the item and modifications between previous and future conditions of use of the item, including:

a) operational situations and operating modes;

b) interfaces with the environment;

c) installation characteristics such as location within the vehicle, vehicle configurations and variants; and

d) a range of environmental conditions e.g. temperature, altitude, humidity, vibrations, Electromagnetic Interference (EMI) and fuel types.

6.4.2.3 The implication of the modification with regard to functional safety shall be identified and described.

6.4.2.4 The affected work products that need to be updated shall be identified and described.

6.4.2.5 The safety activities shall be tailored in accordance with the applicable lifecycle phases.

6.4.2.6 Tailoring shall be based on the results of the impact analysis.

6.4.2.7 The results of tailoring shall be included in the safety plan in accordance with ISO 26262-2:2011, 6.4.3.

6.4.2.8 The affected work products shall be reworked.

NOTE The affected work products include the validation plan (see ISO 26262-4).

6.4.2.9 In the case of missing work products or work products that do not comply with ISO 26262, the necessary activities to reach ISO 26262 compliance shall be determined.

6.5 Work products

6.5.1 **Impact analysis** resulting from the requirements of 6.4.2.1 to 6.4.2.4.

6.5.2 **Safety plan (refined)** resulting from the requirements 6.4.2.5 to 6.4.2.9.

7 Hazard analysis and risk assessment

7.1 Objectives

The objective of the hazard analysis and risk assessment is to identify and to categorise the hazards that malfunctions in the item can trigger and to formulate the safety goals related to the prevention or mitigation of the hazardous events, in order to avoid unreasonable risk.

7.2 General

Hazard analysis, risk assessment and ASIL determination are used to determine the safety goals for the item such that an unreasonable risk is avoided. 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 the estimate of the impact factors, i.e. severity, probability of exposure and controllability. It is based on the item's functional behaviour; therefore, the detailed design of the item does not necessarily need to be known.

7.3 Inputs to this clause

7.3.1 Prerequisites

The following information shall be available:

— item definition in accordance with 5.5.

7.3.2 Further supporting information

The following information can be considered:

— impact analysis, if applicable (see 6.5.1); and

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

7.4 Requirements and recommendations

7.4.1 Initiation of the hazard analysis and risk assessment

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

7.4.1.2 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 providing increased control if it is shown to be available and sufficiently independent.

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.

7.4.2 Situation analysis and hazard identification

7.4.2.1 Situation analysis

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

NOTE The operational situation addresses the limits within which the item is expected to behave in a safe manner. For example, a normal passenger road vehicle is not expected to travel cross-country at high speed.

7.4.2.2 Hazard identification

7.4.2.2.1 The hazards shall be determined systematically by using adequate techniques.

NOTE Techniques such as brainstorming, checklists, quality history, FMEA and field studies can be used for the extraction of hazards at the item level.

7.4.2.2.2 Hazards shall be defined in terms of the conditions or behaviour that can be observed at the vehicle level.

NOTE 1 In general, each hazard will have a variety of potential causes related to the item's implementation but they do not need to be considered in the hazard analysis and risk assessment for the definition of the conditions or behaviour, which result from a functional behaviour of the item.

NOTE 2 Only hazards associated with the item itself can be considered, every other system (external measure) is presumed to be functioning correctly provided it is sufficiently independent.

7.4.2.2.3 The hazardous events shall be determined for relevant combinations of operational situations and hazards.

7.4.2.2.4 The consequences of hazardous events shall be identified.

NOTE If failures at an item level induce the loss of several functions of the item, then the situation analysis and hazard identification considers the resulting hazardous events from the combined malfunctional behaviour of the item or vehicle.

EXAMPLE Failure of the vehicle electrical power supply system can cause the simultaneous loss of a number of functions including “engine torque”, “power assisted steering” and “forward illumination”.

7.4.2.2.5 If there are hazards identified in 7.4.2.2 that are outside of the scope of ISO 26262 (see Clause 1), then the need for appropriate measures to mitigate or control these hazards shall be highlighted and reported to the responsible persons.

