DRAFT INTERNATIONAL STANDARD ISO/DIS 26262-2

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

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

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

Road vehicles — Functional safety —

Part 2:
Management of functional safety

Véhicules routiers — Sécurité fonctionnelle —

Partie 2: Gestion de la sécurité fonctionnelle

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 26262-2 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.

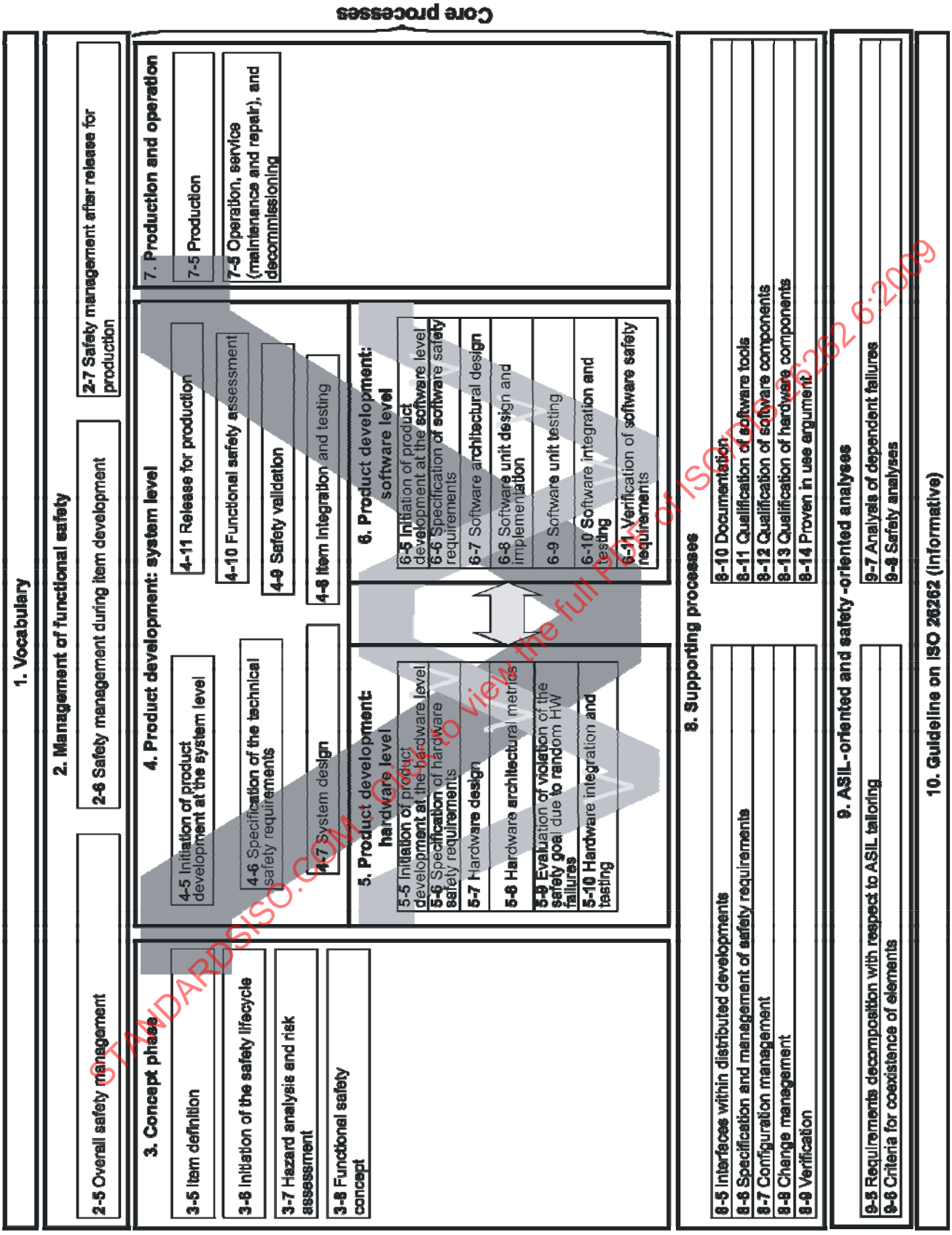

Figure 1 — Overview of ISO 26262

Road vehicles — Functional safety — Part 2: Management of functional safety

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 ISO 26262 specifies the requirements on functional safety management for automotive applications. These requirements cover the project management activities of all safety lifecycle phases and consist of project-independent requirements, project-dependent requirements to be followed during development, and requirements that apply after release for production.

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 26262-3: —[1] *Road vehicles – Functional Safety — Part 3: Concept phase*

ISO 26262-4: —[1] *Road vehicles – Functional Safety — Part 4: Product development: system level*

ISO 26262-5: —[1] *Road vehicles – Functional Safety — Part 5: Product development: hardware level*

ISO 26262-6: —[1] *Road vehicles – Functional Safety — Part 6: Product development: software level*

ISO 26262-7: —[1] *Road vehicles – Functional Safety — Part 7: Production and operation*

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*

[1] To be published

3 Terms, definitions, abbreviated terms

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

4 Requirements for compliance

4.1 General requirements

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

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 Overall safety management

5.1 Objectives

The objective of this clause is to define the requirements on the organizations that are responsible for the safety lifecycle, or that perform safety activities in the item's safety lifecycle.

