DRAFT INTERNATIONAL STANDARD ISO/DIS 26262-3

ISO/TC **22**/SC **3** Secretariat: **DIN**

Voting begins on: **2009-07-08** Voting terminates on: **2009-12-08**

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION

Road vehicles — Functional safety —

Part 3: Concept phase

Véhicules routiers — Sécurité fonctionnelle —

Partie 3: Phase de conception

ICS 43.040.10

In accordance with the provisions of Council Resolution 15/1993 this document is circulated in the English language only.

Conformément aux dispositions de la Résolution du Conseil 15/1993, ce document est distribué en version anglaise seulement.

To expedite distribution, this document is circulated as received from the committee secretariat. ISO Central Secretariat work of editing and text composition will be undertaken at publication stage.

Pour accélérer la distribution, le présent document est distribué tel qu'il est parvenu du secrétariat du comité. Le travail de rédaction et de composition de texte sera effectué au Secrétariat central de l'ISO au stade de publication.

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: system level*

— *Part 5: Product development: hardware level*

— *Part 6: Product development: software level*

— *Part 7: Production and operation*

— *Part 8: Supporting processes*

— *Part 9: 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 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 elements that provide safety-related functions.

Safety is one of the key issues of future automobile development. New functionality not only in the area of driver assistance but also in vehicle dynamics control and active and passive safety systems increasingly touches the domain of safety engineering. Future development and integration of these functionalities will even strengthen the need of safe system development processes and the possibility to provide evidence that all reasonable safety objectives are satisfied.

With the trend of increasing 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 feasible requirements and processes.

System safety is achieved through a number of safety measures, which are implemented in a variety of technologies (for example: mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic etc). Although ISO 26262 is concerned with E/E systems, it provides a framework within which safety-related systems based on other technologies can be considered.

ISO 26262:

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

— provides an automotive specific risk-based approach for determining risk classes (Automotive Safety Integrity Levels, ASILs);

— uses ASILs for specifying the item's necessary safety requirements for achieving an acceptable residual risk; and

— provides requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety being achieved.

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 the development activities and work products.

Figure 1 shows the overall structure of ISO 26262. ISO 26262 is based upon a V-Model as a reference process model for the different phases of product development. The shaded "V"s represents the relations between ISO 26262-3, ISO 26262-4, ISO 26262-5, ISO 26262-6 and ISO 26262-7.