NOTE As these hazards are outside the scope of ISO 26262, hazard classification is not necessary.

7.4.3 Classification of hazardous events

7.4.3.1 All hazardous events identified in 7.4.2.3 shall be classified, except those that are outside the scope of ISO 26262.

NOTE If classification of a given hazard with respect to severity, probability of exposure or controllability is difficult to make, it is classified conservatively, i.e. whenever there is any doubt, a higher ASIL classification is given rather than a lower.

7.4.3.2 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. For informative examples of different types of severity and accidents see Annex B.

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

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

NOTE 4 The severity determination is based on a representative sample of individuals for the target markets.

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

7.4.3.3 The severity class S0 may be assigned if the hazard analysis determines that the consequences of a malfunctioning behaviour of the item are clearly limited to material damage and do not involve harm to persons. If a hazard is assigned to severity class S0, no ASIL assignment is required.

7.4.3.4 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 and 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 details 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

7.4.3.5 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.

7.4.3.6 Class E0 may be used for those situations that are suggested during hazard analysis and risk assessment, but which are considered to be extremely unusual, or incredible, and therefore not followed up. A rationale shall be recorded for the exclusion of these situations. If a hazard is assigned to exposure class E0, no ASIL assignment is required.

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

7.4.3.7 The controllability of each hazardous event, by the driver or other persons potentially at risk, 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 and 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 the driver or other persons potentially at risk are 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 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. he/she is not tired), has the appropriate driver training (he/she has a driver's licence) and is complying with all 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.4. Reasonably foreseeable misuse is considered.

NOTE 3 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.

NOTE 4 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 likely 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

7.4.3.8 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). Class C0 may also be assigned if dedicated regulations exist that specify the functional performance with respect to a defined hazard, and C0 is argued using the corresponding existing experience concerning sufficient controllability. If a hazard is assigned to the controllability class C0, no ASIL assignment is required.

EXAMPLE A dedicated regulation is the certification of a vehicle system with a precise definition of forces or acceleration values in the case of a failure.

7.4.4 Determination of ASIL and safety goals

7.4.4.1 An ASIL shall be determined for each hazardous event using the parameters "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.

Table 4 — ASIL determination

Severity class	**Probability 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
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

7.4.4.2 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 of the corresponding safety goals.

NOTE A very detailed list of operational situations (see 7.4.2.1.1) for one hazard, with regard to the vehicle state, road conditions and environmental conditions, can lead to a very granular 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 of the corresponding safety goals.

7.4.4.3 A safety goal shall be determined for each hazardous event with an ASIL evaluated in the hazard analysis. 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.

7.4.4.4 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 7.4.4.3, the highest ASIL shall be assigned to the combined safety goal.

NOTE If combined safety goals refer to the same hazard in different situations, then the resulting ASIL of the safety goal is the highest one of the considered safety goals of every situation.

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

NOTE Safe states are further elaborated in Clause 8.

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

7.4.4.6 The safety goals together with their attributes (ASIL) shall be specified in accordance with ISO 26262-8:2011, Clause 6.

NOTE The safety goal can include features such as 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.

7.4.5 Verification

7.4.5.1 The hazard analysis, risk assessment and the safety goals shall be verified in accordance with ISO 26262-8:2011, Clause 9, to show their:

a) completeness with regard to situations (7.4.2.1) and hazards (7.4.2.2);

b) compliance with the item definition;

c) consistency with related hazard analyses and risk assessments;

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

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

NOTE This verification review checks the hazard analysis and risk assessment of the item for correctness and completeness, i.e. considered situations, hazards and parameter estimations (severity, probability of exposure and controllability). In contrast, the confirmation review of the hazard analysis and risk assessment in accordance with ISO 26262-2, checks formally that the hazard analysis and risk assessment procedure complies with the requirements of Clause 7. The confirmation review is performed by a person or persons from a different department or organisation, than the developers of the item.

