INTERNATIONAL STANDARD

ISO 26262-12

First edition
2018-12

Road vehicles — Functional safety —

Part 12: Adaptation of ISO 26262 for motorcycles

Véhicules routiers — Sécurité fonctionnelle —

Partie 12: Adaptation de l'ISO 26262 pour les motocycles

Reference number
ISO 26262-12:2018(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee SC 32, *Electrical and electronic components and general system aspects*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

A list of all parts in the ISO 26262 series can be found on the ISO website.

Introduction

The ISO 26262 series of standards is the adaptation of IEC 61508 series of standards to address the sector specific needs of electrical and/or electronic (E/E) systems within road vehicles.

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

Safety is one of the key issues in the development of road vehicles. Development and integration of automotive functionalities strengthen the need for functional safety and the need to provide evidence that functional safety objectives are satisfied.

With the trend of increasing technological complexity, software content and mechatronic implementation, there are increasing risks from systematic failures and random hardware failures, these being considered within the scope of functional safety. ISO 26262 series of standards includes guidance to mitigate these risks by providing appropriate requirements and processes.

To achieve functional safety, the ISO 26262 series of standards:

a) provides a reference for the automotive safety lifecycle and supports the tailoring of the activities to be performed during the lifecycle phases, i.e., development, production, operation, service and decommissioning;

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

c) uses ASILs to specify which of the requirements of ISO 26262 are applicable to avoid unreasonable residual risk;

d) provides requirements for functional safety management, design, implementation, verification, validation and confirmation measures; and

e) provides requirements for relations between customers and suppliers.

The ISO 26262 series of standards is concerned with functional safety of E/E systems that is achieved through safety measures including safety mechanisms. It also provides a framework within which safety-related systems based on other technologies (e.g. mechanical, hydraulic and pneumatic) can be considered.

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

Safety is intertwined with common function-oriented and quality-oriented activities and work products. The ISO 26262 series of standards addresses the safety-related aspects of these activities and work products.

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

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

— for motorcycles:

  — ISO 26262-12:2018, Clause 8 supports ISO 26262-3;

  — ISO 26262-12:2018, Clauses 9 and 10 support ISO 26262-4;

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

EXAMPLE “2-6” represents ISO 26262-2:2018, Clause 6.

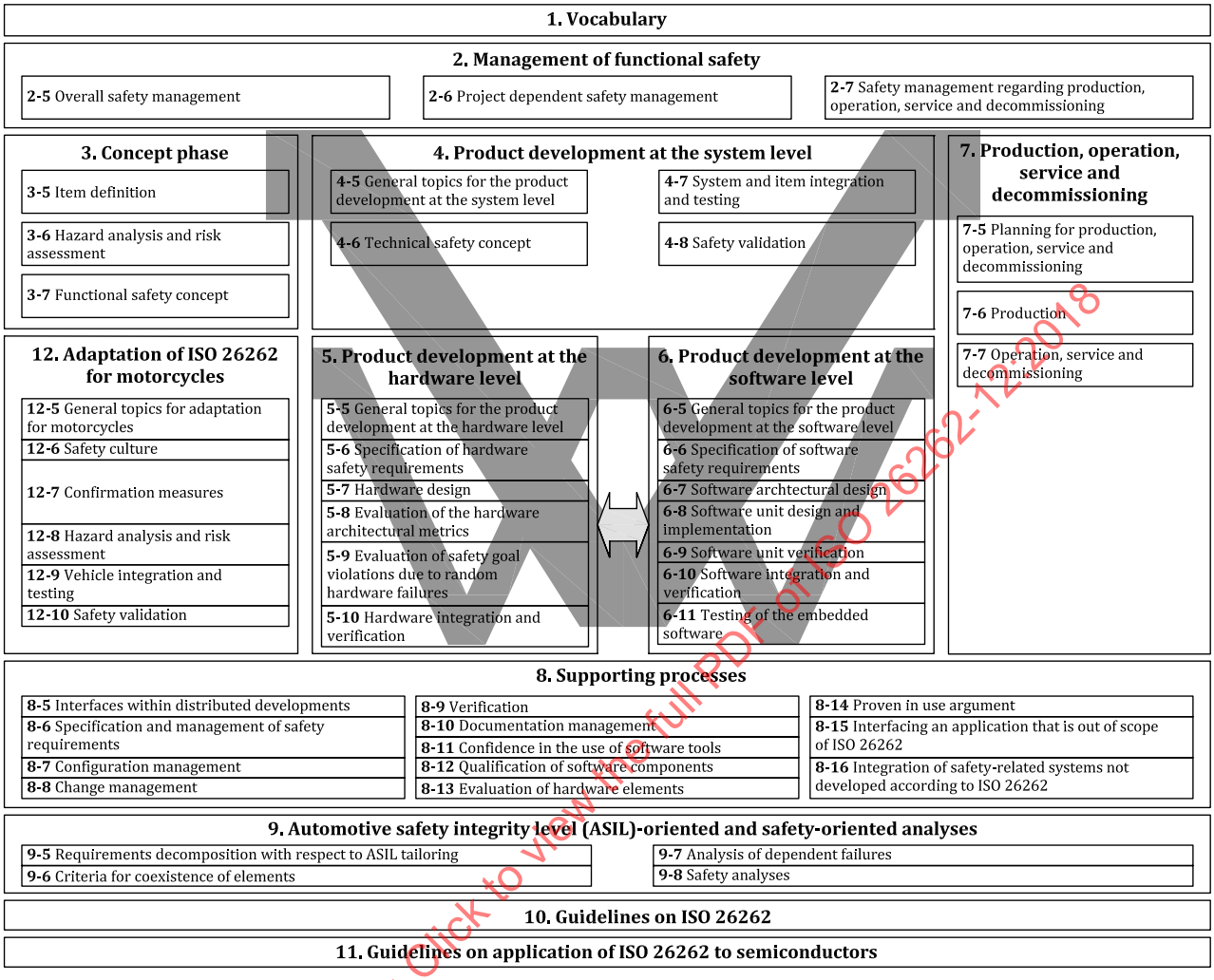

Figure 1 — Overview of the ISO 26262 series of standards

Road vehicles — Functional safety —

Part 12:
Adaptation of ISO 26262 for motorcycles

1 Scope

This document is intended to be applied to safety-related systems that include one or more electrical and/or electronic (E/E) systems and that are installed in series production road vehicles, excluding mopeds. This document does not address unique E/E systems in special vehicles such as E/E systems designed for drivers with disabilities.

NOTE Other dedicated application-specific safety standards exist and can complement the ISO 26262 series of standards or vice versa.

Systems and their components released for production, or systems and their components already under development prior to the publication date of this document, are exempted from the scope of this edition. This document addresses alterations to existing systems and their components released for production prior to the publication of this document by tailoring the safety lifecycle depending on the alteration. This document addresses integration of existing systems not developed according to this document and systems developed according to this document by tailoring the safety lifecycle.

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

This document describes a framework for functional safety to assist the development of safety-related E/E systems. This framework is intended to be used to integrate functional safety activities into a company-specific development framework. Some requirements have a clear technical focus to implement functional safety into a product; others address the development process and can therefore be seen as process requirements in order to demonstrate the capability of an organization with respect to functional safety.

This document does not address the nominal performance of E/E systems.

This document specifies the requirements for adaptation for motorcycles, including the following:

— general topics for adaptation for motorcycles;

— safety culture;

— confirmation measures;

— hazard analysis and risk assessment;

— vehicle integration and testing; and

— safety validation.