This clause serves as a prerequisite to all the ISO°26262 activities in the item's safety lifecycle.

5.2 General

5.2.1 Overview of the safety lifecycle concept

The safety lifecycle (see Figure°2) encompasses principal safety activities during the concept phase, product development, and after the release for production. The planning, coordination and documentation of these activities for all phases of the safety lifecycle is a key management task.

Figure°2 represents the standard safety lifecycle model, but tailoring of the safety lifecycle, including iterations of subphases, is allowed.

NOTE The activities during concept phase, product development and after release for production are described in detail in ISO°26262-3, ISO°26262-4, ISO°26262-5, ISO°26262-6 and ISO°26262-7.

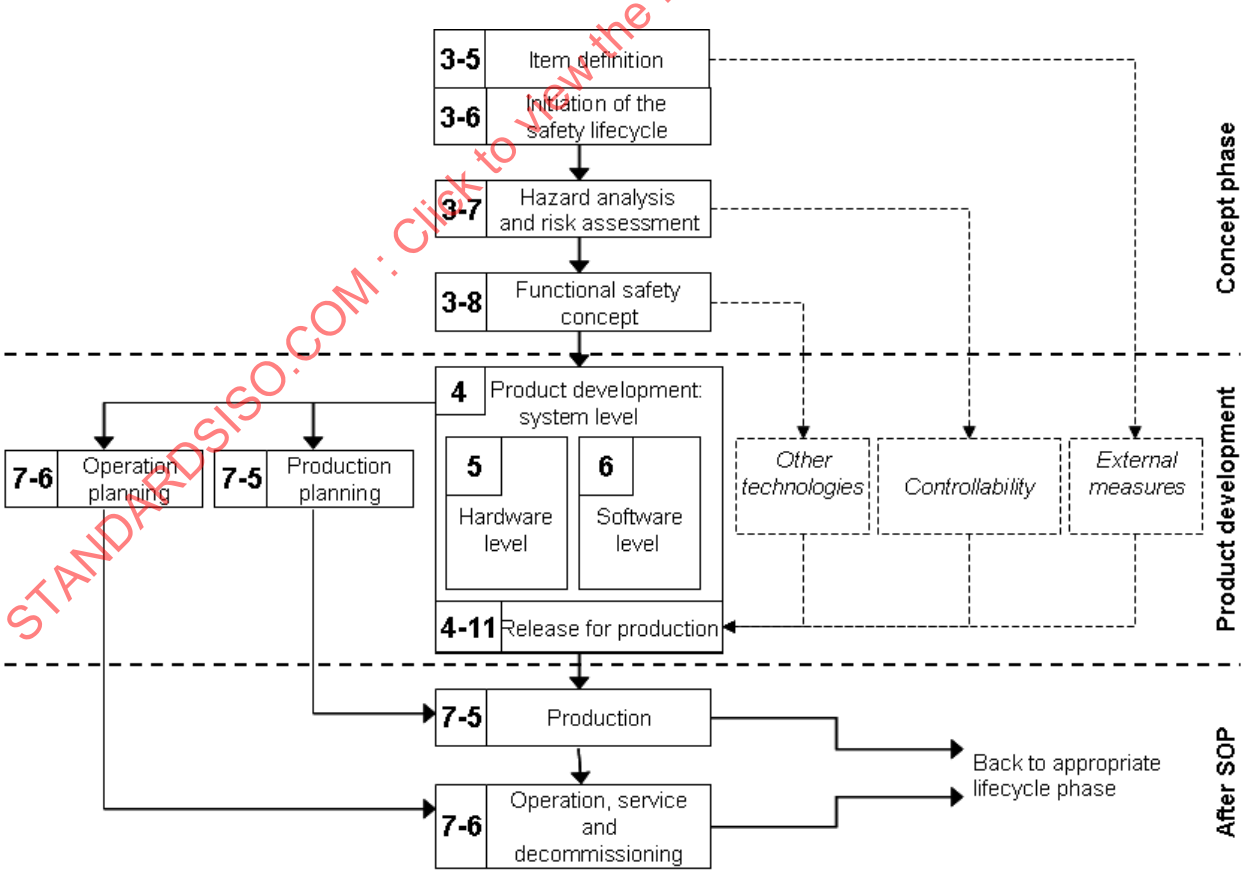

Figure 2 — Safety lifecycle

5.2.2 Explanatory remarks on the lifecycle

The organization developing safety-related systems will fulfil the requirements on functional safety, in accordance with ISO°26262, including the management of functional safety.

The key management tasks are to plan, coordinate and track the activities related to functional safety. These management tasks apply to all phases of the safety lifecycle. The respective requirements for management of functional safety are given in this Part, which distinguishes:

- Overall safety management (see this Clause);
- Safety management during development of the item (see Clause°6);
- Safety management after release for production (see Clause°7).

The following descriptions elaborate on the definitions of the different phases of the safety lifecycle:

- Item definition

  The initiating task of the safety lifecycle is to develop a description of the item with regard to its functionality, interfaces, environmental conditions, legal requirements, hazards etc. The boundary of the item and its interfaces, as well as assumptions concerning other functions, systems and components are determined (see ISO°26262-3, Clause°5).