7.5 Work products

7.5.1 Hazard analysis and risk assessment resulting from the requirements of 7.4.1.1 to 7.4.4.2

7.5.2 Safety goals resulting from the requirements of 7.4.4.3 to 7.4.4.6

7.5.3 Verification review report of the hazard analysis and risk assessment and the safety goals resulting from the requirement of 7.4.5.

8 Functional safety concept

8.1 Objectives

The objective of the functional safety concept is to derive the functional safety requirements, from the safety goals, and to allocate them to the preliminary architectural elements of the item, or to external measures.

8.2 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.

The functional safety concept addresses:

— fault detection and failure mitigation;

— transitioning to a safe state;

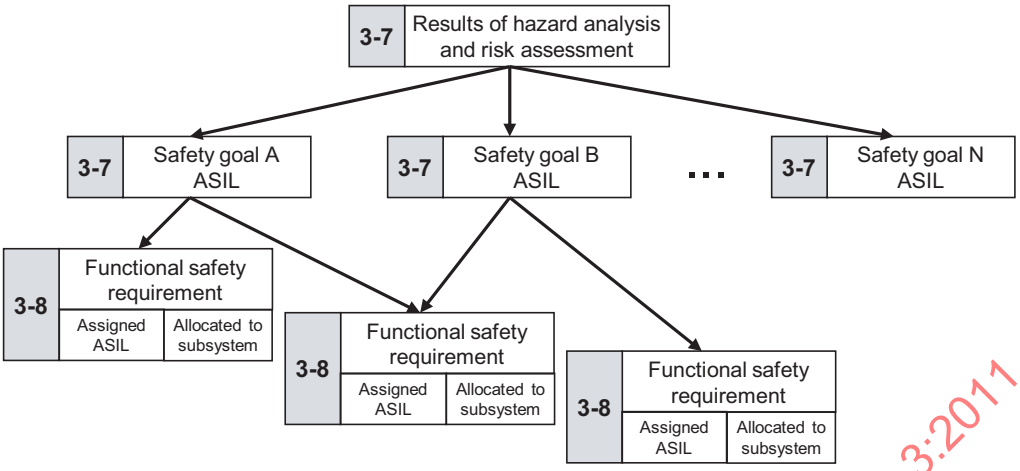
— fault tolerance mechanisms, where a fault does not lead directly to the violation of the safety goal(s) and which maintains the item in a safe state (with or without degradation);

— fault detection and driver warning in order to reduce the risk exposure time to an acceptable interval (e.g. engine malfunction indicator lamp, ABS fault warning lamp); and

— arbitration logic to select the most appropriate control request from multiple requests generated simultaneously by different functions.

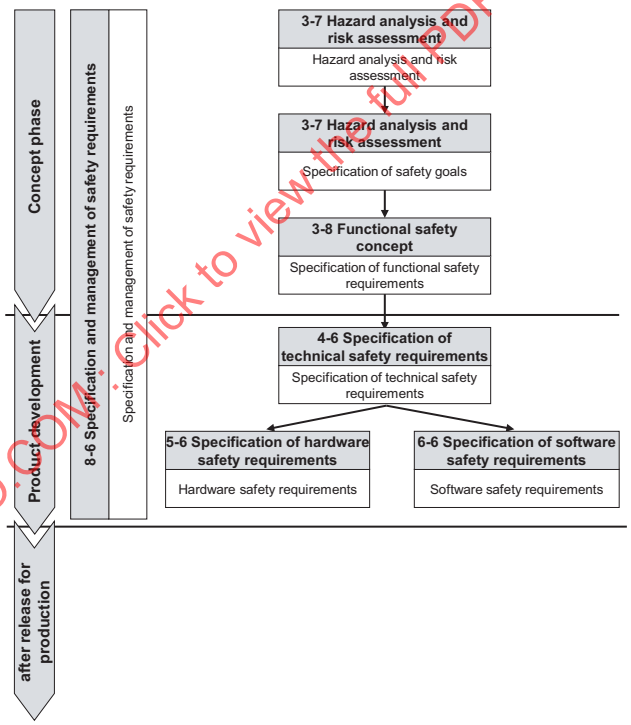
Figure 2 illustrates the hierarchical approach by which the safety goals are determined as a result of the hazard analysis and risk assessment. The functional safety requirements are then derived from the safety goals.