Annex A provides an overview on objectives, prerequisites and work products of this document.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

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

ISO 26262-3:2018, *Road vehicles — Functional safety — Part 3: Concept phase*

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

ISO 26262-5:2018, *Road vehicles — Functional safety — Part 5: Product development at the hardware level*

ISO 26262-6:2018, *Road vehicles — Functional safety — Part 6: Product development at the software level*

ISO 26262-7:2018, *Road vehicles — Functional safety — Part 7: Production, operation, service and decommissioning*

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

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

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at https://www.iso.org/obp

4 Requirements for compliance

4.1 Purpose

This clause describes how:

a) to achieve compliance with the ISO 26262 series of standards;

b) to interpret the tables used in the ISO 26262 series of standards; and

c) to interpret the applicability of each clause, depending on the relevant ASIL(s).

4.2 General requirements

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

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

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

Informative content, including notes and examples, is only for guidance in understanding, or for clarification of the associated requirement, and shall not be interpreted as a requirement itself or as complete or exhaustive.

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

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

4.3 Interpretations of tables

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

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

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

For consecutive entries, all listed highly recommended and recommended methods in accordance with the ASIL apply. It is allowed to substitute a highly recommended or recommended method by others not listed in the table, in this case, a rationale shall be given describing why these comply with the corresponding requirement. If a rationale can be given to comply with the corresponding requirement without choosing all entries, a further rationale for omitted methods is not necessary.

For alternative entries, an appropriate combination of methods shall be applied in accordance with the ASIL indicated, independent of whether they are listed in the table or not. If methods are listed with different degrees of recommendation for an ASIL, the methods with the higher recommendation should be preferred. A rationale shall be given that the selected combination of methods or even a selected single method complies with the corresponding requirement.

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

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

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

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

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

4.4 ASIL-dependent requirements and recommendations

The requirements or recommendations of each sub-clause shall be met for ASIL A, B, C and D, if not stated otherwise. These requirements and recommendations refer to the ASIL of the safety goal. If ASIL decomposition has been performed at an earlier stage of development, in accordance with ISO 26262-9:2018, Clause 5, the ASIL resulting from the decomposition shall be met.

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

4.5 Adaptation for motorcycles

For items or elements of motorcycles for which requirements of this document are applicable, the requirements of this document supersede the corresponding requirements in other parts.

4.6 Adaptation for trucks, buses, trailers and semi-trailers

Content that is intended to be unique for trucks, buses, trailers and semi-trailers (T&B) is indicated as such.

5 General topics for adaptation for motorcycles

5.1 Objectives

The objective of this clause is to give an overview of the adaptation of the ISO 26262 series of standards for motorcycles.

5.2 General

In order for E/E systems on motorcycles to comply with the ISO 26262 series of standards, all of the requirements of ISO 26262-2 through ISO 26262-9 shall be met. However, as described in 4.5, some requirements may require a degree of tailoring in order to apply to motorcycles. In such cases, these tailored requirements supersede the corresponding requirements of the ISO 26262 series of standards.

The specific requirements for motorcycles described in this document correspond to requirements of ISO 26262-2:2018, 5.4.2, requirements in ISO 26262-2:2018, 6.4.9, requirements in ISO 26262-3:2018, Clause 6, ISO 26262-3:2018, Annex B, requirements in ISO 26262-4:2018, 7.4.4, and requirement in ISO 26262-4:2018, Clause 8.

NOTE The following definitions and abbreviations are specific for motorcycles and are used in this document. These are described in ISO 26262-1:

— expert rider;

— motorcycle;

— Motorcycle Safety Integrity Level (MSIL); and

— Controllability Classification Panel (CCP).

Annex A provides the overview of and work flow for motorcycles to implement ISO 26262-2:2018, ISO 26262-3:2018 and ISO 26262-4:2018.

Annex B gives a general explanation of the hazard analysis and risk assessment.

Annex C provides examples of controllability evaluation techniques considering motorcycle dynamics in the context of conventional product development.

Figure 2 shows the relation of this document and the other parts of ISO 26262.

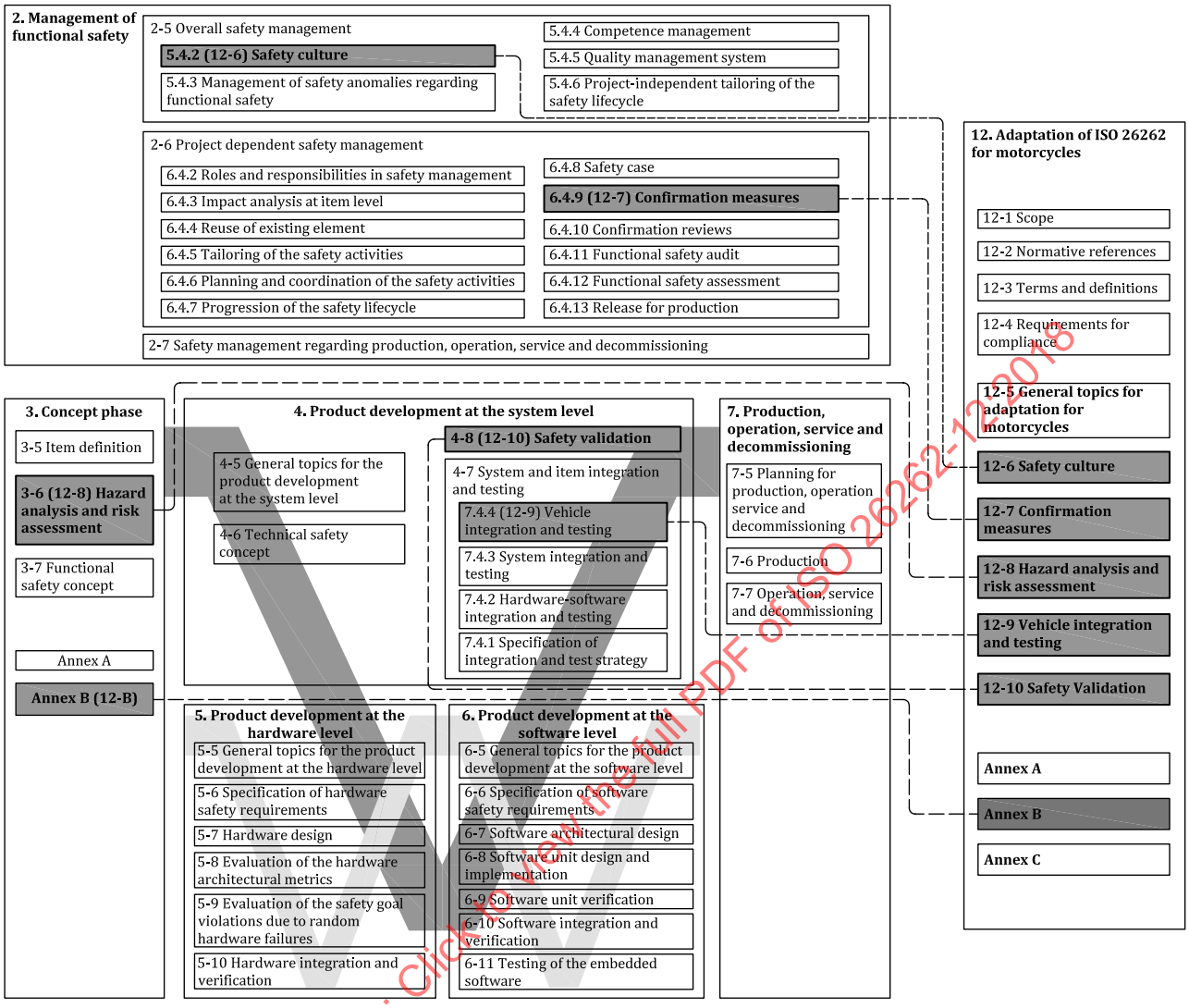

Figure 2 — Overview of this document and the relation to the other parts

6 Safety culture

6.1 Objective

To provide a tailoring of ISO 26262-2:2018, 5.4.2 for motorcycles.