- Initiation of the safety lifecycle

  Upon the item definition, the safety lifecycle is initiated by distinguishing between either a new development, or a modification. In the case of a modification, the results of the impact analysis can be used to tailor the safety lifeycle.

- Hazard analysis and risk assessment

  After the initiation of the safety lifecycle, the hazard analysis and risk assessment is performed in accordance with ISO°26262-3, Clause°7. The hazard analysis & risk assessment procedure, which considers the probability of exposure, controllability and severity, determines the ASIL of the item. In the next step, a safety goal for each hazard is derived and the respective ASIL is assigned.

- Functional safety concept

  Based on the safety goals, a functional safety concept (see ISO°26262-3, Clause°8) is specified considering preliminary architectural assumptions. The functional safety concept is detailed and specified by functional safety requirements that are allocated to the elements of the item. Systems outside the item's boundary as well as other technologies can be considered as part of the functional safety concept. The requirements for implementation in other technologies or for external measures are not in the scope of ISO°26262.

- Product development at the system level

  After having specified the functional safety concept, the item is developed from the system level perspective, in accordance with ISO°26262-4. The system development process is based on the concept of a V-model with the specification of the technical safety requirements, the system design, and their testing, on the left-hand branch and the integration, verification, validation and assessment of functional safety on the right-hand branch.

  Product development includes

  - the safety validation results of those aspects of the functional safety concept implemented in other technologies;

— the validation of assumptions concerning the effectiveness and the performance of external measures; and

— the validation of assumptions concerning human response, including controllability and operational tasks.

For an overview of the subphases of the product development at the system level, see Figure°1.

— Product development at the hardware level

Based on the system design specification, the item is developed from the hardware level perspective in accordance with ISO°26262-5. The hardware development process is based on the concept of a V-model with the specification of the hardware requirements and the hardware design on the left-hand branch and the hardware integration and verification on the right-hand branch.

For an overview of the subphases of the product development at the hardware level, see Figure°1.

— Product development at the software level

Based on the system design specification, the item is developed from the software level perspective in accordance with ISO°26262-6. The software development process is based on the concept of a V-model with the specification of the software requirements and the software architectural design on the left-hand branch, and the software integration and the verification of the software safety requirements on the right-hand branch.

For an overview of the subphases of the product development at the software level, see Figure°1.

— Production planning and operation planning

The planning for production and operation, and the specification of the associated requirements, starts during product development at the system level (see ISO°26262-4). The requirements on production and operation are given in ISO°26262-7, Clause° 5 and Clause°6.

— Release for production

The release for production is the final subphase of the product development and provides the item's sign-off, as given in ISO°26262-4, Clause°11.

— Production and operation, service and decommissioning

The requirements to be complied with during the subphases: production, operation, service and decommissioning are given in ISO°26262-7, Clause°5 and Clause°6.

— Controllability

In the hazard analysis and risk assessment (see ISO°26262-3, Clause°7), credit can be taken from the ability of the driver, or other endangered persons, to control hazardous situations.

The means of providing the evidence of the effectiveness of the controllability is outside the scope of ISO°26262, but without such evidence the safety case is not complete.

NOTE The exposure and the severity are factors that depend on the scenario. The controllability is influenced by the design of the item and is therefore evaluated during the validation (see ISO°26262-4, 9.4.3.2).

— External measures

The external measures refer to the measures outside the item, described in the item definition (see ISO°26262-3, Clause°5), that reduce or mitigate the risks resulting from the item. External risk reduction

measures can include additional in-vehicle devices like dynamic stability controllers or run-flat tyres, but also devices external to the vehicle, like guardrails or tunnel fire-fighting systems.

External risk reduction measures can be considered in the hazard analysis and risk assessment.

The means of providing the evidence of the effectiveness of the external measures is outside the scope of ISO°26262, unless the external measures are realized by E/E, but without such evidence the safety case is not complete.

— Other technologies

Other technologies are those different from E/E-technologies covered by ISO°26262, e.g. mechanical and hydraulic technology. These are considered during the specification of the functional safety concept (see ISO°26262-3, Clause 8) or during the allocation of the safety requirements.

NOTE As an alternative to the straightforward ASIL determination, it might be useful to repeat the hazard analysis and risk assessment and to re-determine the ASIL, in order to consider other technologies as an external means of risk reduction.

The means of providing the evidence of the effectiveness of risk reduction by other technologies is outside the scope of ISO°26262, but without such evidence the safety case is not complete.

5.3 Inputs to this Clause

5.3.1 Prerequisites

None

5.3.2 Further supporting information

The following information may be considered:

Evidence of a quality management system, complying with a quality standard, such as ISO°TS°16949, ISO°9001 or equal, and conforming to the requirements of this part of ISO°26262.

5.4 Requirements and recommendations

5.4.1 General

The requirements of 5.4.2 to 5.4.5, shall apply to all the organizations involved in the item's safety lifecycle.

5.4.2 Safety culture

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

EXAMPLE Leading and trailing indicators of a safety culture are given in Annex°B.

5.4.2.2 The organization shall establish, execute, and maintain, organization specific rules and processes to comply with the requirements of ISO°26262.