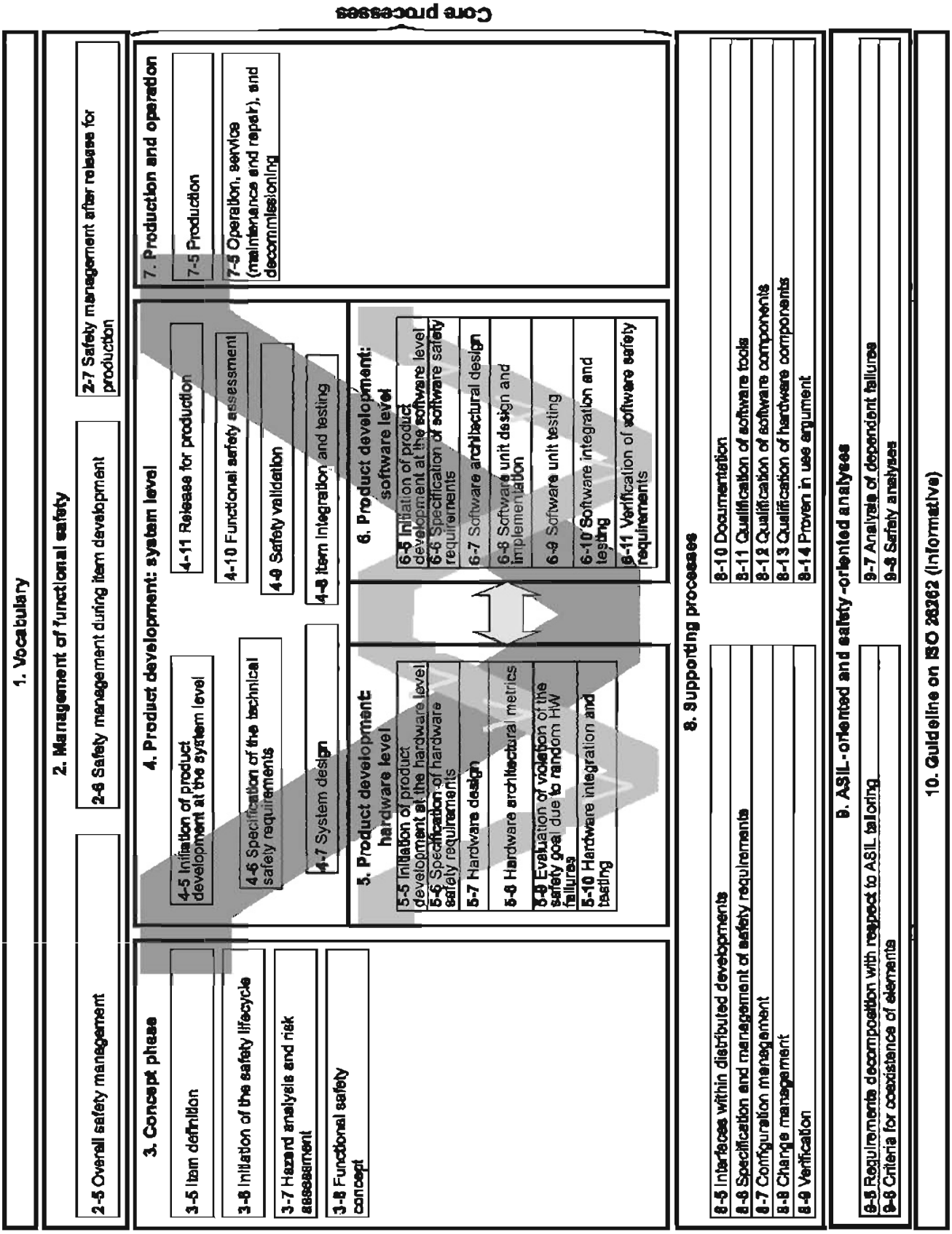

Figure 1 — Overview of ISO 26262

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 E/E systems and that are installed in series production passenger cars with a max gross weight up to 3.5 t. ISO 26262 does not address unique E/E systems in special purpose vehicles such as vehicles designed for drivers with disabilities. Systems developed prior to the publication date of ISO 26262 are exempted from the scope.

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 as 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 (for example active and passive safety systems, brake systems, ACC).

This part of the International Standard specifies the requirements on the concept phase for automotive applications. These requirements include the item definition, the initiation of the safety lifecycle, the hazard analysis and risk assessment and the 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: —[1] *Road vehicles – Functional Safety — Part 1: Vocabulary*

ISO 26262-2: —[1] *Road vehicles – Functional Safety — Part 2: Management of functional safety*

ISO 26262-8: —[1] *Road vehicles – Functional Safety — Part 8: Supporting processes*

ISO 26262-9: —[1] *Road vehicles – Functional Safety — Part 9: ASIL-oriented and safety-oriented analyses*

3 Terms, definitions, abbreviated terms

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

[1] To be published

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:

1) Tailoring in accordance with ISO 26262-2 has been planned and shows that the requirement does not apply.

2) 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" is only for guidance in understanding, or for clarification of, the associated requirement and shall not be interpreted as a requirement itself.

4.2 Interpretations of tables

Tables may be normative or informative depending on their context.

The different methods listed in a table contribute to the level of confidence that the corresponding requirement shall apply.

Each method in a table is either a consecutive entry (marked by a sequence number in the leftmost column, e.g. 1, 2, 3) or an alternative entry (marked by a number followed by a letter in leftmost column, e.g., 2a, 2b, 2c).

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

For alternative entries an appropriate combination of methods shall be applied in accordance with the ASIL, independently of whether they are listed in the table or not. If methods are listed with different degrees of recommendation for an ASIL the higher one should be preferred. A rationale shall be given that the selected combination of methods complies with the corresponding requirement. If all highly recommended methods listed for a particular ASIL are selected a rationale needs not to be given.

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

”++” The method is highly recommended for this ASIL.

“+“ The method is recommended for this ASIL.

“o“ The method has no recommendation for or against its usage for this ASIL.

4.3 ASIL dependent requirements and recommendations

The requirements or recommendations of each subclause shall apply to 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—: Clause 5 the ASIL resulting from the decomposition will apply.

If an ASIL is given in parentheses, the corresponding subclause shall be read as a recommendation rather than a requirement for this ASIL.

5 Item definition

5.1 Objectives

The first objective of the item definition is to define and describe the item.

The second objective is to support an adequate understanding of the item so that each activity defined in the safety lifecycle can be performed.

5.2 General

Clause 5 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).

5.3 Inputs to this clause

5.3.1 Prerequisites

The following information shall be available:

None

5.3.2 Further supporting information

The following information may 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 systems etc.

5.4 Requirements and recommendations

5.4.1 The functional requirements of the item as well as the dependencies between the item and its environment shall be available. This information includes:

a) The purpose and functionality of the item;

b) Non-functional requirements if available, e.g. operational and environmental requirements and constraints;

c) Legal requirements (especially laws and regulations), national and international standards, if already known.

5.4.2 Already known safety requirements for the item shall be available, based on:

a) Behaviour achieved by similar functions, systems or elements, if any;

b) Assumptions on behaviour expected from the item; and

c) Potential consequences of behaviour shortfalls including known failure modes and hazards.

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

5.4.3 It shall be ensured that the boundary of the item and the item's interfaces, as well as assumptions concerning other items and elements, are determined by considering:

a) The elements of the item;

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

c) Requirements received from other items, elements and the environment;

d) Requirements on other items, elements and the environment;

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

f) Operating scenarios of the item if they impact the functionality of the item

5.5 Work products

Item definition as a result of requirements 5.4.1, 5.4.2 and 5.4.3.