6.2 Requirements and recommendations

6.2.1 The organization shall create, foster, and sustain a safety culture that supports and encourages the effective achievement of functional safety for motorcycles.

NOTE ISO 26262-2:2018, Annex B provides more details of what can constitute a safety culture.

6.2.2 The organization shall institute, execute and maintain organization-specific rules and processes to achieve and maintain functional safety and to comply with the requirements of the ISO 26262 series of standards.

NOTE Such organization-specific rules and processes can include the creation and maintenance of generic plans (e.g. a generic safety plan) or generic process descriptions.

6.2.3 The organization shall institute and maintain effective communication channels between functional safety, cybersecurity, and other potentially interacting disciplines that are related to the achievement of functional safety, if applicable.

EXAMPLE 1 Communication channels between functional safety and cybersecurity in order to exchange relevant information (e.g. in the case it is identified that a cybersecurity issue might violate a safety goal or a safety requirement, or in the case a cybersecurity requirement might compete with a safety requirement).

EXAMPLE 2 Communication channels between functional safety and quality.

NOTE Guidance on potential interaction of functional safety with cybersecurity is given in ISO 26262-2:2018, Annex E.

6.2.4 During the execution of the safety lifecycle, the organization shall perform the required safety activities, including the creation and management of the associated documentation in accordance with ISO 26262-8:2018, Clause 10.

6.2.5 The organization shall provide the resources required for the achievement of functional safety.

NOTE Resources include human resources, tools, databases, guidelines and work instructions.

6.2.6 The organization shall institute, execute and maintain a continuous improvement process, based on:

— learning from the experiences gained during the execution of the safety lifecycle of other items, including field experience; and

— derived improvements for application on subsequent items.

6.2.7 The organization shall ensure that the persons responsible for achieving or maintaining functional safety, or for performing or supporting the safety activities, are given sufficient authority to fulfil their responsibilities.

7 Confirmation measures

7.1 Objective

The objective of this clause is to define the independency requirements of confirmation measures associated with ASIL.

7.2 Requirements and recommendations

7.2.1 The functional safety of the item and its elements shall be confirmed, based on:

a) confirmation reviews to judge whether the key work products, i.e. those included in Table 1, provide sufficient and convincing evidence of their contribution to the achievement of functional safety, considering the corresponding objectives and requirements of the ISO 26262 series of standards, in accordance with Table 1 and ISO 26262-2:2018, 6.4.10;

NOTE 1 For motorcycles, Table 1 of this document replaces ISO 26262-2:2018, Table 1.

NOTE 2 The confirmation reviews are performed for those work products that are specified in Table 1 and required by the safety plan.

b) a functional safety audit to judge the implementation of the processes required for functional safety, in accordance with Table 1 and ISO 26262-2:2018, 6.4.11; and

NOTE 3 The reference processes required for functional safety are defined in the ISO 26262 series of standards. The processes pertaining to an item or element are defined through the activities referenced or specified in the safety plan.

c) a functional safety assessment to judge the achieved functional safety of the item, or the contribution to the achievement of functional safety by the developed elements, in accordance with Table 1 and ISO 26262-2:2018, 6.4.12.

NOTE 4 The aim of the independence defined in Table 1 is to ensure an objective, unbiased viewpoint and to avoid conflict of interest. The use of the term independence in this document relates to organizational independence.

NOTE 5 Guidance for the confirmation measure is given in ISO 26262-2:2018, Annex C.

NOTE 6 A report that is a result of a confirmation measure includes the name and revision number of the work products or process documents analysed (see ISO 26262-8:2018, Clause 10).

NOTE 7 If the item changes subsequent to the completion of confirmation measures, then the pertinent confirmation measures will be repeated or supplemented (see ISO 26262-8:2018, 8.4.5.2).

NOTE 8 Confirmation measures such as confirmation reviews and functional safety audits can be merged and combined with the functional safety assessment to support the handling of comparable variants of an item.

Table 1 — Required confirmation measures, including the required level of independence

Confirmation measures	Level of independence[a] applies to				Scope
	QM	ASIL A	ASIL B	ASIL C	
Confirmation review of the impact analysis at item level (see ISO 26262-2:2018, 6.5.1) Independence with regard to those creating the work product	I3	I3	I3	I3	Judgement of whether the impact analysis in accordance with ISO 26262-2:2018, 6.4.3 correctly identified the item as being a new item, a modification of an existing item or an existing item with a modified environment. Judgement of whether the impact analysis in accordance with ISO 26262-2:2018, 6.4.3 adequately identified the implications on functional safety caused by the modification(s); and the safety activities to be performed.
Confirmation review of the hazard analysis and risk assessment (see Clause 8) Independence with regard to those creating the work product	I3	I3	I3	I3	Judgement of whether the selection of the operational situations pertinent to the hazardous events and the definitions of the hazardous events are appropriate. Judgement of whether the determined ASILs, quality management ("QM") ratings of the identified hazardous events for the item and the parameters resulting in no ASIL e.g. C0/S0/E0 are correct. Judgement of whether the specified safety goals cover the identified hazardous events.
Confirmation review of the safety plan (see ISO 26262-2:2018, 6.5.3) Independence with regard to those creating the work product NOTE 1 A confirmation review of the safety plan includes a review of the impact analyses at element level performed due to the reuse of existing elements (see ISO 26262-2:2018, 6.5.2). NOTE 2 The safety plan includes the proven in use arguments (analysis, data and credit) of the proven in use candidates and the corresponding tailoring, if applicable (see ISO 26262-2:2018, 6.4.6 and ISO 26262-8:2018, Clause 14). NOTE 3 The safety plan includes tailoring due to the use of software tools, if applicable (see ISO 26262-2:2018, 6.4.6 and ISO 26262-8:2018, Clause 11).	—	I1	I1	I2	Applies to the highest ASIL among the safety requirements

Table 1 *(continued)*

Confirmation measures	Level of independence[a] applies to				Scope
	QM	ASIL A	ASIL B	ASIL C	
Confirmation review of the Functional Safety Concept (see ISO 26262-3:2018, Clause 7), supported by the results of the corresponding-safety analyses and dependent failure analyses (see ISO 26262-9:2018, Clause 8 and ISO 26262-9:2018, Clause 7, respectively) Independence with regard to those creating the work product	—	I1	I1	I2	Applies to the highest ASIL among the safety goals of the item
Confirmation review of the Technical Safety Concept (see ISO 26262-4:2018, Clause 6), supported by the results of the corresponding safety analyses and dependent failure analyses (see ISO 26262-9:2018, Clause 8 and ISO 26262-9:2018, Clause 7, respectively) Independence with regard to those creating the work product	—	I1	I1	I2	Applies to the highest ASIL among the functional safety requirements from which the technical safety requirements are derived. If ASIL decomposition has been applied to the functional safety concept then the resulting ASIL from the decomposition may be considered.
Confirmation review of the integration and test strategy (see ISO 26262-4:2018, Clause 7) Independence with regard to those creating the work product	—	I0	I1	I2	Applies to the highest ASIL among the safety requirements
Confirmation review of the safety validation specification (see ISO 26262-4:2018, Clause 8) Independence with regard to those creating the work product	—	I0	I1	I2	Applies to the highest ASIL among the safety requirements
Confirmation review of the safety analyses and the dependent failure analyses (see ISO 26262-9:2018, Clause 8 and ISO 26262- 9:2018, Clause 7, respectively) Independence with regard to those creating the work product	—	I1	I1	I2	Applies to the highest ASIL among the safety requirements
Confirmation review of the safety case (see ISO 26262-2:2018, 6.5.4) Independence with regard to the authors of the safety case	—	I1	I1	I2	Applies to the highest ASIL among the safety requirements

Table 1 *(continued)*

Confirmation measures	Level of independence[a] applies to				Scope
	QM	ASIL A	ASIL B	ASIL C	
Functional safety audit in accordance with ISO 26262-2:2018, 6.4.11 Independence with regard to the developers of the item and project management	—	—	I0	I2	Applies to the highest ASIL among the safety requirements
Functional safety assessment in accordance with ISO 26262-2:2018, 6.4.12 Independence with regard to the developers of the item and project management	—	—	I0	I2	Applies to the highest ASIL among the safety requirements

NOTE Figure 3 shows a simplified structure for a better understanding of independence. In different companies, the organizational units could be named differently.

