INTERNATIONAL STANDARD

ISO 26262-10

First edition
2012-08-01

Road vehicles — Functional safety —

Part 10: Guideline on ISO 26262

Véhicules routiers — Sécurité fonctionnelle —

Partie 10: Lignes directrices relatives à l'ISO 26262

Reference number
ISO 26262-10:2012(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

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

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 26262-10 was prepared by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee SC 3, *Electrical and electronic equipment*.

ISO 26262 consists of the following parts, under the general title *Road vehicles — Functional safety*:

- *Part 1: Vocabulary*
- *Part 2: Management of functional safety*
- *Part 3: Concept phase*
- *Part 4: Product development at the system level*
- *Part 5: Product development at the hardware level*
- *Part 6: Product development at the software level*
- *Part 7: Production and operation*
- *Part 8: Supporting processes*
- *Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses*
- *Part 10: Guideline on ISO 26262*

Introduction

ISO 26262 is the adaptation of IEC 61508 to comply with needs specific to the application sector of electrical and/or electronic (E/E) systems within road vehicles.

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

Safety is one of the key issues of future automobile development. New functionalities not only in areas such as driver assistance, propulsion, in vehicle dynamics control and active and passive safety systems increasingly touch the domain of system safety engineering. Development and integration of these functionalities will strengthen the need for safe system development processes and the need to provide evidence that all reasonable system safety objectives are satisfied.

With the trend of increasing technological complexity, software content and mechatronic implementation, there are increasing risks from systematic failures and random hardware failures. ISO 26262 includes guidance to avoid these risks by providing appropriate requirements and processes.

System safety is achieved through a number of safety measures, which are implemented in a variety of technologies (e.g. mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic) and applied at the various levels of the development process. Although ISO 26262 is concerned with functional safety of E/E systems, it provides a framework within which safety-related systems based on other technologies can be considered. ISO 26262:

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

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

c) uses ASILs to specify applicable requirements of ISO 26262 so as to avoid unreasonable residual risk;

d) provides requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety being achieved;

e) provides requirements for relations with suppliers.

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

Safety issues are intertwined with common function-oriented and quality-oriented development activities and work products. ISO 26262 addresses the safety-related aspects of development activities and work products.

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

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

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

EXAMPLE “2-6” represents Clause 6 of ISO 26262-2.