6 Initiation of the safety lifecycle

6.1 Objectives

The objective of the initiation of the safety lifecycle is to make the distinction between a new development and a modification to a previously existing item.

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

6.2 General

Based on the item definition, the safety lifecycle is initiated by distinguishing between either a new development or a modification, and 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 (see 5.5)

6.3.2 Further supporting information

The following information may 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

It shall be determined whether the item is a new development, or if it is a modification of an existing item with already existing work products in accordance with ISO 26262, or if it is a modification of an existing item with already existing work products.

a) In the case of a new development, the entire safety lifecycle (see ISO 26262-2: —, 5.2) shall be applied.

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

c) In the case of the reuse of already existing systems or elements, activities of ISO 26262 may be tailored, providing that the applicable work products are available and comply with the requirements for the corresponding work products of ISO 26262.

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

6.4.2.1 An analysis shall be carried out in order to identify the intended modification applied to the item and 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, functional or performance enhancement or cost optimisation. Implementation modifications do not affect specification or performances of the item, but only implementation features. Implementation modifications can result from software fault corrections, 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 behaviour of the item.

NOTE 3 Changes 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 This analysis shall address changes 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 such as temperature, altitude, humidity, vibrations, EMC and gasoline classes.

6.4.2.3 In the case of modifications to the item, the modifications shall be described and the areas affected by the modifications to the item shall be identified.

6.4.2.4 In the case of changes to the environment of the item, the changes to the environment shall be described.

6.4.2.5 In the absence of modifications to the item itself and of changes to its environment, the results of the impact analysis shall be recorded.

6.4.2.6 The implication of the modification on functional safety shall be described.

6.4.2.7 The affected work products that need to be updated shall be identified.

6.4.2.8 The results of the impact analysis shall be recorded.

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

a) Tailoring shall be based on the results of the impact analysis.

b) The results of tailoring shall be included in the safety plan in accordance with ISO 26262-2: —, 6.4.3.1 and ISO 26262-2: —, 6.4.3.4.

c) The affected work products shall be reworked.

NOTE The affected work products include the confirmation plan and validation plan

6.5 Work products

Impact analysis as a result of requirements 6.4.2.1 to 6.4.2.8.

7 Hazard analysis and risk assessment

7.1 Objectives

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

7.2 General

Hazard analysis, risk assessment and ASIL determination are concerned with determining safety goals for the item such that an unreasonable risk is avoided. For this, the item is evaluated with regard to its functional safety. Safety goals and their assigned Automotive Safety Integrity Level (ASIL) are determined by a systematic evaluation of hazardous situations. The rationale of the ASIL determination considers the estimation of the impact factors, that is, 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.

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

7.3 Inputs to this clause

7.3.1 Prerequisites

The following information shall be available:

Item definition (see 5.5)

7.3.2 Further supporting information

The following information may be considered:

None

7.4 Requirements and recommendations

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

7.4.2 The hazard analysis, risk assessment, determination of safety goals and their respective ASIL shall be conducted in accordance with the requirements in 7.4.

7.4.3 The item without a safety mechanism 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 systems shall not be considered as a means for providing risk reduction).

NOTE 1 In the evaluation of an item, there can be benefits from other items such as airbags, if those items are sufficiently independent.

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

7.4.4 Situation analysis and hazard identification

7.4.4.1 The operational situations and operating modes in which an item's malfunctioning behaviour is able to trigger hazards shall be described; both for cases when the item 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.

7.4.4.2 A list of operational situations to be evaluated shall be prepared.

7.4.4.3 The hazards of the item shall be determined systematically.

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

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

NOTE In general, each hazard will have a variety of potential causes (e.g. sensor failures).

7.4.4.5 The consequences of hazardous events shall be identified for relevant operational situations and operating modes.

NOTE If a fault induces the loss of several functions of the item then the situation analysis and hazard identification considers the resulting hazards from the multifunctional degradation of the item or vehicle. For instance, a fault in the vehicle power supply may cause the simultaneous loss of the functions "engine torque", "electrical power steering" and the "front lights".

7.4.4.6 If hazards are identified in the course of hazard identification, which are outside of the scope of ISO 26262 (see Clause 1), then the need for appropriate measures shall be indicated.

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

EXAMPLE Hazards due to misuse while the item works without malfunction.

7.4.5 Hazard classification

7.4.5.1 All hazards identified in 7.4.4 during the previous stage shall be classified, except for 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 unclear or in doubt, it is classified conservatively.

7.4.5.2 Estimation of potential severity

7.4.5.2.1 The severity of potential harm shall be estimated 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 endangered person – including the driver or the passengers of the vehicle causing the hazardous event, and other endangered persons such as cyclists, pedestrians or occupants of other vehicles. The description of the AIS (Abbreviated Injury Scale) 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 S than would result from just looking at single injuries.

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

7.4.5.2.2 The severity class S0 may be assigned if the hazard analysis determines that the consequences of an unintended 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.

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

7.4.5.3 Estimation of the probability of exposure in the operational situations

7.4.5.3.1 The probability of exposure of each operational situation shall be estimated. 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 The difference in probability from one E classification to the next is an order of magnitude.