[a] The indicated levels of independence are intended to represent minimum requirements. The notations are defined as follows:

— —: no requirement and no recommendation for or against regarding this confirmation measure;

— I0: the confirmation measure should be performed; however, if the confirmation measure is performed, it shall be performed by a different person in relation to the person(s) responsible for the creation of the considered work product(s);

— I1: the confirmation measure shall be performed, by a different person in relation to the person(s) responsible for the creation of the considered work product(s);

— I2: the confirmation measure shall be performed, by a person from a team that is different from that responsible for the creation of the considered work product(s), i.e. by a person not reporting to the same direct superior; and

— I3: the confirmation measure shall be performed, by a person from a different department or organization, i.e. not reporting to the same department leader responsible for the release of the work product(s).

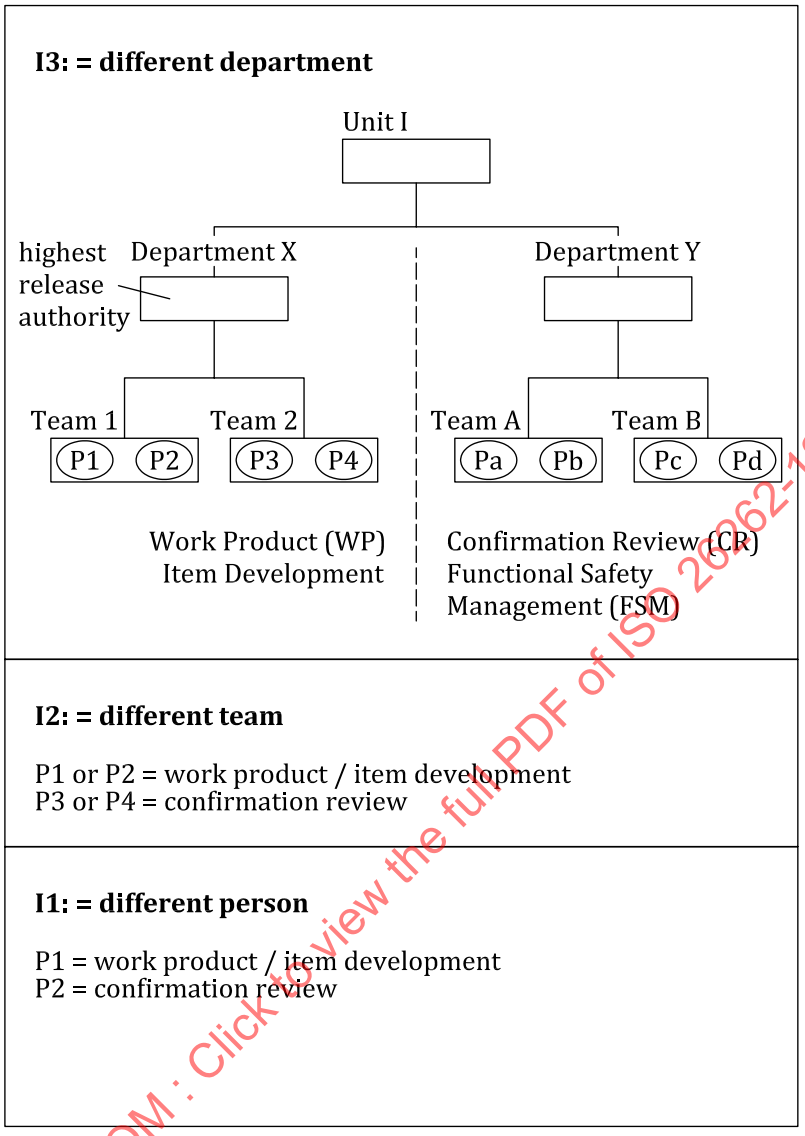

Figure 3 — Independence levels for confirmation reviews

7.2.2 The persons who carry out a confirmation measure shall have access to, and shall be supported by, the persons and organizational entities that carry out safety activities during the item development.

7.2.3 The persons who carry out a confirmation measure shall have access to the relevant information and tools.

8 Hazard analysis and risk assessment

8.1 Objectives

The objectives of this clause are:

a) to specify the necessary requirements that need to be complied with in order to perform a motorcycle specific hazard analysis and risk assessment;

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

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

8.2 General

Due to the fact that the dynamic behaviour of motorcycles differs greatly from that of other vehicles within the scope of the ISO 26262 series of standards, and that controllability of motorcycle specific hazardous events could place more emphasis on the rider, it is recognised that the method of performing risk assessment requires a degree of tailoring to best suit motorcycle specific hazardous events.

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

NOTE Product development processes and technical solutions within the motorcycle industry differ from those of the automobile industry. The worldwide established level of technology ("state-of-the-art") in the motorcycle industry suggests that ASIL classification is inappropriate for motorcycles. Therefore MSIL classification as the output of the HARA is used. An alignment between MSIL and ASIL classification is established to use requirements as defined in other parts of ISO 26262 and accommodate worldwide capability of the motorcycle industry.

8.3 Input to this clause

8.3.1 Prerequisites

The following information shall be available:

— item definition in accordance with ISO 26262-3:2018, 5.5.1.

8.3.2 Further supporting information

The following information can be considered:

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

8.4 Requirements and recommendations

8.4.1 Initiation of the hazard analysis and risk assessment

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

8.4.1.2 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.

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.

8.4.2 Situation analysis and hazard identification

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

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

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

EXAMPLE 1 A normal motorcycle is not expected to travel on unimproved or unpaved surfaces at high speed.

EXAMPLE 2 A normal motorcycle is not expected to be used for road race, motocross or trial events.

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

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

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

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

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

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

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

8.4.2.5 Relevant hazardous events shall be determined.

8.4.2.6 The consequences of hazardous events shall be identified.

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

EXAMPLE Failure of the vehicle's electrical power supply system can lead to a simultaneous loss of a number of functions including “engine torque” and “forward illumination”.

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

NOTE A very detailed list of operational situations (see 8.4.2.1) for one hazard, with regard to the vehicle state, road conditions and environmental conditions, can lead to a fine granularity of situations for the classification of hazardous events. This can make it easier to rate controllability and severity. However, a larger number of different operational situations can lead to a consequential reduction of the respective classes of exposure, and thus to an inappropriate lowering of the MSIL. This can be avoided by aggregating similar situations.

8.4.3 Classification of hazardous events

8.4.3.1 All hazardous events identified in 8.4.2 shall be classified, except those that are outside the scope of ISO 26262.

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

8.4.3.2 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 Table2.

NOTE 1 The risk assessment of hazardous events focuses on the harm to each person potentially at risk — including the rider or the passengers of the vehicle causing the hazardous event, and other persons potentially at risk such as cyclists, pedestrians or occupants of other vehicles. The description of the Abbreviated Injury Scale (AIS) can be used for characterising the severity and can be found in Annex B, along with informative examples of different types of severity and accidents. Where available, motorcycle appropriate accident databases can be used to provide a basis for determining severity levels.

NOTE 2 The severity class can be based on a combination of injuries, resulting in a higher classification of the severity than from considering a single injury.