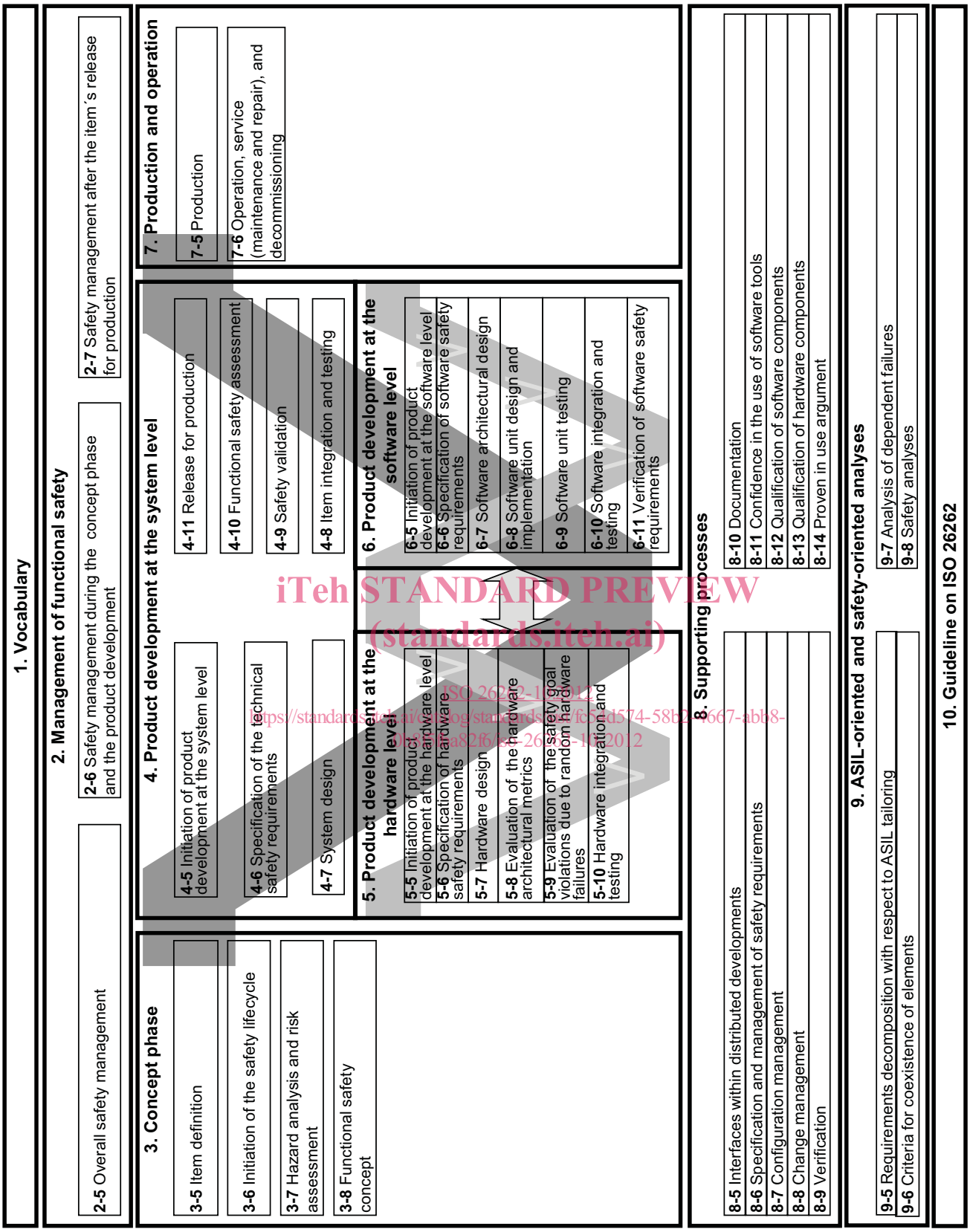


Figure 1 — Overview of ISO 26262

Road vehicles — Functional safety —

Part 10:
Guideline on ISO 26262

1 Scope

ISO 26262 is intended to be applied to safety-related systems that include one or more electrical and/or electronic (E/E) systems and that are installed in series production passenger cars with a maximum gross vehicle mass up to 3 500 kg. ISO 26262 does not address unique E/E systems in special purpose vehicles such as vehicles designed for drivers with disabilities.

Systems and their components released for production, or systems and their components already under development prior to the publication date of ISO 26262, are exempted from the scope. For further development or alterations based on systems and their components released for production prior to the publication of ISO 26262, only the modifications will be developed in accordance with ISO 26262.

ISO 26262 addresses possible hazards caused by malfunctioning behaviour of E/E safety-related systems, including interaction of these systems. It does not address hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy and similar hazards, unless directly caused by malfunctioning behaviour of E/E safety-related systems.

ISO 26262 does not address the nominal performance of E/E systems, even if dedicated functional performance standards exist for these systems (e.g. active and passive safety systems, brake systems, Adaptive Cruise Control).

This part of ISO 26262 provides an overview of ISO 26262, as well as giving additional explanations, and is intended to enhance the understanding of the other parts of ISO 26262. It has an informative character only and describes the general concepts of ISO 26262 in order to facilitate comprehension. The explanation expands from general concepts to specific contents.

In the case of inconsistencies between this part of ISO 26262 and another part of ISO 26262, the requirements, recommendations and information specified in the other part of ISO 26262 apply.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 26262-1:2011, *Road vehicles — Functional safety — Part 1: Vocabulary*

ISO 26262-2:2011, *Road vehicles — Functional safety — Part 2: Management of functional safety*

ISO 26262-3:2011, *Road vehicles — Functional safety — Part 3: Concept phase*

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

ISO 26262-5:2011, *Road vehicles — Functional safety — Part 5: Product development at the hardware level*

ISO 26262-6:2011, *Road vehicles — Functional safety — Part 6: Product development at the software level*

ISO 26262-7:2011, *Road vehicles — Functional safety — Part 7: Production and operation*

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

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

3 Terms, definitions and abbreviated terms

For the purposes of this document, the terms, definitions and abbreviated terms given in ISO 26262-1:2011 apply.