NOTE One of the means for performing the activities of the safety lifecycle, in accordance with ISO°26262, can be the creation and maintenance of a generic safety plan, and process description, in the organization.

5.4.2.3 The organization shall institute, execute and maintain processes to ensure that unresolved functional safety anomalies are explicitly communicated to the safety manager, and other responsible persons.

NOTE The role of the safety manager is specified in Clause°6.

5.4.2.4 The organization shall institute, execute and maintain a safety anomaly resolution process to ensure that the analysis, evaluation, resolution and disposition of functional safety anomalies is performed in a timely and effective manner.

NOTE The anomaly resolution process might include a root cause analysis that results in a corrective action for the future.

5.4.2.5 The organization shall ensure the fulfilment of the functional safety activities over the safety lifecycle, including the associated documentation.

5.4.2.6 The organization shall provide adequate resources for the achievement of functional safety.

NOTE Resources include: human resources, tools, databases, and templates.

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

— learning from the experiences made in the safety lifecycle of each item, including field experience, and

— deriving improvements for application on subsequent items.

5.4.2.8 The organization shall ensure that the persons performing, or supporting, the safety activities are given sufficient authority to fulfil their responsibilities.

5.4.3 Competence management

5.4.3.1 The organization shall ensure that the persons assigned to carry out activities provided by ISO°26262 have a sufficient level of skills, competences and qualification.

NOTE 1 One of the means, to achieve a sufficient level of skills and competences in development, is a training and qualification programme that considers the knowledge areas:

- usual safety practices, concepts and designs;
- ISO°26262 and, if applicable, further safety standards;
- organization specific rules for functional safety;
- functional safety processes instituted in the organization;
- methodology expertise.

NOTE 2 To evaluate the skills, competences and qualifications to carry out activities of ISO°26262, the experience from previous professional activities can be considered e.g.

- domain of the item;
- environment of the item;
- management experience.

NOTE 3 The required knowledge, experience, qualification and training can depend on the complexity of the item and the ASILs of the respective requirements.

5.4.4 Quality management during the safety lifecycle

5.4.4.1 All the organizations involved in the safety lifecycle of the item shall have a quality management system complying with a quality standard, such as ISO°TS°16949, ISO°9001, or equal.

5.4.4.2 The quality management system shall support the application of ISO°26262.

5.4.5 Project independent tailoring of the safety lifecycle

5.4.5.1 The safety lifecycle may be tailored, independent of the project, but only in one or more of the following ways:

a) the combining or splitting of subphases, activities or tasks;

NOTE Individual subphases can be combined if the method used makes it difficult to clearly distinguish between the individual subphases. For example, computer-aided development tools can support activities of several subphases within one step.

b) the performing of an activity, or task, in a different phase or subphase;

c) the performing of an activity, or task, in an added phase or subphase;

d) iterations within, or of, phases or subphases.

5.5 Work products

5.5.1 Organization specific rules and processes for functional safety, as a result of 5.4.2.

5.5.2 Evidence that the persons assigned to carry out activities provided by ISO°26262 have a sufficient level of skills, competences and qualification, as a result of 5.4.3.

5.5.3 Evidence of an operational E/E quality management system, conforming to the requirements of this part of ISO°26262, as a result of 5.4.4.

6 Safety management during the item development

6.1 Objectives

The first objective of this clause is to define the safety management roles and responsibilities, regarding the development phases in the item's safety lifecycle (see Figure°1 and Figure°2).

The second objective of this clause is to define the requirements on the safety management during the development phases, including the planning of the safety activities, the application of the safety lifecycle, the creation of the safety case, and the execution of the confirmation measures.

Safety management includes the responsibility to ensure that the confirmation measures are performed in accordance with the required levels of independence, regarding resources, management and responsibility for release for production.

Confirmation measures include confirmation reviews, functional safety audits and functional safety assessments.

The confirmation reviews are intended to check the compliance of the associated work products, with the requirements of ISO°26262.

Note, there are also verification reviews which are specified in other parts of ISO°26262. These are intended to review the technical correctness of the associated work products, regarding functional safety.

Table 1 lists all the confirmation reviews. Annex D lists all the confirmation reviews and all the verification reviews.

6.2 General

See 5.2.

6.3 Inputs to this Clause

6.3.1 Prerequisites

The following information shall be available:

— Organization specific rules and processes for functional safety (see 5.5.1)

— Evidence that the persons assigned to carry out activities provided by ISO°26262 have a sufficient level of skills, competences and qualification (see 5.5.2)

— Evidence of an operational E/E quality management system, conforming to the requirements of this part of ISO°26262 (see 5.5.3)

6.3.2 Further supporting information

The following information may be considered:

— Overall project plan (from external sources)

— Dependencies on other activities, including other safety activities

6.4 Requirements and recommendations

6.4.1 General

The requirements of 6.4.2 to 6.4.6 shall apply to items that have at least 1 safety goal with an ASIL A, B, C, or D, unless stated otherwise.

6.4.2 Roles and responsibilities in safety management

6.4.2.1 A project manager shall be appointed at the initiation of the project.

6.4.2.2 The project manager shall be assigned with the responsibility, and the authority, to ensure that:

a) the safety activities are performed; and

b) compliance with ISO°26262 is achieved.