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

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

NOTE 5 Standard protective equipment (e.g. helmet, protective jacket, gloves and boots) as prescribed in the vehicle user manual is assumed to be in use.

Table 2 — 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

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

EXAMPLE For an automotive application, the item under consideration includes an airbag functionality to reduce crash violence. For an accident in which the airbag fails to deploy, the crash violence could be assumed to correspond to a severity class of S3. If a correctly operating airbag would have reduced the crash violence to a level corresponding to a severity class of S2, the difference would be one severity class. Hence the severity class for the failure to deploy the airbag in this situation can be set to S1.

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

8.4.3.5 The probability of exposure of each operational situation shall be estimated based on a defined rationale for each hazardous event. The probability of exposure shall be assigned to one of the probability classes, E0, E1, E2, E3 or E4 in accordance with Table 3.

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

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

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

Table 3 — 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

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

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

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

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

8.4.3.8 The controllability of each hazardous event, by the rider or other persons involved in the operational situation, shall be estimated based on a defined rationale for each hazardous event. The controllability shall be assigned to one of the controllability classes C0, C1, C2 or C3 in accordance with Table 4.

NOTE 1 The evaluation of the controllability is an estimate of the probability that someone is able to gain sufficient control of the hazardous event, such that they are able to avoid the specific harm. For this purpose, the parameter C is used, with the classes C0, C1, C2 and C3, to classify the potential of avoiding harm. Some examples, which serve as an interpretation of these classes, are listed in Table B.4. Estimates can be made using either experimental or analytical procedures.

NOTE 2 For motorcycles, It is assumed that the rider is in an appropriate condition to ride (e.g. they are not tired), has the appropriate riding training (they have a rider's licence), understands the operational characteristics of the motorcycle in use and is complying with the applicable legal regulations, including due care requirements to avoid risks to other traffic participants.

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 or may not be aware that a potentially hazardous situation evolves.

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 assumed action of other participants.

NOTE 5 For motorcycle hazardous events, the evaluation of controllability levels is described in Annex C.

NOTE 6 Dedicated regulations that specify a functional performance with regard to the applicable hazardous event can be used as part of a rationale when selecting a suitable controllability class, if applicable, and supported by evidence, e.g. real usage experience.

NOTE 7 Dedicated regulation refers to requirements set by a governmental agency, which can specify minimum performance limits that must be met by all manufacturers in order for their vehicles to be approved for sale and use.

Table 4 — Classes of controllability

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

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

8.4.3.10 An MSIL shall be determined for each hazardous event based on the classification of severity, probability of exposure and controllability, in accordance with Table 5.

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

Table 5 — MSIL determination

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

8.4.3.11 The MSIL shall be mapped to an ASIL in accordance with Table 6, prior to the definition of the safety goals, so that the applicable requirements of the ISO 26262 series of standards can be adopted.

NOTE 1 In addition to these three ASILs, the class QM (quality management) denotes no requirement to comply with ISO 26262. Nevertheless, the corresponding hazardous event can have consequences with regards to safety and safety requirements can be formulated in this case. The classification QM indicates that quality processes are sufficient to manage the identified risk.

NOTE 2 The MSIL is mapped to ASIL so that the most appropriate degree of rigour is used in avoiding unreasonable residual risk associated with malfunctioning E/E items or elements used in motorcycle applications.

NOTE 3 The indicated ASIL levels, determined from MSIL levels, are intended to represent minimum requirements.

Table 6 — Mapping of MSIL to ASIL

MSIL	ASIL
QM	QM
A	QM
B	A
C	B
D	C

8.4.4 Determination of safety goals

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

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

8.4.4.2 The ASIL, mapped from MSIL, 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 8.4.4.1, the highest ASIL shall be assigned to the combined safety goal.

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

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

8.4.4.4 Assumptions used for, or resulting from the hazard analysis and risk assessment which are relevant for ASIL determination (if applicable, including hazardous events classified QM or with no MSIL assigned) shall be identified. These assumptions shall be validated in accordance with Clause 10 for the integrated item.

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

8.4.5 Verification

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

a) appropriate selection with regard to operational situations and hazard identification;

b) compliance with the item definition;

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

d) completeness of the coverage of the hazardous events;

e) consistency of the safety goals with the assigned ASILs mapped from MSILs and the corresponding hazardous events; and

f) consistency of MSIL-ASIL mapping.

8.5 Work products

8.5.1 Hazard analysis and risk assessment report resulting from requirements in 8.4.1 to 8.4.4.

8.5.2 Verification report of the hazard analysis and risk assessment resulting from requirements in 8.4.5.

9 Vehicle integration and testing

9.1 Objective

This clause provides a tailoring of ISO 26262-4:2018, 7.4.4 for motorcycles.

The vehicle integration is the integration of the item with other systems within a vehicle and with the vehicle itself.

9.2 Requirements and recommendations

9.2.1 Vehicle integration

9.2.1.1 The item shall be integrated into the vehicle and the vehicle integration tests shall be carried out.

NOTE When planning the vehicle level integration and verification, the correct vehicle behaviour under typical and extreme vehicle conditions and environments can be considered, but with a subset being sufficient (see ISO 26262-4:2018, Table 3).

9.2.1.2 The verification of the interface specification of the item with the in-vehicle communication network and the in-vehicle power supply network shall be performed.

9.2.2 Test goals and test methods during vehicle testing

9.2.2.1 Test goals resulting from the requirements 9.2.2.2 to 9.2.2.5 shall be addressed by the application of adequate test methods as listed in the corresponding tables.

NOTE 1 These will support the detection of systematic faults during vehicle integration.

NOTE 2 Depending on the implemented functionality, its complexity or the distributed nature of the system, it could be feasible to perform tests in other integration subphases provided adequate rationale is given.

NOTE 3 If concerns over rider safety exist, it can be appropriate to select alternative test methods or move test activities to other sub-phases.

9.2.2.2 The correct implementation of the functional safety requirements at the vehicle level shall be demonstrated where feasible using test methods listed in Table 7.

Table 7 — Correct implementation of the functional safety requirements at the vehicle level

Methods		ASIL		
		A	B	C
1a	Requirement-based test[a]	++	++	++
1b	Fault injection test[b]	++	++	++
1c	Long-term test[c]	++	++	++
1d	User test under real-life conditions[c,d]	++	++	++

[a] A requirements-based test denotes a test against functional and non-functional requirements.

[b] A fault injection test uses special means to introduce faults into the item. This can be done within the item via a special test interface or specially prepared elements or communication devices. The method is often used to improve the test coverage of the safety requirements, because during normal operation safety mechanisms are not invoked.

[c] A long-term test and a user test under real-life conditions are similar to tests derived from field experience but use a larger sample size, normal users as testers, and are not bound to prior specified test scenarios, but performed under real-life conditions during everyday life. These tests can have limitations if necessary to ensure the safety of the testers, e.g. with additional safety measures or disabled actuators. Long-term tests can be infeasible for motorcycles.

[d] User tests can be infeasible for motorcycles.

9.2.2.3 This requirement applies to ASIL (A), (B), and C. The correct functional performance, accuracy and timing of the safety mechanisms at the vehicle level shall be demonstrated using test methods listed in Table 8.

Table 8 — Correct functional performance, accuracy and timing of safety mechanisms at the vehicle level

Methods		ASIL		
		A	B	C
1a	Performance test[a]	+	+	++
1b	Long-term test[b]	+	+	++
1c	User test under real-life conditions[b,c]	+	+	++
1d	Fault injection test[d]	o	+	++
1e	Error guessing test[e]	o	+	++
1f	Test derived from field experience[f]	o	+	++

[a] A performance test can verify the performance (e.g. fault tolerant time intervals on vehicle level and vehicle controllability in the presence of faults) of the safety mechanisms concerning the item.