4 Key concepts of ISO 26262

4.1 Functional safety for automotive systems (relationship with IEC 61508)

IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems*, is designated by IEC as a generic standard and a basic safety publication. This means that industry sectors will base their own standards for functional safety on the requirements of IEC 61508.

In the automotive industry, there are a number of issues with applying IEC 61508 directly. Some of these issues and corresponding differences in ISO 26262 are described below.

IEC 61508 is based upon the model of “equipment under control”, for example an industrial plant that has an associated control system as follows:

a) A hazard analysis identifies the hazards associated with the equipment under control (including the equipment control system), to which risk reduction measures will be applied. This can be achieved through E/E/PE systems, or other technology safety-related systems (e.g. a safety valve), or external measures (e.g. a physical containment of the plant). ISO 26262 contains a normative automotive scheme for hazard classification based on severity, probability of exposure and controllability.

b) Risk reduction allocated to E/E/PE systems is achieved through safety functions, which are designated as such. These safety functions are either part of a separate protection system or can be incorporated into the plant control. It is not always possible to make this distinction in automotive systems. The safety of a vehicle depends on the behaviour of the control systems themselves.

ISO 26262 uses the concept of safety goals and a safety concept as follows:

— a hazard analysis and risk assessment identifies hazards and hazardous events that need to be prevented, mitigated or controlled;

— a safety goal is formulated for each hazardous event;

— an Automotive Safety Integrity Level (ASIL) is associated with each safety goal;

— the functional safety concept is a statement of the functionality to achieve the safety goal(s);

— the technical safety concept is a statement of how this functionality is implemented on the system level by hardware and software; and

— software safety requirements and hardware safety requirements state the specific safety requirements which will be implemented as part of the software and hardware design.

EXAMPLE

— The airbag system: one of the hazards is unintended deployment.

— An associated safety goal is that the airbag does not deploy unless a crash occurs that requires the deployment.

— The functional safety concept can specify a redundant function to detect whether the vehicle is in a collision.

— The technical safety concept can specify the implementation of two independent accelerometers with different axial orientations and two independent firing circuits. The squib deploys if both are closed.

IEC 61508 is aimed at singular or low volume systems. The system is built and tested, then installed on the plant, and then safety validation is performed. For mass-market systems such as road vehicles, safety validation is performed before the release for volume (series) production. Therefore, the order of lifecycle activities in ISO 26262 is different. Related to this, ISO 26262-7 addresses requirements for production. These are not covered in IEC 61508.

IEC 61508 does not address specific requirements for managing development across multiple organizations and supply chains, whereas ISO 26262 addresses explicitly the issue, including the Development Interface Agreement (DIA) [see ISO 26262-8:2011, Clause 5 (Interfaces within distributed developments)], because automotive systems are produced by one or more suppliers of the customer, e.g. the vehicle manufacturer, the supplier of the customer, or the customer.

IEC 61508 does not contain normative requirements for hazard classification. ISO 26262 contains an automotive scheme for hazard classification. This scheme recognizes that a hazard in an automotive system does not necessarily lead to an accident. The outcome will depend on whether the persons at risk are actually exposed to the hazard in the situation in which it occurs, and whether they are able to take steps to control the outcome of the hazard. An example of this concept applied to a failure which affects the controllability of a moving vehicle is given in Figure 2.

NOTE This concept is intended only to demonstrate that there is not necessarily a direct correlation between a failure occurring and the accident. It is not a representation of the hazard analysis and risk assessment process, although the parameters evaluated in this process are related to the probabilities of the state transitions shown in the figure.