NOTE 2 The exposure value of E1 or E2 is selected only if a rational is available for their use, considering each target market for the vehicle.

NOTE 3 The exposure determination is based on a representative sample of customers for the target markets

NOTE 4 For details and examples related to the probability of exposure see Annex B

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

NOTE The hazard analysis and risk assessment is performed assuming all vehicles are 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.

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

EXAMPLE E0 may be used in case of force majeure risk.

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

7.4.5.4 Estimation of controllability

7.4.5.4.1 The controllability of each hazardous event, by the driver or other traffic participants, shall be estimated. The controllability shall be assigned to one of the controllability classes C0, C1, C2 and C3 in accordance with Table 3.

NOTE 1 The evaluation of possibilities of the avoidance of a specific harm, that is the controllability, is an estimation of the probability that the driver or other endangered persons are able to gain control of the hazardous event that is arising and are able to avoid the specific harm. For this purpose, the estimation 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 with respect to the general population (for example not exhausted), has the appropriate driver training (has a driver's license) and is complying with legal regulations. However, a reasonably foreseeable misuse is considered. The corresponding examples, which serve as an interpretation of these classes, are listed in Table B.4.

NOTE 2 Where the hazard 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 estimation 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 may not be familiar with the operation of the item.

Table 3 — Classes of controllability

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

7.4.5.4.2 Class C0 may be used for hazards addressing the unavailability of the item if it does not affect the safe operation of the vehicle (e.g. driver assisting system). Class C0 may also be assigned if dedicated regulations exist that specify the functional performance with respect to a defined hazard and this is argued using the corresponding existing experience. If a hazard is assigned to the controllability class C0, no ASIL assignment is required.

7.4.6 An ASIL shall be determined for each hazardous event using the estimation parameters severity (S), probability of exposure (E) and controllability (C) 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 in accordance with ISO 26262.

Table 4 — ASIL determination

		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

7.4.7 During hazard analysis and risk assessment, having established the list of operational situations and having estimated the values of the S, E and C parameters for each situation, 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 operating situations (see 7.4.4.2) for one hazard, with regard to the vehicle state, road conditions and environmental conditions, can lead to a very granular classification. This can make it easier to rate controllability C and severity S. 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.

7.4.8 A safety goal shall be determined for each hazardous event evaluated in the hazard analysis.

NOTE 1 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 hazard. Safety goals are not expressed in terms of technological solutions, but in terms of functional objectives.

a) The ASIL determined for the hazardous event shall be assigned to the corresponding safety goal.

b) If similar safety goals are determined, these can be combined into one safety goal.

c) If similar safety goals are combined into a single one, in accordance with b), the highest ASIL shall be assigned to the combined safety goal.

NOTE 2 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.

d) If this safety goal can be achieved by transitioning to a particular state, then for each safety goal, there shall be a requirement that specifies a safe state that achieves the safety goal.

EXAMPLE Safe states: switched off, locked, vehicle standstill, continued operation over a defined time.

e) The safety goals together with their attributes (ASIL, safe state, if applicable) shall be specified in accordance with ISO 26262-8: —, Clause 6.

7.4.9 The hazard analysis, risk assessment and the safety goals shall be reviewed: To show completeness with regard to situations and hazards, compliance with the item definition, and consistency with related hazard analyses and risk assessments.

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

7.5 Work products

7.5.1 Hazard analysis and risk assessment as a result of requirements 7.4.1 to 7.4.7.

7.5.2 Safety goals as a result of requirement 7.4.8.

7.5.3 Verification review of hazard analysis and risk assessment and safety goals as a result of requirement 7.4.9.

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 risk reduction measures in order to ensure the required functional safety.

8.2 General

To comply with the safety goals, the functional safety concept specifies the basic safety mechanisms and safety measures in the form of functional safety requirements. The functional safety requirements are allocated to elements in the system architecture.

To specify safety mechanisms the functional safety concept addresses the following:

— 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 goals and which maintains the system 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 (repair request, stop request); and

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

The structure and distribution of the safety requirements within the corresponding Parts of ISO 26262 are illustrated in Figure 2.