The structure and distribution of the safety requirements within the corresponding Parts of ISO 26262 are illustrated in Figure 3. The functional safety requirements are allocated to the elements of the preliminary architecture.



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 Clause 6 of ISO 26262-3.

Figure 2 — Hierarchy of safety goals and functional safety requirements



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 Clause 6 of ISO 26262-3.

Figure 3 — Structure of the safety requirements

8.3 Inputs to this clause

8.3.1 Prerequisites

The following information shall be available:

— item definition in accordance with 5.5;

— hazard analysis and risk assessment in accordance with 7.5.1; and

— safety goals in accordance with 7.5.2.

8.3.2 Further supporting information

The following information can be considered:

— preliminary architectural assumptions (from external source).

8.4 Requirements and recommendations

8.4.1 General

The functional safety requirements shall be specified in accordance with ISO 26262-8:2011, Clause 6.

8.4.2 Derivation of functional safety requirements

8.4.2.1 The functional safety requirements shall be derived from the safety goals and safe states, taking into account the preliminary architectural assumptions.

8.4.2.2 At least one functional safety requirement shall be specified for each safety goal.

NOTE One functional safety requirement can be valid for several safety goals.

8.4.2.3 Each functional safety requirement shall be specified by considering the following, if applicable:

a) operating modes;

b) fault tolerant time interval;

c) safe states;

d) emergency operation 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.

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

EXAMPLE When a safe state cannot be reached by immediately switching off a system, a suitable emergency operation needs to be specified.

8.4.2.5 The warning and degradation concept shall be specified as functional safety requirements.

NOTE The transitions to and from a safe state and the conditions for transitioning (switching to the safe state and recovering from the safe state) are described in the warning and degradation concept.

EXAMPLE 1 Fault detection and failure mitigation by switching to a safe state.

EXAMPLE 2 Fault detection and driver warning in order to reduce the risk exposure time to an acceptable interval (e.g. engine malfunction indicator lamp, ABS fault warning lamp).

8.4.2.6 If assumptions are made about the necessary actions of the driver, or other persons potentially at risk, in order to comply with the safety goals, 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 ACC: the override of brake activation by the driver pushing 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 potentially at risk shall be specified in the functional safety concept.

NOTE 1 Driver task analysis can be helpful to consider prevention of driver overload, prevention of driver surprise/panic/shock (loss of capability to control vehicle), and mode confusion (an incorrect assumption about the operating mode).

NOTE 2 The specification of the warning and degradation concept and the necessary actions of the driver and other persons potentially at risk is an input for the user manual (see ISO 26262-7:2011, 6.4.1).

8.4.3 Allocation of functional safety requirements

8.4.3.1 The functional safety requirements shall be allocated to the elements of the preliminary architectural assumptions:

NOTE Redundancy and independence issues can be checked by an analysis of dependent failures (see ISO 26262-9:2011, Clause 7).

a) During the course of allocation, the ASIL and information given in 8.4.2.3 shall be inherited from the associated safety goal or, if ASIL decomposition is applied, from the level above.

b) If several functional safety requirements are allocated to the same architectural element, then the architectural element shall be developed in accordance with the highest ASIL for those safety requirements if independence or freedom from interference cannot be argued in the preliminary architecture.

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

d) If ASIL decomposition is applied during the allocation of the functional safety requirements, then it shall be applied in accordance with ISO 26262-9:2011, Clause 5.

8.4.3.2 If the functional safety concept is to rely 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.

d) No ASIL should be assigned to these elements.

NOTE The adequacy of elements of other technologies is shown during validation activities (see ISO 26262-4).