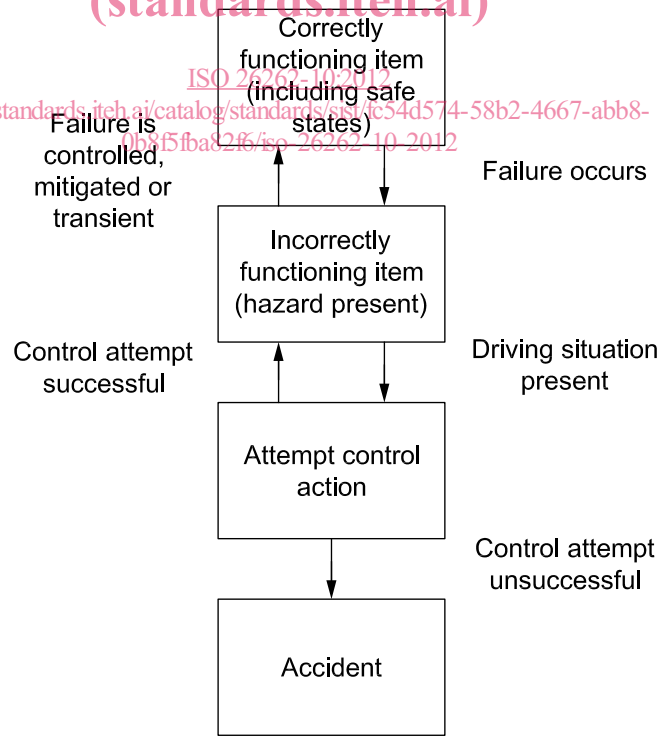


Figure 2 — State machine model of automotive risk

The requirements for hardware development (ISO 26262-5) and software development (ISO 26262-6) are adapted for the state-of-the-art in the automotive industry. Specifically, ISO 26262-6 contains requirements concerned with model-based development; IEC 61508 prescribes the application of specific methods. A detailed rationale for the use of any alternative method has to be provided. For the methods listed in

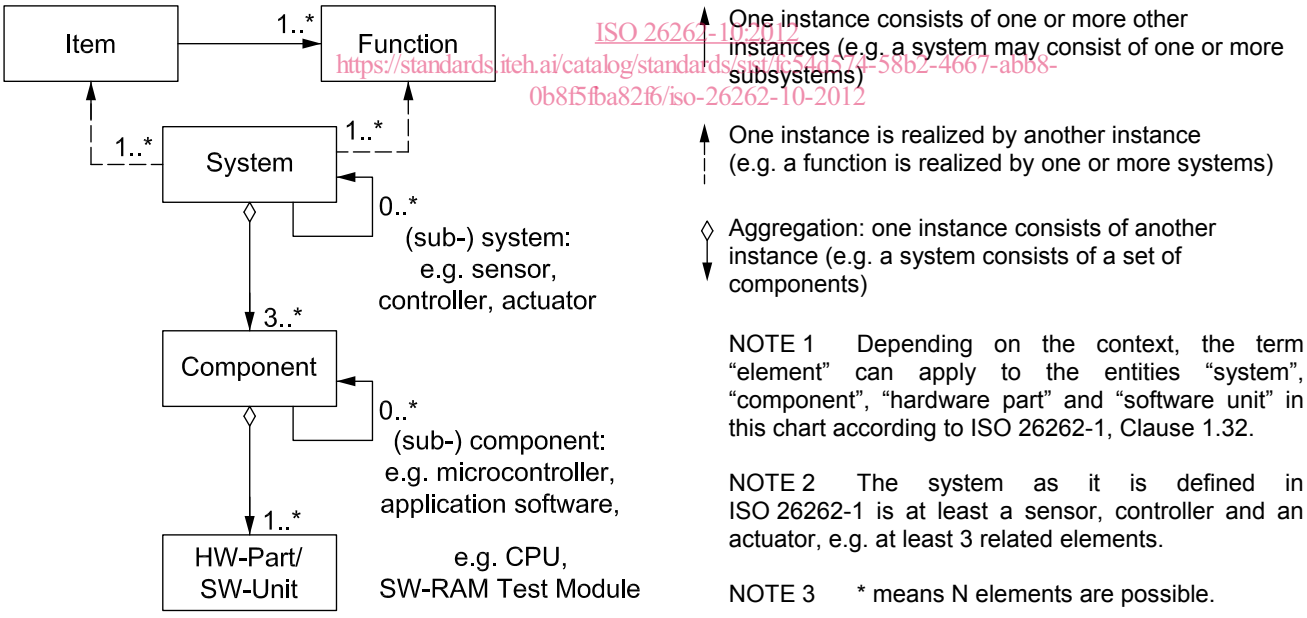
ISO 26262, specific goals are provided. To achieve these goals, the provided methods can be applied, or a rationale that alternative methods can also achieve the goal is provided.