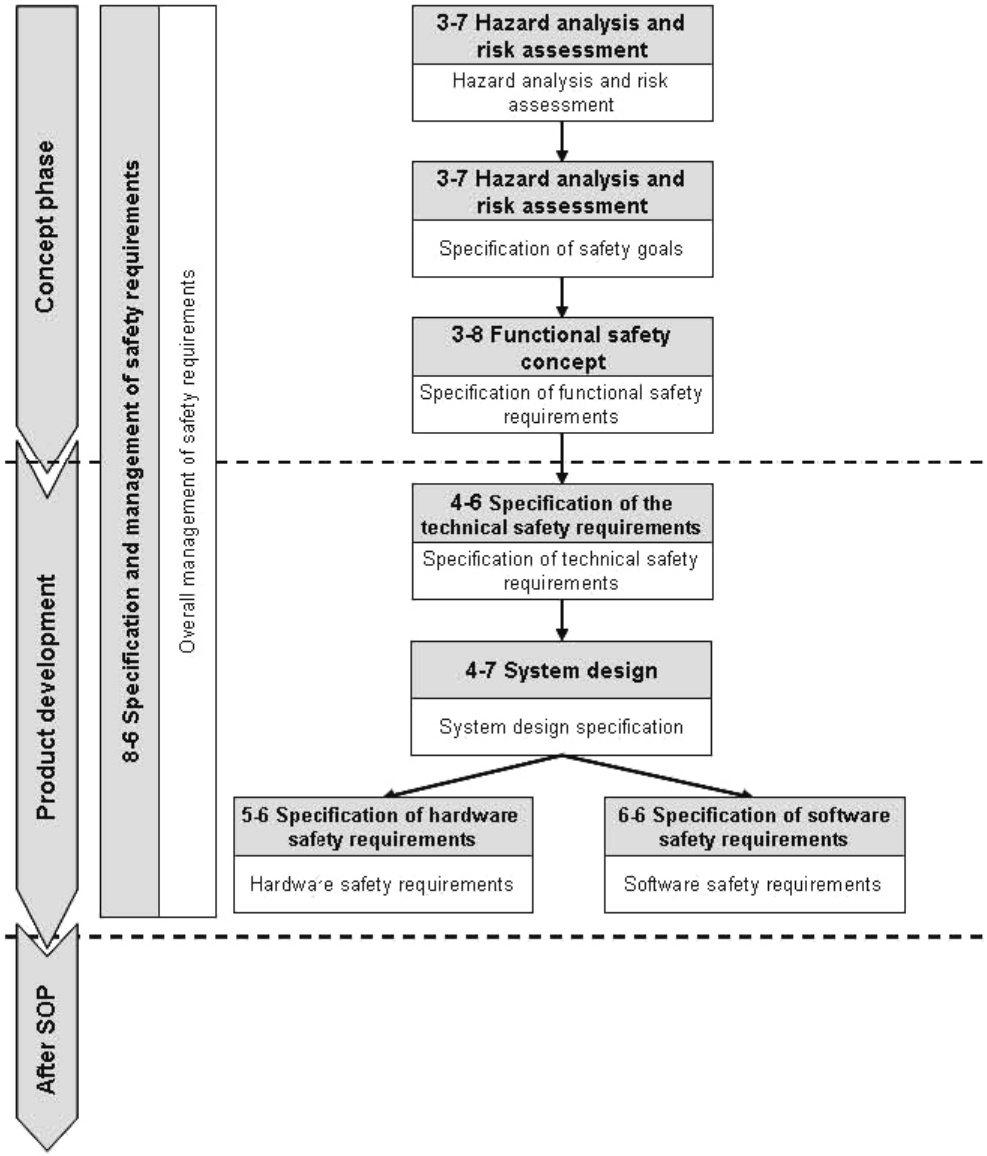

Figure 2 — Structure of the safety requirements

Figure 3 illustrates the hierarchical approach by which the safety goals are determined as results of the hazard analysis and risk assessment. In a second hierarchical step the functional safety requirements are derived from the safety goals.

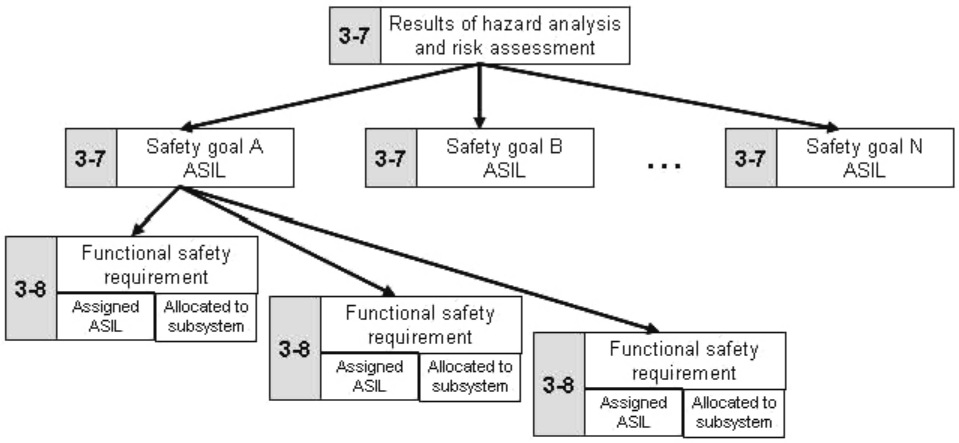

Figure 3 — Hierarchy of safety goals and functional safety requirements

8.3 Inputs to this clause

8.3.1 Prerequisites

The following information shall be available:

— Item definition (see 5.5)

— Hazard analysis and risk assessment (see 7.5.1)

— Safety goals (see 7.5.2)

8.3.2 Further supporting information

The following information may be considered:

— Preliminary architectural assumptions (from external source)

— Functional concept (from external source)

— Operating modes and system states (from external source)

8.4 Requirements and recommendations

8.4.1 General

The functional safety requirements shall be specified in accordance with the overall management of safety requirements (see ISO 26262-8: —, 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, considering the preliminary architectural assumptions, functional concept, operating modes and system states.