8.4.3.3 If the functional safety concept is to rely 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.

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

d) The implementation of functional safety requirements by external measures shall be ensured.

NOTE The adequacy of external measures is shown during validation activities (see ISO 26262-4).

8.4.4 Validation criteria

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

NOTE For further requirements on detailing the criteria and a list of characteristics to be validated, see ISO 26262-4:2011, 6.4.6.2 and 9.4.3.2.

8.4.5 Verification of the functional safety concept

8.4.5.1 The functional safety concept shall be verified in accordance with ISO 26262-8:2011, Clause 9, to show

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

b) its ability to mitigate or avoid the hazardous events.

NOTE 1 The verification of the ability to mitigate or avoid a hazardous event during concept phase can be based on the same methods that are used for validation. The results of the evaluation can give an indication for concept improvements. However, it has to be kept in mind that the basis for safety validation in ISO 26262-4:2011, Clause 9, is an item developed according to ISO 26262 and safety validation cannot be based on concept studies (e.g. prototypes).

EXAMPLE The ability to mitigate or to avoid a hazardous event 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 hazardous event 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. if the item complies with the functional safety requirements, then the item complies with the safety goals as a result of this requirement.

8.5 Work products

8.5.1 **Functional safety concept** resulting from the requirements of 8.4.1 to 8.4.4.

8.5.2 **Verification report of the functional safety concept** resulting from the requirements of 8.4.5.

Annex A
(informative)

Overview and document flow 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 first objective is to define and describe the item, its dependencies on and interaction with the environment and other items. The second objective is to support an adequate understanding of the item so that the activities in subsequent phases can be performed.	None	5.5 Item definition
6 Initiation of the safety lifecycle	The first objective of the initiation of the safety lifecycle is to make the distinction between a new item development and a modification to a existing item (see ISO 26262-2:2011, Figure 2) The second objective is to define the safety lifecycle activities (see ISO 26262-2:2011, Figure 2) that will be carried out in the case of a modification.	Item definition	6.5.1 Impact analysis 6.5.2 Safety plan (refined)
7 Hazard analysis and risk assessment	The objective of the hazard analysis and risk assessment is to identify and to categorise the hazards that malfunctions in the item can trigger and to formulate the safety goals related to the prevention or mitigation of the hazardous events, in order to avoid unreasonable risk.	Item definition	7.5.1 Hazard analysis and risk assessment 7.5.2 Safety goals 7.5.3 Verification review report of the hazard analysis and risk assessment and the safety goals
8 Functional safety concept	The objective of the functional safety concept is to derive the functional safety requirements, from the safety goals, and to allocate them to the preliminary architectural elements of the item, or to external measures.	Item definition Hazard analysis and risk assessment Safety goals	8.5.1 Functional safety concept 8.5.2 Verification report of the functional safety concept

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 Clauses 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), with the frequency of occurrence (f) of a hazardous event, the ability to avoid specific harm or damage through timely reactions of the persons involved, that is the controllability (C) and the potential severity (S) of the resulting harm or damage:

$$R = F(f,C,S)$$

The frequency of occurrence f is, in turn, influenced by several 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 driving scenario taking place in which the hazardous event can occur (exposure, E). Another factor is the failure rate of the item that could lead to the hazardous event (failure rate, λ). The failure rate is characterised by hazardous hardware random failures and systematic faults that remained in the system:

$$f = E \times \lambda$$

Hazard analysis and risk assessment is concerned with setting requirements for the item such that unreasonable risk is avoided.

The ASILs that result from the 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 subphase comprises three steps, as described below.

a) Situation analysis and hazard identification (see 7.4.2): 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; and

   — interaction between operational systems.

b) Classification of hazardous events (see 7.4.3): 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 7.4.4): determining the required automotive safety integrity level.

B.2 Examples of severity

B.2.1 General

The potential injuries as a result of a hazard are evaluated for the driver, passengers and people around the vehicle, or to individuals 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.

Because of 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 [2], [4], [5]).

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). (See Reference [2]). 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;