6.4.2.3 The project manager shall verify that the organization has provided the required resources for the functional safety activities, in accordance with 5.4.2.6.

NOTE The estimation, determination and allocation of sufficient resources are generally performed in the planning phase.

6.4.2.4 The project manager shall ensure that a person is appointed to fill the role of safety manager, who is then responsible for functional safety management during the item development.

NOTE 1 The role of the safety manager can be filled by the project manager.

NOTE 2 The tasks of the safety manager can be tailored in accordance with the complexity of the item and the highest ASIL among the safety goals of the item.

NOTE 3 Functional safety management tasks include the timely and professional delivery of safety activity results. Certain tasks can be delegated, subject to the required competences, in accordance with 5.4.3.

6.4.3 Safety management during development

6.4.3.1 The safety manager shall plan the safety activities in the development subphases of the safety lifecycle.

NOTE Depending on whether the item is a new development, or a modification of an already existing item (see ISO°26262-3, Clause°6), the level of detail of the safety activities can vary, and will be planned accordingly.

6.4.3.2 The safety manager shall be responsible for the maintenance of the safety plan, and for monitoring the progress of the safety activities against the safety plan.

6.4.3.3 The safety plan shall either be

a) a plan referenced in the overall project plan; or

b) included in the overall project plan, such that the safety activities are distinguishable.

NOTE The safety plan can incorporate cross-references to other information under configuration management. Cross-references are generally preferable to the parallel description of activities in different work products, or in other documents that are under configuration management.

6.4.3.4 The item's safety lifecycle may be tailored. In this case, the tailoring shall be defined in the safety plan and a rationale shall be available and documented in accordance with ISO°26262-8, Clause°10. Furthermore:

a) if the safety lifecycle is tailored, because of a modification to an already existing item, then ISO°26262-3, Clause°6 shall be complied with;

b) if the safety lifecycle is tailored, because of a proven in use argument, then ISO-26262-8, Clause°14 shall be complied with;

c) if the safety lifecycle is tailored, in a non project specific manner, then 5.4.5 shall be complied with.

6.4.3.5 The safety plan shall include the planning of:

a) the implementation of strategies, activities, and procedures for achieving functional safety;

b) the development interface agreement (DIA) as specified in ISO°26262-8, Clause°5, if applicable;

c) the supporting processes, in accordance with ISO°26262-8;

d) the hazard analysis and risk assessment, in accordance with ISO°26262-3, Clause°7;

e) the development, and implementation, of the safety requirements in accordance with ISO°26262-3, Clause°8, ISO°26262-4, Clause°6 and Clause°7, ISO°26262-5 and ISO°26262-6;

f) the analysis of dependent failures, and the safety analyses, in accordance with ISO°26262-9, Clause°7 and Clause°8, respectively;

g) the verification and validation activities in accordance with ISO°26262-8, Clause°9 and ISO°26262-4, Clause°9, respectively;

NOTE The safety plan includes only the scheduling, or a general planning, of the verification and validation activities. The details are given in the integration and testing plan, and validation plan, respectively (see ISO°26262-4, 5.5.5 and 7.5.4, and ISO°26262-4, 5.5.3, 6.5.2 and 9.5.1 respectively).

h) the confirmation measures for functional safety in accordance with 6.4.6, Table°1, and Table°2;

NOTE1 The confirmation measures and the form of the result are defined, and the level of independence and the qualification of those carrying out the confirmation measures are given, in the safety plan.

NOTE2 The safety plan can include only the scheduling, or a general planning, of the confirmation measures. In this case, the details are given in the confirmation plan (see 6.4.6.1 and 6.5.5).

i) the inclusion of the overall safety activities (see Clause°5) into project-specific safety management;

j) the provision of the proven in use arguments, of the candidates, as specified in ISO°26262-8, Clause°14, if applicable; and

k) the definition of the tailored safety activities, in accordance with 6.4.3.4, if applicable.

6.4.3.6 The activities, described in the safety plan, shall include:

a) the objective;

b) the dependence on other activities or information;

EXAMPLE The results of the confirmation measures.

c) the required resources for performing the activity;

d) the starting point in time and duration; and

e) the identification of the respective work product.

6.4.3.7 This requirement applies to ASIL B, C, and D: the safety plan shall be approved, considering the confirmation review of the safety plan in accordance with Table°1, and authorised.

EXAMPLE The authorisation of the safety plan can be carried out by the project manager, or by the department manager.

6.4.4 Application of the safety lifecycle during development

6.4.4.1 The safety activities in a subsequent subphase of the safety lifecycle shall be started only when there is sufficient information from the preceding subphases.

NOTE Information can be considered as sufficient, if the lack of information does not cause an unacceptable risk to the achievement of the item's safety goals.

6.4.4.2 The safety activities may be tailored, i.e. omitted or performed in a different manner. In this case, a rationale shall be available and documented in accordance with ISO°26262-8, Clause°10. Furthermore:

a) if a safety activity is tailored by using a proven in use argument, then ISO 26262-8, Clause°14 shall be complied with,

b) if a safety activity is not applied, as a result of ASIL decomposition, then ISO°26262-9, Clause 5 shall be complied with.