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 considering the following information, if applicable:

a) Operating modes;

b) Fault tolerant time interval;

c) Safe states, if transitioning to a safe state can comply with this requirement;

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) in order to develop a complete set of effective functional safety requirements.

8.4.2.4 The warning and degradation concept shall be specified.

NOTE The transitions to and from a safe state and the conditions for transitioning (conditions to switch to the safe state and recovery conditions from the safe state) are described in terms of technical functions.

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 (repair request, stop request)

8.4.2.5 If a safe state cannot be reached by immediately switching off, an emergency operation shall be specified.

8.4.2.6 If assumptions are made on the necessary actions of the driver, or other endangered persons, in order to comply with the safety goals:

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

b) The adequate means and controls of the driver or other endangered persons shall be specified in the functional safety concept;

NOTE 1 The actions include those for which credit was taken during the hazard analysis and risk assessment 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.

NOTE 2 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).

8.4.3 Allocation of functional safety requirements

8.4.3.1 A safety architecture concept shall be developed.

NOTE The safety architecture concept includes the redundancy and independence concept for the elements and can be given in block diagrams form. An analysis of dependent failures (see ISO 26262-9: —, Clause 7) can be useful to check independence concept.

8.4.3.2 The functional safety requirements shall be allocated:

a) The allocation of functional safety requirements shall be based on the elements of the preliminary architectural assumptions for the item.

b) In the course of allocation, the ASIL and the information given in 8.4.2.3 shall be inherited from the level above.

c) 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 requirements.

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

e) If ASIL decomposition is applied, it shall be applied in accordance with ISO 26262-9: —, Clause 5.

f) If safety requirements are allocated to elements of other technologies then no ASIL should be assigned to them.

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

a) The functional safety requirements implemented by other technologies shall be derived and allocated to the corresponding elements.

b) The functional safety requirements relating to the interfaces with other technologies shall be specified.

c) The implementation of functional safety requirements, by other technologies, shall be ensured through specific measures.

NOTE The adequacy of other technologies can be shown during validation activities.

8.4.3.4 If the functional safety concept relies on external risk reduction measures then the following shall apply:

a) The functional safety requirements applying to external risk reduction measures shall be derived and allocated to the corresponding external risk reduction measures.

b) The functional safety requirements of interfaces with external risk reduction measures shall be specified.

c) If the external risk reduction measures consist of E/E systems, the functional safety requirements shall be addressed using ISO 26262.

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

NOTE The adequacy of external risk reduction measures can be shown during validation activities.

8.4.4 The functional safety concept shall be verified in accordance with ISO 26262-8: —, Clause 9 for consistency and compliance with the safety goals.

NOTE For verification a traceability based argument can be used, that is, if the item complies with the functional safety requirements then the item complies with the safety goals as a result of this requirement.

8.4.5 The functional safety requirements should be evaluated to determine their effectiveness.

EXAMPLE The effectiveness can be evaluated by tests and trials; with prototypes, studies, subject tests, or simulations.

NOTE The evaluation of the effectiveness of a safety requirement addresses the behaviour of the fault, such as transient and permanent faults

8.4.6 The criteria for safety validation of the item shall be specified in the functional safety concept.

8.4.7 A review of the functional safety requirements shall provide a rationale that the functional safety requirements comply with the safety goals.

8.5 Work products

8.5.1 **Functional safety concept** as a result of requirements 8.4.2 to 8.4.6

8.5.2 **Review of the functional safety requirements** as a result of requirements 8.4.7

Annex A
(informative)

Overview on and document flow of concept phase

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

Table A.1 — Overview: Concept phase

Clause	Title	Objectives	Prerequisites	Work products
5	Item definition	The first objective of the item definition is to define and describe the item The second objective is to support an adequate understanding of the item so that each activity defined in the safety lifecycle can be performed.	None	5.5 Item definition
6	Initiation of the safety lifecycle	The objective of the initiation of the safety lifecycle is to make the distinction between a new development and a modification to a previously existing item. In the case of a modification the second objective is to define the safety lifecycle activities (see ISO 26262-2: —, Figure 2) that will be carried out.	Item definition	6.5 Impact analysis
7	Hazard analysis and risk assessment	The objective of the hazard analysis and risk assessment is to identify and categorise the hazards of the item and formulate the safety goals related to the prevention or mitigation of these hazards, 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 of hazard analysis and risk assessment and 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 risk reduction measures in order to ensure the required functional safety.	Item definition Hazard analysis and risk assessment Safety goals	8.5.1 Functional safety concept 8.5.2 Review of functional safety requirements

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 clause B.2 (severity), clause B.3 (probability of exposure), and clause B.4 (controllability) are for information only and are not exhaustive.

For the analytical approach, a risk (R = risk) can be described as a function F, with the frequency (f = frequency) of occurrence of a hazardous event, the ability of the avoidance of specific harm or damage through timely reactions of the persons involved (C = controllability), and the potential severity of the resulting harm or damage (S = severity):

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

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 (E = exposure).