Safety requirements in ISO 26262 are assigned an ASIL (Automotive Safety Integrity Level) rather than a SIL (Safety Integrity Level). The main motivation for this is that the SIL in IEC 61508 is stated in probabilistic terms (see IEC 61508-1:2010, Table 3). IEC 61508 states: "It is accepted that only with respect to the hardware safety integrity will it be possible to quantify and apply reliability prediction techniques in assessing whether the target failure measures have been met. Qualitative techniques and judgements have to be made with respect to the precautions necessary to meet the target failure measures with respect to the systematic safety integrity." An ASIL is not based on this probabilistic requirement concerning the occurrence of the hazard; however, there are probabilistic targets associated with compliance to the requirements of an ASIL.

4.2 Item, system, element, component, hardware part and software unit

The terms item, system, element, component, hardware part, and software unit are defined in ISO 26262-1. Figure 3 shows the relationship of item, system, component, hardware part and software unit. Figure 4 shows an example of item dissolution. A divisible element can be labelled as a system, a subsystem or a component. A divisible element that meets the criteria of a system can be labelled as a system or subsystem. The term subsystem is used when it is important to emphasize that the element is part of a larger system. A component is a non-system-level, logically and technically separable element. Often the term component is applied to an element that is only comprised of parts and units, but can also be applied to an element comprised of lower-level elements from a specific technology area, e.g. electrical/electronic technology (see Figure 4).

EXAMPLE In the case of a microcontroller or ASIC, the following partitioning can be used: the whole microcontroller is a component, the processing unit (e.g. a CPU) is a part, the registers inside the processing unit (e.g. the CPU register bank) is a sub-part. In the case of microcontroller (MCU) analyses, a higher level of detail in the partitioning could be needed; to aid in this purpose, it is possible to partition a part into sub-parts which can be further divided into basic/elementary sub-parts.



NOTE 1 Depending on the context, the term “element” can apply to the entities “system”, “component”, “hardware part” and “software unit” in this chart according to ISO 26262-1, Clause 1.32.

NOTE 2 The system as it is defined in ISO 26262-1 is at least a sensor, controller and an actuator, e.g. at least 3 related elements.

NOTE 3 * means N elements are possible.

Figure 3 — Relationship of item, system, component, hardware part and software unit