NOTE The rationale considers the complexity of the item and the ASILs of the respective requirements.

6.4.4.3 The supporting processes, given in ISO°26262-8, shall start before, or at, the product development at system level.

6.4.5 Safety case

6.4.5.1 The requirements of 6.4.5 apply to items that have at least 1 safety goal with an ASIL (A), B, C, or°D.

6.4.5.2 The safety case shall:

a) be developed in accordance with the authorised safety plan, and

b) progressively compile the work products that are generated during the safety lifecycle, or a tailored safety lifecycle.

6.4.5.3 The safety case shall be sufficiently complete to evaluate the achievement of functional safety of the item.

6.4.5.4 The work products referenced in the safety case:

— shall be subject to configuration and change management, in accordance with ISO°26262-8, Clause°7 and Clause°8, starting from the phase: product development at system level (see ISO°26262-4); and

— shall be documented, in accordance with ISO°26262-8, Clause°10.

6.4.6 Confirmation measures for ensuring functional safety

6.4.6.1 The confirmation measures shall be planned.

NOTE 1 The confirmation plan can be included in the safety plan.

NOTE 2 The confirmation plan can include only the scheduling, or a general planning, of the functional safety assessment. In this case, more details will be given in the functional safety assessment plan (see 6.5.5, 6.5.6, and ISO°26262-4, 5.5.4).

6.4.6.2 The confirmation measures, as specified in Table°1, shall be performed during the item development, including the following:

a) the confirmation reviews;

NOTE 1 A confirmation review includes the checking of correctness with respect to formality, contents, adequacy and completeness regarding the requirements of ISO°26262.

NOTE 2 Table°1 includes all the required confirmation reviews. An overview of all the verification reviews and confirmation measures is given in Annex°D.

b) applies to ASIL (B), C, and D: Audit of functional safety processes; and

c) applies to ASIL (B), C, and D: Assessment of functional safety, in accordance with 6.4.6.7.

NOTE 3 The confirmation reviews, functional safety audits, and functional safety assessment reports include the name and revision number of the work products or process documents analysed.

NOTE 4 If the item changes subsequent to the completion of reviews and assessments, then the reviews or assessments will be repeated or supplemented (see ISO°26262-8, 8.4.5.2).

NOTE5 The aim of each confirmation review is given in Annex°C.

Table 1 — Required confirmation measures, including required independence

Confirmation measures					
Confirmation review of the hazard analysis & risk assessment, of the item that is dealt with in accordance with ISO°26262 (see ISO°26262-3, Clause 7 and if applicable, ISO 26262-8, Clause 5) - independent from the developers of the item	I3				For all ASILs, and including hazards rated as QM
	applies to ASIL				of the
	A	**B**	**C**	**D**	
Confirmation review of the safety plan (see Clause 6) - independent from the developers of the item / project management	-	I1	I2	I3	highest ASIL among safety goals of the item
Confirmation review of the integration and testing plan (see ISO°26262-4, Clause 5) -independent from the developers of the item / project management	I0	I1	I2	I2	highest ASIL among safety goals of the item
Confirmation review of the validation plan (see ISO°26262-4, Clause 5) -independent from the developers of the item / project management	I0	I1	I2	I2	highest ASIL among safety goals of the item
Confirmation review of the safety analyses (FMEA, FTA): (see ISO°26262-9, 8.4.8)	I1	I1	I2	I3	highest ASIL among safety goals of the item
Confirmation review of the qualification of software tools (see ISO°26262-8, Clause 11) - independent from the person performing the qualification of the software tool	-	I0	I1	I1	highest ASIL among safety goals of the item
Confirmation review of the proven in use arguments (analysis, data and credit), of the candidates. See ISO°26262-8, Clause 14. -independent from the supplier of the argument	I0	I1	I2	I3	ASIL of the safety goal or requirement related to the considered behaviour, or function, of the candidate
Confirmation review of the completeness of the safety case (see 6.4.5) - independent from authors of safety case	I0	I1	I2	I3	highest ASIL among safety goals of the item
Audit of functional safety processes (see 6.4.6) - independent from the persons working in accordance with the processes required for functional safety	-	I0	I2	I3	highest ASIL among safety goals of the item
Functional safety assessment (see 6.4.6.7) -independent from the supplier of the safety case	-	I0	I2	I3	highest ASIL among safety goals of the item

6.4.6.3 The confirmation measures shall be performed in accordance with Table°2.

Table 2 — Types of confirmation measures for ensuring functional safety

	Functional safety audit	Confirmation review	Functional safety assessment
Subject	Implementation of the processes required for functional safety	Work product	Item as described in the item definition (see ISO°26262-3, Clause°5)
Result	Audit report[a]	Confirmation review report[a]	Assessment report on functional safety of the item
Responsibility of the Auditor/Reviewer/ Safety Assessor	Adequate evaluation of the processes against the definition of the activity, referenced or listed in the safety plan.	Adequate evaluation of the compliance of the work product with the respective requirements of ISO°26262	Adequate evaluation of the achieved functional safety level
Timing during lifecycle	During implementation of the required processes	After completion of the corresponding safety activity Completion before product release	Progressively during development, or in a single block Completion before product release
Scope and depth	Determined by the auditor	Planned prior to the review, in accordance with the safety plan	Review of processes and safety measures required for functional safety

[a] can be included in a functional safety assessment report

NOTE 1 If the functional safety assessment is performed by a qualified SPICE assessor, then the functional safety audit and a SPICE assessment can be performed simultaneously. There is sufficient commonality in content between ISO°26262 and SPICE to allow synchronization of the planning, and execution of, for some supporting processes. Otherwise, if synchronized, the certified SPICE assessor can provide feedback to the safety assessor.