[b] A long-term test and a user test under real-life conditions are similar to tests derived from field experience but use a larger sample size, normal users as testers, and are not bound to prior specified test scenarios, but performed under real-life conditions during everyday life. These tests can have limitations if necessary to ensure the safety of the testers, e.g. with additional safety measures or disabled actuators. Long-term tests can be infeasible for motorcycles.

[c] User tests can be infeasible for motorcycles.

[d] A fault injection test uses special means to introduce faults into the item. This can be done within the item via a special test interface or specially prepared elements or communication devices. The method is often used to improve the test coverage of the safety requirements, because during normal operation safety mechanisms are not invoked.

[e] An error guessing test uses expert knowledge and data collected through lessons learned to anticipate errors in the system. Then a set of tests along with adequate test facilities is designed to check for these errors. Error guessing is an effective method given a tester who has previous experience with similar systems.

[f] A test derived from field experience and data gathered from the field.

9.2.2.4 This requirement applies to ASIL (A), (B), and C. The consistency and correctness of the implementation of the interfaces internal and external to the vehicle shall be demonstrated using test methods listed in Table 9.

NOTE Internal interfaces are between items/systems. External interfaces are between an item and the vehicle environment.

Table 9 — Correct implementation of internal and external interfaces at the vehicle level

Methods		ASIL		
		A	B	C
1a	Test of internal interfaces[a]	+	+	++
1b	Test of external interfaces[a]	+	+	++
1c	Test of interaction/communication[b]	+	+	++

[a] An interface test at the vehicle level tests the interfaces of the vehicle systems for compatibility. This can be done statically by validating value ranges, ratings or geometries as well as dynamically during operation of the whole vehicle.

[b] A communication and interaction test includes tests of the communication between the systems of the vehicle during runtime against functional and non-functional requirements.

9.2.2.5 This requirement applies to ASIL (A), (B), and C. The level of robustness at the vehicle level shall be demonstrated using test methods listed in Table 10.

Table 10 — Level of robustness at the vehicle level

Methods		ASIL		
		A	B	C
1a	Resource usage test[a]	+	+	++
1b	Stress test[b]	+	+	++
1c	Test for interference resistance and robustness under certain environmental conditions[c]	+	+	++
1d	Long-term test[d]	+	+	++

[a] At the vehicle level, resource usage testing is usually performed in dynamic environments (e.g. electronic control unit network environments, prototypes or whole vehicles). Issues to test include item internal resources, power consumption or limited resources of other vehicle systems.

[b] A stress test verifies the correct operation of the vehicle under high operational loads or high demands from the environment. Therefore tests under high loads on the vehicle or with extreme user inputs or requests from other systems as well as tests with extreme temperatures, humidity or mechanical shocks can be applied.

[c] A test for interference resistance and robustness, under certain environmental conditions, is a special case of stress testing. This includes EMC and ESD tests (e.g. see References [4] and [5]).

[d] A long-term test and a user test under real-life conditions are similar to tests derived from field experience but use a larger sample size, normal users as testers, and are not bound to prior specified test scenarios, but performed under real-life conditions during everyday life. Long-term tests can be infeasible for motorcycles.

10 Safety validation

10.1 Objective

This clause provides a tailoring of ISO 26262-4:2018, Clause 8 for motorcycles.

The objectives of this clause are:

a) to provide evidence that the safety goals are achieved by the item when being integrated into the respective vehicle(s); and

b) to provide evidence that the functional safety concept and the technical safety concept are appropriate for achieving functional safety for the item.

10.2 General

The purpose of the preceding verification activities (e.g. design verification, safety analyses, hardware, software, and item integration and test) is to provide evidence that the results of each particular activity comply with the specified requirements.

The safety validation of the integrated item in representative vehicle(s) aims to provide evidence of appropriateness for the intended use and aims to confirm the adequacy of the safety measures for a class or set of vehicles. Safety validation provides assurance that the safety goals have been achieved, based on examination and test.

10.3 Inputs to this clause

10.3.1 Prerequisites

The following information shall be available:

— hazard analysis and risk assessment report in accordance with 8.5.1; and

— functional safety concept in accordance with ISO 26262-3:2018, 7.5.1.

10.3.2 Further supporting information

The following information can be considered:

— technical safety concept (see ISO 26262-4:2018, 6.5.2);

— item definition (see ISO 26262-3:2018, 5.5.1); and

— safety analyses report (see ISO 26262-4:2018, 6.5.7).

10.4 Requirements and recommendations

10.4.1 Safety validation environment

10.4.1.1 The safety goals shall be validated for the item in a representative context at vehicle level.

NOTE This integrated item includes, where applicable: system, software, hardware, elements of other technologies, external measures.

10.4.1.2 For the definition of a representative context, representative vehicles based on vehicle types and vehicle configurations shall be considered.

NOTE The Hazard Analysis and Risk Assessment report might be used as a source of information regarding relevant input for the choice of representative vehicles (see 8.5.1).

10.4.1.3 Safety goals shall be validated giving consideration to variance in operation that impacts the technical characteristics, which have been considered in the hazard analysis and risk assessment.

10.4.2 Specification of safety validation

10.4.2.1 The safety validation specification shall be defined, including:

a) the configuration of the item subjected to safety validation including its calibration data in accordance with ISO 26262-6:2018, Annex C;

NOTE If a complete safety validation of each item configuration is not feasible, then a reasonable subset can be selected.

b) the specification of safety validation procedures, test cases, riding manoeuvres, and acceptance criteria; and

c) the equipment and the required environmental conditions.

10.4.3 Execution of safety validation

10.4.3.1 If testing is used for safety validation, then the same requirements as provided for verification testing (see ISO 26262-8:2018, 9.4.2 and 9.4.3) may be applied.

10.4.3.2 The achievement of functional safety for the item when being integrated into the vehicle shall be validated by evaluating the following aspects:

a) the controllability;

NOTE 1 Controllability can be validated using operating scenarios, including intended use and foreseeable misuse.

NOTE 2 One acceptance criterion for the safety validation might be a sufficient controllability in a safe state defined in ISO 26262-3:2018, 7.4.2.5.

NOTE 3 A single acceptance criterion might not be sufficient to verify a safe state.

b) the effectiveness of the external measures;

c) the effectiveness of the elements of other technologies; and

d) assumptions that influence the ASIL mapped from MSIL in the hazard analysis and risk assessment (see 8.4.4.4) that can be checked only in the final vehicle.

EXAMPLE If a mechanical component is assumed to prevent or mitigate a specific hazard potentially caused by a malfunction of an E/E system, the effectiveness of this component to prevent or mitigate that hazard is validated on vehicle level.

10.4.3.3 The safety validation at the vehicle level, based on the safety goals, the functional safety requirements and the intended use, shall be executed as planned using:

a) the safety validation procedures and test cases for each safety goal including detailed pass/fail criteria; and

b) the scope of application. This may include issues such as configuration, environmental conditions, riding situations, operational use cases, etc.

NOTE Operational use cases can be created to help focus the safety validation at the vehicle level.

10.4.3.4 An appropriate set of the following methods shall be applied:

a) repeatable tests with specified test procedures, test cases, and pass/fail criteria;

EXAMPLE 1 Positive tests of functions and safety requirements, black box testing, simulation, tests under boundary conditions, fault injection, durability tests, stress tests, highly accelerated life testing (HALT), simulation of external influences.

b) analyses;

EXAMPLE 2 FMEA, FTA, ETA, simulation.

c) long-term tests, such as vehicle driving schedules and captured test fleets;

NOTE 1 Long-term tests with targeted users can be infeasible for motorcycles.

d) user tests under real-life conditions, panel or blind tests, expert panels; and

NOTE 2 User test can be infeasible for motorcycles. Real-life condition can be conducted using simulated condition.

e) reviews.