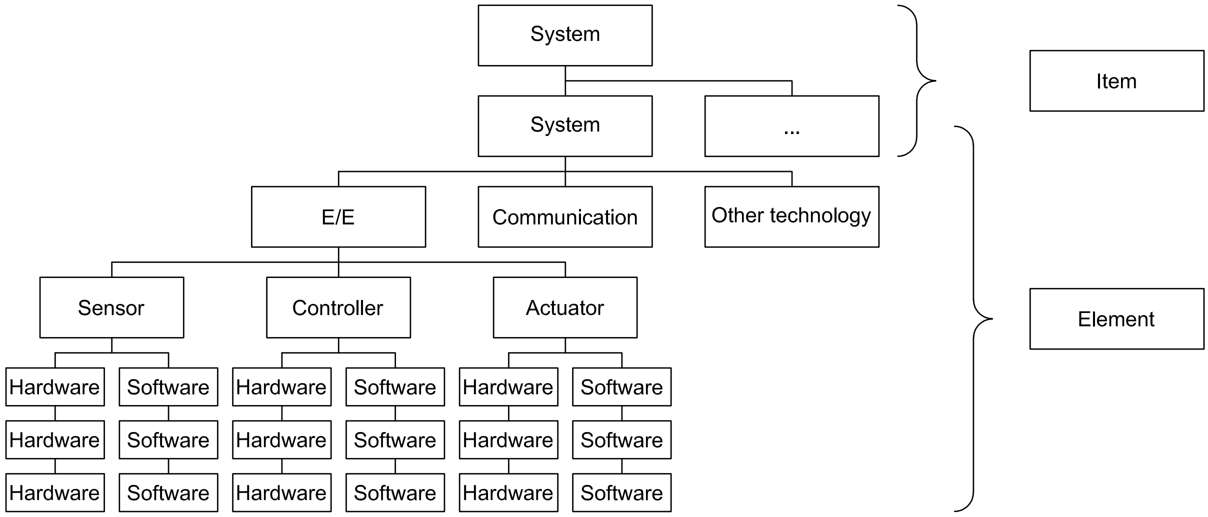


Figure 4 — Example item dissolution

4.3 Relationship between faults, errors and failures

The terms fault, error and failure are defined in ISO 26262-1. Figure 5 depicts the progression of faults to errors to failures from three different types of causes: systematic software issues, random hardware issues and systematic hardware issues. Systematic faults (see ISO 26262-1) are due to design or specifications issues; software faults and a subset of hardware faults are systematic. Random hardware faults (see ISO 26262-1) are due to physical processes such as wear-out, physical degradation or environmental stress. At the component level, each different type of fault can lead to different failures. However, failures at the component level are faults at the item level. Note that in this example, at the vehicle level, faults from different causes can lead to the same failure. A subset of failures at the item level will be hazards (see ISO 26262-1) if additional environmental factors permit the failure to contribute to an accident scenario.

EXAMPLE If unexpected behaviour of the vehicle occurs while the vehicle is starting to cross an intersection, a crash can occur, e.g. the risk of the hazardous event "vehicle bucking when starting to cross intersection" is assessed for severity, exposure and controllability ("bucking" refers to making sudden jerky movements).