NOTE 2 An organization's process definitions can address multiple standards at the same time, e.g., functional safety requirements of ISO°26262 and SPICE. This might help to avoid duplication of work or process inconsistencies. In those cases, organization specific reference lists of process references to ISO°26262 requirements and to SPICE base practices can be provided.

6.4.6.4 The confirmation measures shall be carried out in accordance with Table 1, wherein the notations: -, I0, I1, I2 I3 are defined as:

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

— I0: the confirmation measure should be performed;

— I1: the confirmation measure shall be performed;

— I2: the confirmation measure shall be performed, by a person from a different team, i.e. 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. independent from the relevant department, regarding management, resources, and responsibility for release for production.

NOTE 1 The notations I2 and I3 include the level of independence required for the reviewer.

NOTE2 The relevant department is specified in Table°1.

NOTE3 The absence of a confirmation review in Table°1 does not imply that the associated work product is not generated.

6.4.6.5 The planning of the confirmation measures shall be accepted by the persons that:

— execute the confirmation measures,

— provide the subject to be confirmed, and

— need the results.

6.4.6.6 This requirement applies to ASIL (A), B, C, and D: The results of the confirmation measures shall be added to the safety case.

6.4.6.7 Functional safety assessment

6.4.6.7.1 A functional safety assessment shall be carried out for items, whereof the highest ASIL among the safety goals is ASIL (B), C, or D, in accordance with Table°1**,** Table°2, and the requirements of 6.4.6.7.

6.4.6.7.2 The planning of the functional safety assessment shall be initiated.

NOTE 1 The functional safety assessment plan is refined during the product development, at system level. See also ISO°26262-4, Clause 5.

NOTE 2 The functional safety assessment plan can be included in the confirmation plan, or in the safety plan.

NOTE 3 An example of an agenda for a functional safety assessment is given in Annex°E.

6.4.6.7.3 One or more persons shall be appointed to carry out a functional safety assessment, and they shall provide a judgement of functional safety.

6.4.6.7.4 The person(s) appointed to conduct the functional safety assessment shall have access to, and shall be supported by, the persons and organizational entities that carry out safety activities during the item development.

6.4.6.7.5 The person(s) appointed to conduct the functional safety assessment shall have access to the relevant information and tools.

6.4.6.7.6 The scope of the functional safety assessment shall include the work products of ISO°26262, the processes required for functional safety, and a general review of safety measures.

NOTE 1 Measures for production cannot be assessed at the end of the development. These measures are re-assessed when production processes are established and the capability of these processes is proven.

NOTE 2 The evaluation of the processes, required for functional safety, can be based on the results of the functional safety audit.

6.4.6.7.7 The functional safety assessment shall consider:

a) the confirmation plan;

b) the recommendations from the previous functional safety assessment, if available; and

c) the results from the functional safety audits and the confirmation reviews.

6.4.6.7.8 The conclusion of the functional safety assessment shall include a recommendation for acceptance, conditional acceptance, or rejection of the functional safety of the item, and

a) conditional acceptance shall only be given, if the functional safety of the item is considered evident, despite the identified open issues. In this case, the corrective actions, listed in the functional safety assessment report, should be carried out.

NOTE In the case of conditional acceptance, the recommendation records the deviations from the functional safety assessment criteria, including the rationale as to why the deviation was considered acceptable.

b) in the case of rejection, adequate corrective actions shall be initiated and the functional safety assessment shall be repeated.

6.5 Work products

6.5.1 **Safety plan**, as a result of 6.4.3.

6.5.2 **Overall project plan (refined)**, as a result of 6.4.3.3.

6.5.3 **Safety case**, as a result of 6.4.5.

6.5.4 **Results of the confirmation measures**, as a result of 6.4.6.

6.5.5 **Confirmation plan**, as a result of 6.4.6.1.

6.5.6 **Functional safety assessment plan**, as a result of 6.4.6.7.2.

7 Safety management after release for production

7.1 Objectives

The objective of this clause is to define the responsibilities of the organizations and persons responsible for functional safety after release for production. This relates to the general activities for ensuring the required functional safety of the item during the lifecycle phases after release for production.

7.2 General

See Clause 5.2.

7.3 Inputs to this Clause

7.3.1 Prerequisites

The following information shall be available:

Evidence of an operational E/E quality management system, conforming to the requirements of this part of ISO°26262 (see 5.5.3).

7.3.2 Further supporting information

None.

7.4 Requirements and recommendations

7.4.1 General

The requirements 7.4.2 to 7.4.6 shall apply to items that have at least 1 safety goal with an ASIL A, B, C or D, and shall apply to all the involved organizations.

7.4.2 The activities for ensuring the functional safety after the item's release for production shall be planned, in accordance with ISO°26262-7, and shall be initiated during system development.