10.4.4 Evaluation

10.4.4.1 The results of the safety validation shall be evaluated to provide evidence that the implemented safety goals achieve functional safety for the item.

10.5 Work products

10.5.1 Safety validation specification including safety validation environment description resulting from requirements in 10.4.1 and 10.4.2.

10.5.2 Safety validation report resulting from requirements in 10.4.3 and 10.4.4.

Annex A
(informative)

Overview of and workflow of adaptation of the ISO 26262 series of standards for motorcycles

A.1 General

This annex provides the overview of and work flow for motorcycles to implement ISO 26262-2:2018, ISO 26262-3:2018 and ISO 26262-4:2018.

A.2 Overview of and workflow of management of functional safety

Table A.1 provides an overview of objectives, prerequisites and work products of management of functional safety for motorcycles.

Table A.1 — Overview of Functional safety management

Clause	Objectives	Prerequisites	Work products
ISO 26262-2:2018, Clause 5 Overall safety management In this document Clause 6 Safety culture	The intent of this clause is to ensure the organizations involved in the execution of the safety lifecycle, i.e. those that are responsible for the safety lifecycle or are performing safety activities in the safety lifecycle, achieve the following objectives: a) to institute and maintain a safety culture that supports and encourages the effective achievement of functional safety and promotes effective communication with other disciplines related to functional safety; b) to institute and maintain adequate organization-specific rules and processes for functional safety; c) to institute and maintain processes to ensure an adequate resolution of identified safety anomalies; d) to institute and maintain a competence management system to ensure that the competence of the involved persons is commensurate with their responsibilities; and e) to institute and maintain a quality management system to support functional safety. This clause serves as a prerequisite to the activities in the ISO 26262 safety lifecycle.	None	ISO 26262-2:2018, 5.5.1 Organization-specific rules and processes for functional safety ISO 26262-2:2018, 5.5.2 Evidence of competence management ISO 26262-2:2018, 5.5.3 Evidence of a quality management system ISO 26262-2:2018, 5.5.4 Identified safety anomaly reports, if applicable

Table A.1 *(continued)*

Clause	Objectives	Prerequisites	Work products
ISO 26262-2:2018, Clause 6 Project dependent safety management In this document Clause 7 Confirmation measures	The intent of this clause is to ensure that the following objectives are achieved by the organizations involved in the concept phase or the development phases at the system, hardware or software level: a) to define and assign the roles and responsibilities regarding the safety activities; b) to perform an impact analysis at the item level to identify whether the item is a new item, a modification of an existing item, or an existing item with a modified environment; and in the case of one or more modifications, to analyse the implications of the identified modifications on functional safety; c) to perform an impact analysis at element level in the case an existing element is reused, to evaluate whether the reused element is able to comply with the safety requirements allocated to that element, considering the operational context in which the element is reused; d) to define the tailored safety activities, to provide the corresponding rationales for tailoring and to review the provided rationales; e) to plan the safety activities; f) to coordinate and track the progress of the safety activities in accordance with the safety plan; g) to plan the distributed developments (refer to ISO 26262-8:2018, Clause 5); h) to ensure a correct progression of the safety activities throughout the safety lifecycle; i) to create a comprehensible safety case in order to provide the argument for the achievement of functional safety; j) to judge whether the item achieves functional safety (i.e. the functional safety assessment), or to judge the contribution to the achievement of functional safety concerning an element (i.e. the functional safety assessment activities performed by a supplier) or work product (e.g. a confirmation review); and	Organization-specific rules and processes for functional safety (see ISO 26262-2:2018, 5.5.1) Evidence of competence management (see ISO 26262-2:2018, 5.5.2) Evidence of a quality management system (see ISO 26262-2:2018, 5.5.3)	ISO 26262-2:2018, 6.5.1 Impact analysis at the item level ISO 26262-2:2018, 6.5.2 Impact analyses at element level, if applicable ISO 26262-2:2018, 6.5.3 Safety plan ISO 26262-2:2018, 6.5.4 Safety case ISO 26262-2:2018, 6.5.5 Confirmation measure reports ISO 26262-2:2018, 6.5.6 Release for production report

Table A.1 *(continued)*

Clause	Objectives	Prerequisites	Work products
	k) to decide at the end of development whether the item, or element(s), can be released for production based on the evidence that supports confidence in the achieved functional safety.		
ISO 26262-2:2018, Clause 7 Safety management regarding production, operation, service and decommissioning	The objective of this clause is to define the responsibilities of the organizations and persons responsible for achieving and maintaining functional safety regarding production, operation, service and decommissioning.	Organization-specific rules and processes for functional safety (see ISO 26262-2:2018, 5.5.1) Evidence of competence management (see ISO 26262-2:2018, 5.5.2) Evidence of a quality management system (see ISO 26262-2:2018, 5.5.3) Release for production report (see ISO 26262-2:2018, 6.5.6)	ISO 26262-2:2018, 7.5.1 Evidence of safety management regarding production, operation, service and decommissioning

A.3 Overview of and workflow of concept phase

Table A.2 provides an overview of objectives, prerequisites and work products of concept phase for motorcycles.

Table A.2 — Overview of concept phase

Clause	Objectives	Prerequisites	Work products
ISO 26262-3:2018, Clause 5 Item definition	The objectives of this clause are: a) to define and describe the item, its functionality, dependencies on, and interaction with, the driver, the environment and other items at the vehicle level; and b) to support an adequate understanding of the item so that the activities in subsequent phases can be performed.	None	ISO 26262-3:2018, 5.5.1 Item definition resulting from requirements in ISO 26262-3:2018, 5.4
In this document Clause 8 Hazard analysis and risk assessment	The objectives of this clause are: a) to specify the necessary requirements that need to be complied with in order to perform a motorcycle specific hazard analysis and risk assessment; b) to identify and classify the hazardous events caused by malfunctioning behaviour of the item; and	Item definition (see ISO 26262-3:2018, 5.5.1)	8.5.1 Hazard analysis and risk assessment report resulting from requirements 8.4.1 to 8.4.4 8.5.2 Verification report of the hazard analysis and risk assessment resulting from requirement 8.4.5

Table A.2 *(continued)*

Clause	Objectives	Prerequisites	Work products
	c) to formulate the safety goals with their corresponding ASILs, mapped from MSILs, related to the prevention or mitigation of the hazardous events, in order to avoid unreasonable risk.		
ISO 26262-3:2018, Clause 7 Functional safety concept	The objectives of this clause are: a) to specify the functional or degraded functional behaviour of the item in accordance with its safety goals; b) to specify the constraints regarding suitable and timely detection and control of relevant faults in accordance with its safety goals; c) to specify the item level strategies or measures to achieve the required fault tolerance or adequately mitigate the effects of relevant faults by the item itself, by the driver or by external measures; d) to allocate the functional safety requirements to the system architectural design, or to external measures, and e) to verify the functional safety concept and specify the safety validation criteria.	Item definition (see ISO 26262-3:2018, 5.5.1) Hazard analysis and risk assessment report (see 8.5.1) System architectural design (from external source)	ISO 26262-3:2018, 7.5.1 Functional safety concept resulting from requirements ISO 26262-3:2018, 7.4.1 to 7.4.3 ISO 26262-3:2018, 7.5.2 Verification report of the functional safety concept resulting from requirements in ISO 26262-3:2018, 7.4.4

A.4 Overview of and workflow of product development of system level

Table A.3 provides an overview of objectives, prerequisites and work products of product development at system level for motorcycles.