— Another factor is the failure rate of the item that could lead to the hazardous event (λ = failure rate). This factor is characterised by undetected hardware random failures and by hazardous systematic faults that remained in the system.

$$f = E \times \lambda$$

Because development in accordance with ISO 26262 leads to safe systems, the resulting ASIL determines the minimum set of requirements for compliance by the item, in order to avoid random hardware failures and systematic faults. For this reason, λ of the item is not considered in the risk assessment.

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

The hazard analysis and risk assessment subphase comprises three steps:

a) Situation analysis and hazard identification (see 7.4.4): 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 may 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) Hazard classification (see 6.4.5): The hazard classification scheme comprises the determination of the severity (S), the exposure (E) and the controllability (C) associated with the considered hazard of the item. For a given hazard, this classification will result in one or more combinations of S, E, and C classes. As such, each combination represents an estimate of potential harm in a particular driving situation, with the severity determined by the potential harm and the exposure determined by the 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 situation.

c) ASIL determination (see 7.4.6): Determining the required automotive safety integrity level.

B.2 Examples of severity

B.2.1 General

Table B.1 gives examples for severity classes.

Table B.1 — Examples of severity classification

Class	S0	S1	S2	S3
Description	No injuries	light and moderate injuries	Severe injuries, possibly life-threatening, survival probable	Life-threatening injuries (survival uncertain) or fatal injuries
Reference for single injuries (from AIS scale)	AIS 0 Damage that cannot be classified safety-related, e.g. bumps with roadside infrastructure	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
Informative examples	-Pushing over roadside infrastructure, e.g. post or fence -Light collision -Light grazing damage -Damage while entering or leaving a parking space -Leaving the road without collision or rollover			
-Side collision, e.g. crashing into a tree (impact to passenger cell) 15 < Δv < 25 km/h		Δv <15km/h	15 < Δv <25 km/h	Δv >25 km/h
Side collision with a passenger car (impact to passenger cell)		Δv <15km/h	15< Δv <35 km/h	Δv >35 km/h
Rear/front collision between two passenger cars		Δv < 20km/h	20< Δv <40 km/h	Δv>40 km/h,
Other collisions		-Scrape collision with little vehicle to vehicle overlap (< 10%)		-Roof or side collision with considerable deformation
Under riding a truck		Without deformation of the passenger cell		With deformation of the passenger cell
Pedestrian/bicycle accident			E.g. during a turning manoeuvre inside built-up area	Outside built-up area

NOTE Δv defines the difference of speed at the moment of collision.

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 the effects of the accidents. 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 type 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 MAIS, ISS and NISS may 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 (Abbreviated Injury Scale), ISS (Injury Severity Score), and NISS (New Injury Severity Score), can vary over the time (see Bibliography [14], [15]).

B.2.2 Description of the AIS stages

To describe the severity, the AIS (Abbreviated Injury Scale) classification is used. The AIS represents a classification of the severity of injuries and is issued by AAAM (Association for the Advancement of Automotive Medicine, see Bibliography [13]). The guidelines were created to enable an international comparison of the 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.

B.3 Examples and explanations of the probability of exposure

Within the scope of ISO 26262 the driving or operating situations of vehicles range from everyday parking and driving in the city or on the highway, to extreme situations that require various environmental factors to occur together and therefore making the occurrence extremely seldom.

Apart from these situations, there are situations that are suggested during hazard and risk analysis, but that are considered to be so unusual, or incredible, that most vehicles will never experience the event within their lifetime and therefore are not followed up. For these situations the class E0 may be used.

Example: Typical examples of E0 include:

1) A very unusual co-occurrence of circumstances, e.g.

   — vehicle involved in an accident with another vehicle that is carrying a hazardous material. (note this does not apply to a vehicle which is designed to carry that material)

   — vehicle involved in an incident which includes an aeroplane landing on a highway.

2) Natural disasters, e.g. earthquake, hurricane, forest fire- Infeasible co-occurrence of circumstances, e.g.

   — vehicle involved in an accident with other vehicles carrying fissionable materials resulting in a nuclear explosion.

Table B.2 gives examples of situation classifications that may become hazardous if a failure will occur while the situation is present (temporal overlap).

In this case, the probability of exposure typically can be estimated by the proportion of total operating time (ignition on). In special cases the total operating time can be the vehicle life-time (including ignition off).

Some estimations of exposures can be determined more appropriately by using the frequency of occurrence from Table B.3. The examples in Table B.2 and B.3 might not lead to the same exposure category.

NOTE The examples of driving and operating situations given in tables B.2 and B.3 are strictly only for cars; when considering busses or trucks, the driving and operating situations can be different.