7.4.3 The organization shall institute, execute and maintain processes in order to maintain the functional safety of the item in the lifecycle phases after release for production.

7.4.4 The organization shall appoint persons with the responsibility, and the authority, to maintain the functional safety of the item after release for production.

7.4.5 The organization shall institute, execute and maintain a field monitoring process with respect to functional safety.

NOTE 1 The field monitoring process includes the reporting, and the correcting actions, concerning safety incidents, including the processes for decisions and measures e.g. a recall.

NOTE 2 The data collected from field monitoring can be used for proven in use arguments.

7.4.6 If the item changes after release for production, the release for production shall be reissued.

NOTE These changes are subject to change management, in accordance with ISO°26262-8, Clause°8 (see also 6.4.5.4).

7.5 Work products

Evidence of a field monitoring process, as a result of 7.4.5.

Annex A
(informative)

Overview on and document flow of management of functional safety

Table A.1 provides an overview on objectives, prerequisites and work products of the particular phases of the management of functional safety.

Table A.1 — Management of functional safety: overview

Clause	Title	Objectives	Prerequisites	Work products
5	Overall safety management	The objective of this clause is to define the requirements on the organizations that are responsible for the safety lifecycle, or that perform safety activities in the item's safety lifecycle. This clause serves as a prerequisite to all the activities, in the item's safety lifecycle.	None	5.5.1 Organization specific rules and processes for functional safety. 5.5.2 Evidence that the persons assigned to carry out activities provided by ISO°26262 have a sufficient level of skills, competences and qualification. 5.5.3 Evidence of an operational E/E quality management system, conforming to the requirements of this part of ISO°26262.
6	Safety management during development of the item	The first objective of this clause is to define the safety management roles and responsibilities, regarding the development phases in the safety item's lifecycle. The second objective of this clause is to define the requirements on the safety management during the development phases, including the planning of the safety activities, the application of the safety lifecycle, the creation of the safety case, and the confirmation measures.	Organization specific rules and processes for functional safety (see 5.5.1) Evidence that the persons assigned to carry out activities provided by ISO°26262 have a sufficient level of skills, competences and qualification (see 5.5.2) Evidence of an operational E/E quality management system, conforming to the requirements of this part of ISO°26262 (see 5.5.3)	6.5.1 Safety plan. 6.5.2 Overall project plan (refined). 6.5.3 Safety case. 6.5.4.Results of confirmation measures 6.5.5 Confirmation plan. 6.5.6 Functional safety assessment plan.
7	Safety management after release for production	The objective of this Clause is to define the responsibilities of the organizations and persons responsible for functional safety after release for production. This relates to the general activities for ensuring the required functional safety of the item during the lifecycle phases after release for production.	Evidence of an operational E/E quality management system, confirming to the requirements of this part of ISO°26262 (see 5.5.3).	7.5 Evidence of a field monitoring process.

Annex B
(informative)

Examples of leading and trailing indicators of a safety culture

Table B.1 — Examples of leading indicators of a safety culture

Examples of an unacceptable level	Examples indicative of a good safety culture
Accountability is not traceable	1. The process assures the accountability for effective achievement of functional safety
The reward system favours cost and schedule over safety and quality	2. The reward system supports and motivates the effective achievement of functional safety. 2.1. It penalises those who take shortcuts that jeopardise safety or quality.
Personnel assessing safety, quality, and their governing processes are influenced unduly by those responsible for execution.	3. The process provides adequate checks and balances, e.g., the appropriate degree of independence in the integral processes (safety, quality, verification & validation, and configuration management).
— Group Think. — "Stacking the deck" when forming review groups. — Dissenter is ostracised or labelled as "not a team player". — Dissent reflects negatively on performance reviews.	4. The process uses diversity to advantage. 4.1. Intellectual diversity is sought, valued, and integrated in all processes. 4.2. Counter-behaviour is discouraged and penalised.
— Heavy dependence on testing at the end of the product development cycle. — Management reacts only when there is a problem in the field.	5. Safety and quality issues are discovered and resolved from the earliest stage in the product lifecycle.
— "Minority dissenter" is labelled or treated as "troublemaker" or "not a team player" or "whistleblower." — Concerned employees fear repercussion.	6. Supporting communication and decision-making channels exist and the management encourages their usage 6.1. Self-disclosure is encouraged 6.2. Disclosure of discovery by anyone else is encouraged 6.3. The discovery and resolution process continues in the field
The required resources are not planned or allocated in a timely manner.	7. The required resources are allocated. 7.1. Skilled resources have the competence commensurate to the activity assigned.
No systematised continuous improvement processes or learning cycles or other forms of "lessons learned".	8. Continuous improvement is integral to all processes.

Table B.2 — Examples of trailing indicators of a safety culture

Behaviours indicating unacceptable level	Behaviours indicative of a good safety culture
Cost and schedule always take precedence over safety and quality	1. Safety is the highest priority
Processes are "ad hoc" or implicit.	2. A defined, documented, disciplined process is followed at all levels: 2.1. Management 2.2. Engineering 2.3. Procurement 2.4. Verification 2.5. Validation 2.6. Functional Safety audit 2.7. Functional safety assessment