Table A.3 — Overview of and workflow of product development at the system level for motorcycles

Clause	Objectives	Prerequisites	Work products
ISO 26262-4:2018, Clause 5 General topics for the product development at the system level	The objective of this Clause is to provide an overview of the product development at the system level.	—	—
ISO 26262-4:2018, Clause 6 Technical Safety Concept	The objectives of this Clause are: a) to specify technical safety requirements regarding the functionality, dependencies, constraints and properties of the system elements and interfaces needed for their implementation; b) to specify technical safety requirements regarding the safety mechanisms to be implemented in the system elements and interfaces; c) to specify requirements regarding the functional safety of the system and its elements during production, operation, service and decommissioning; d) to verify that the technical safety requirements are suitable to achieve functional safety at the system level and are consistent with the functional safety requirements; e) to develop a system architectural design and a technical safety concept that satisfy the safety requirements and that are not in conflict with the non-safety-related requirements; f) to analyse the system architectural design in order to prevent faults and to derive the necessary safety-related special characteristics for production and service; and g) to verify that the system architectural design and the technical safety concept are suitable to satisfy the safety requirements according to their respective ASIL.	Functional safety concept, see ISO 26262-3:2018, 7.5.1; System architectural design (from an external source, see ISO 26262-3:2018, 7.3.1) Requirements to the item from other safety relevant items if applicable	ISO 26262-4:2018, 6.5.1 Technical safety requirements specification resulting from requirements in ISO 26262-4:2018, 6.4.1 and 6.4.2 ISO 26262-4:2018, 6.5.2 Technical safety concept resulting from requirements in ISO 26262-4:2018, 6.4.3 to 6.4.6 ISO 26262-4:2018, 6.5.3 System architectural design specification resulting from requirements in ISO 26262-4:2018, 6.4.3 to 6.4.6 ISO 26262-4:2018, 6.5.4 Hardware-software interface (HSI) specification resulting from requirements in ISO 26262-4:2018, 6.4.7 ISO 26262-4:2018, 6.5.5 Specification of requirements for production, operation, service and decommissioning resulting from requirements in ISO 26262-4:2018, 6.4.8 ISO 26262-4:2018, 6.5.6 Verification report for system architectural design, the hardware-software interface (HSI) specification, the specification of requirements for production, operation, service and decommissioning, and the technical safety concept resulting from requirements in ISO 26262-4:2018, 6.4.9 ISO 26262-4:2018, 6.5.7 Safety analyses report resulting from requirements in ISO 26262-4:2018, 6.4.4

Table A.3 *(continued)*

Clause	Objectives	Prerequisites	Work products
ISO 26262-4:2018, Clause 7 Item integration and testing in this document Clause 9 Vehicle integration and testing	The objectives of this Clause are: a) to define the integration steps and to integrate the system elements until the system is fully integrated; b) to verify that the defined safety measures, resulting from safety analyses at the system architectural level, are properly implemented; and c) to provide evidence that the integrated system elements fulfil their safety requirements according to the system architectural design.	Safety goals from the hazard analysis and risk assessment report (see ISO 26262-3:2018, 6.5.1) Functional safety concept (see ISO 26262-3:2018, 7.5.1) Technical safety concept (see ISO 26262-4:2018, 6.5.2) System architectural design specification (see ISO 26262-4:2018, 6.5.3) Hardware-software interface specification (HSI) (see ISO 26262-4:2018, 6.5.4, ISO 26262-5:2018, 6.5.2 and ISO 26262-6:2018, 6.5.2)	ISO 26262-4:2018, 7.5.1 Integration and test strategy resulting from requirements in ISO 26262-4:2018, 7.4.1 ISO 26262-4:2018, 7.5.2 Integration and test report resulting from requirements in ISO 26262-4:2018, 7.4.2, 7.4.3 and 7.4.4
In this document Clause 10, Safety validation	This clause provides a tailoring of ISO 26262-4:2018, Clause 8 for motorcycles. The objectives of this Clause are: a) to provide evidence that the safety goals are achieved by the item when being integrated into the respective vehicle(s); and b) to provide evidence that the functional safety concept and the technical safety concept are appropriate for achieving functional safety for the item.	Hazard analysis and risk assessment report (see 8.5.1); Functional safety concept (see ISO 26262-3:2018, 7.5.1)	10.5.1 Safety validation specification including safety validation environment description resulting from requirements in 10.4.1 and 10.4.2 10.5.2 Safety validation report resulting from requirements in 10.4.3 and 10.4.4

Annex B
(informative)

Hazard analysis and risk assessment for motorcycles

B.1 General

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

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

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

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

The hazard analysis and risk assessment subphase comprises three steps, as described below.

a) Situation analysis and hazard identification (see 8.4.2): 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 and urban operation, parking and off-road;

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

   — reasonably foreseeable rider use and misuse; and

   — interaction between operational systems.

b) Classification of hazardous events (see 8.4.3): 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 riding situation, while the probability of exposure is determined by the corresponding situation. The controllability rates how easy or difficult it is for the rider 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) MSIL determination (see 8.4.3): determining the required motorcycle safety integrity level.

B.2 Examples of severity

B.2.1 General

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

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

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

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

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

The use of a specific injury scale depends on the state of medical research at the time the analysis is performed. Therefore, the appropriateness of the different injury scales, such as AIS, ISS, and New ISS (NISS), can vary over time (see References [1], [2] and [3]).

B.2.2 Description of the AIS stages

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

— AIS 0: no injuries;

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

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

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

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

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

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

Table B.1 — Examples of severity classification

	Class of Severity(see Table 2)			
	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 and less than 10 % probability of AIS 1-6; or damage that cannot be classified safety-related	more than 10 % probability of AIS 1-6 (and not S2 or S3)	more than 10 % probability of AIS 3-6 (and not S3)	more than 10 % probability of AIS 5-6
Informative examples	Falling alone/loss of balance. Collision with roadside infrastructure/ stationary vehicle at walking speed. Rear collision (passenger car into rear of motorcycle) with differential speed equivalent to typical walking speed.	Collision with roadside infrastructure/ stationary vehicle at typical urban vehicle speeds. Impact with pedestrian/cyclist at typical walking speed. Low side fall at typical urban/main road vehicle speeds with no subsequent impact. High side fall at typical urban road vehicle speeds with no subsequent impact. Side collision (passenger car into side of motorcycle) at typical walking speed. Rear collision (passenger car into rear of motorcycle) with differential speed equivalent to typical urban vehicle speed. Front collision into an oncoming passenger car with differential speed equivalent to typical walking speed.	Collision with roadside infrastructure/ stationary vehicle at typical main road vehicle speeds. Impact with pedestrian/cyclist at typical urban vehicle speeds. Low side fall at typical highway vehicle speeds with no subsequent impact. High side fall at typical main road/highway vehicle speeds with no subsequent impact. Side collision (passenger car into side of motorcycle) at typical urban vehicle speed. Rear collision (passenger car into rear of motorcycle) with differential speed equivalent to typical main road vehicle speed. Front collision into an oncoming passenger car with differential speed equivalent to typical urban vehicle speed.	Collision with roadside infrastructure/ stationary vehicle at typical highway vehicle speeds. Impact with pedestrian/cyclist at typical main road vehicle speeds. Side collision (passenger car into side of motorcycle) at typical main road vehicle speed. Rear collision (passenger car into rear of motorcycle) with differential speed equivalent to typical highway vehicle speed. Front collision into an oncoming passenger car with differential speed equivalent to typical main road/highway vehicle speed.

B.3 Examples and explanations of the probability of exposure

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

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

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

EXAMPLE Typical examples of E0 include the following:

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

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

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

NOTE 1 The classification can depend on, for example, geographical location or type of use (see 8.4.3.5).

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

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

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

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

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

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

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

NOTE 2 With regard to the duration of the considered failure, the hazard analysis and risk assessment does not consider safety mechanisms that are part of the item (see 8.4.1.2).