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

Class	E1	E2	E3	E4
Description	Very low probability	Low probability	Medium probability	High probability
Definition of duration/ probability of exposure	Not specified	< 1% of average operating time	1% - 10% of average operating time	> 10% of average operating time
Informative examples	Highway – lost cargo/obstacle on road Mountain pass – driving down hill with the engine off Jump start Garage – vehicle on roller rig	Pulling a trailer Driving with roof rack Driving on a mountain pass with an unsecured steep slope Snow and ice Driving backwards Fuelling Overtaking Car wash City driving – driving backwards City driving – parking situation Country road – crossing Country road – snow and ice Country road – slippery/leaves Highway – entering Highway – exit Highway – approaching end of congestion Parking – sleeping person in the vehicle Parking – parking with trailer Garage – diagnosis Garage – vehicle on auto lift	Tunnels Hill hold Night driving on roads without streetlights Wet roads Congestion City driving – one way street Highway – heavy traffic/stop and go	Accelerating Braking Steering Parking Driving on highways Driving on secondary roads City driving – changing lane City driving – stopping at traffic lights Country road – free driving Highway – free driving Highway – changing lane Parking – parking lot

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

Class	E1	E2	E3	E4
Description	Very low probability	Low probability	Medium probability	High probability
Definition of frequency	Situations that occur **less often than once a year** for the great majority of drivers	Situations that occur **a few times a year** for the great majority of drivers	Situations that occur **once a month or more often** for an average driver	All situations that occur during **almost every drive on average**
Informative examples	Stop at railway crossing, which requires the engine to be restarted Towing Jump start	Pulling a trailer, driving with a roof rack Driving on a mountain pass with an unsecured steep slope Driving situation with a deviation from the desired path Snow and ice	Fuelling Overtaking Tunnels Hill hold Car wash Wet roads Congestion	Starting Shifting gears Accelerating Braking Steering Using indicators Parking Driving backwards

If the time period, during which a particular failure may remain present is not much shorter than the mean time to the relevant situation, then the respective probability of exposure considers this interval. This typically concerns failures that might lead to the unavailability of crash prevention or mitigation systems, e.g. airbags.

— the relevant situation is one that might lead to harm when combined with the failure.

In this case the probability of exposure can be estimated by the product of σ * T (σ: Rate of occurrence of the situation; T: duration that the failure is not detected by the driver, possibly up to the lifetime of the vehicle). With regards to the duration of the considered failure, note that the hazard analysis and risk assessment does not consider safety mechanisms.

B.4 Examples of controllability (chances to avoid harm)

Table B.4 gives examples for controllability classes.

Table B.4 — Examples of possibly controllable hazards by the driver or by the endangered persons

Class	C0	C1	C2	C3
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable
Definition	Controllable in general	99% or more of all drivers or other traffic participants are usually able to avoid a specific harm.	90% or more of all drivers or other traffic participants are usually able to avoid a specific harm.	Less than 90% of all drivers or other traffic participants are usually able, or barely able, to avoid a specific harm.
Informative examples	Unexpected increase in radio volume Situations that are considered distracting Unavailability of a driver assisting system	When starting the vehicle with a locked steering column, the car can be brought to stop by almost all drivers early enough to avoid a specific harm to persons nearby. Faulty adjustment of seats while driving can be controlled by almost all drivers by bringing the vehicle to a stop.	Driver can normally avoid departing from the lane in case of a failure of ABS during emergency braking. Driver is normally able to avoid departing from the lane in case of a motor failure at high lateral acceleration (motorway exit). Driver is normally able to bring the vehicle to a stop in case of a total lighting failure at medium or high speed on an unlighted country road without departing from the lane in an uncontrolled manner. Driver is normally able to avoid hitting an unlit vehicle on an unlit country road.	Wrong steering with high angular speed at medium or high vehicle speed can hardly be controlled by the driver. Driver normally cannot avoid departing from the lane on snow or ice on a bend in case of a failure of ABS during emergency braking. Driver normally cannot bring the vehicle to a stop if a total loss of braking performance occurs. In the case of faulty airbag release at high or moderate vehicle speed, the driver usually cannot prevent vehicle from departing from the lane.

NOTE 1 For C2, a feasible test scenario in accordance with RESPONSE 3 (see Bibliography [12]) 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 an appropriate indication to provide a 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 huge number of test subjects would be necessary to provide a rationale for this.

NOTE 3 No evidence for category C3 is required, as no controllability is assumed.

Bibliography

[1] Council Directive 70/156/EEC of 6 February 1970 on the approximation of the laws of the Member States relating to the type-approval of motor vehicles and their trailers

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

[3] ISO/IEC Guide 51, Safety aspects - Guidelines for their inclusion in standards

[4] ISO/IEC 2382, Information technology -- Vocabulary

[5] IEC 60050(191), International Electrotechnical Vocabulary – Dependability and quality of service

[6] ISO/IEC 15026:1998, Information Technology - System and Software Integrity Levels

[7] Code of Practice for the design and evaluation of ADAS, EU Project RESPONSE 3: Oct. 2006

[8] Abbreviated injury scale; Association of the advancement of Automotive medicine; Barrington, IL, USA Information is also available at www.carcrash.org or www.unfallforensik.de/body_lexikon.html

[9] S.P. Baker, B. O'Neill, W. Haddon, W.B. Long, 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

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