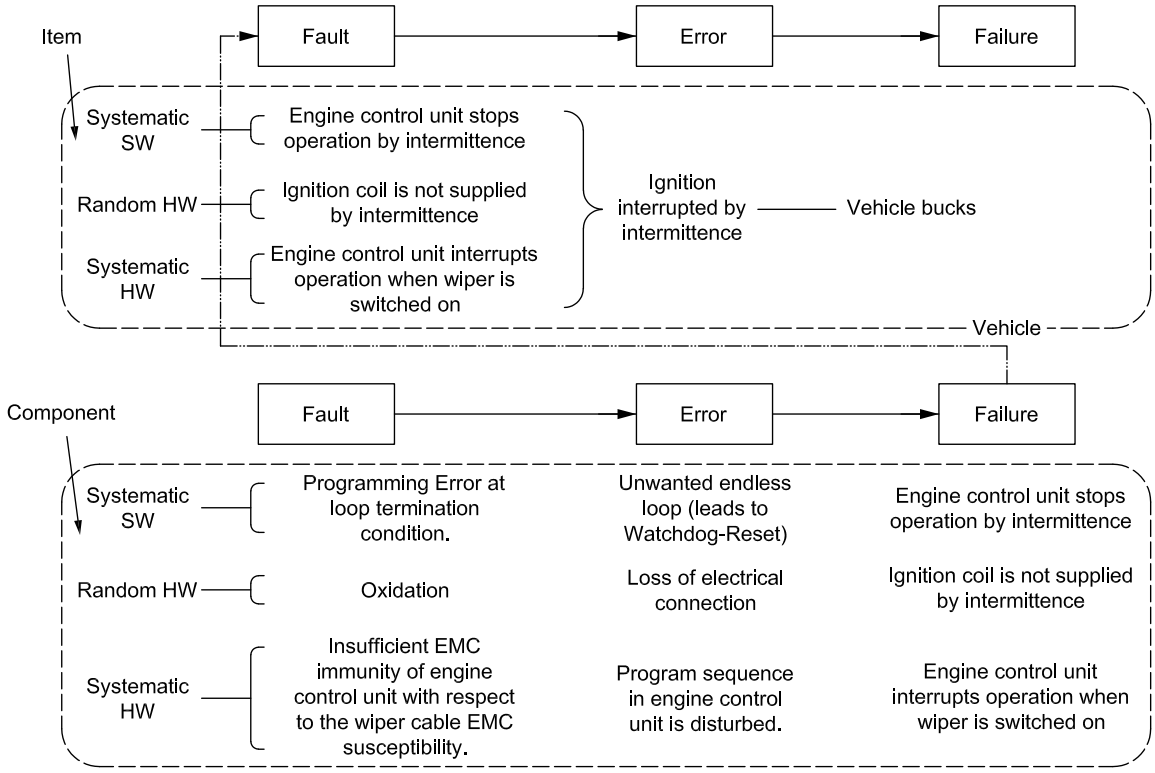


Figure 5 — Example of faults leading to failures

5 Selected topics regarding safety management

5.1 Work product

This subclause describes the term "work product".

A work product is the result of meeting the corresponding requirements of ISO 26262 (see ISO 26262-1). Therefore, a documented work product can provide evidence of compliance with these safety requirements.

EXAMPLE A requirements specification is a work product that can be documented by means of a requirements database or a text file. An executable model is a work product that can be represented by modelling language files that can be executed, e.g. for simulation purposes by using a software tool.

The documentation of a work product [see ISO 26262-8:2011, Clause 10 (Documentation)] serves as a record of the executed safety activities, safety requirements or of related information. Such documentation is not restricted to any form or medium.

EXAMPLE The documentation of a work product can be represented by electronic or paper files, by a single document or a set of documents. It can be combined with the documentation of other work products or with documentation not directly dedicated to functional safety.

To avoid the duplication of information, cross-references within or between documentation can be used.

5.2 Confirmation measures

5.2.1 General

In ISO 26262, specified work products are evaluated during subsequent activities, either as part of the confirmation measures or as part of the verification activities. This subclause describes the difference between verification and confirmation measures.

On the one hand, the verification activities are performed to determine the completeness and correct specification, or implementation, of safety requirements. The verification of work products can include:

— verification reviews to verify the specification, or implementation, of derived safety requirements against the safety requirements at a higher level, regarding completeness and correctness; or

— the execution of test cases or the examination of test results to provide evidence of the fulfilment of specified safety requirements, by exercising the item or its element(s).

The verification activities are specified in ISO 26262-3, ISO 26262-4, ISO 26262-5 and ISO 26262-6. Furthermore, generic requirements regarding the verification activities in ISO 26262 are specified in ISO 26262-8:2011, Clause 9 (Verification), and further details specific to the verification of safety requirements are specified in ISO 26262-8:2011, Clause 6 (Specification and management of safety requirements).

On the other hand, the confirmation measures are performed to evaluate the item's achievement of functional safety, including a confirmation of:

— the proper definition, tailoring and execution of the safety activities performed during the item development and of the implemented safety processes, with regard to the ISO 26262 requirements; and

— the proper content of the work products with regard to the corresponding ISO 26262 requirements.

The confirmation measures are specified in ISO 26262-2:2011, Clause 6 (Safety management during the concept phase and the product development).

EXAMPLE If an ASIL decomposition is applied during the system design phase:

— the verification of the resulting system design is performed against the technical safety concept (see ISO 26262-4:2011, 7.4.8); and

— the confirmation of the correct application of the ASIL decomposition can be performed as part of a functional safety assessment, with regard to ISO 26262-9:2011, Clause 5 (Requirements decomposition with respect to ASIL tailoring), including the confirmation that a dependent failure analysis has been performed and justifies the claim of sufficient independence between the elements that implement the corresponding redundant safety requirements.

5.2.2 Functional safety assessment

If the highest ASIL of the item's safety goals is ASIL C or D, a functional safety assessment is performed to evaluate an item's achievement of functional safety. In ISO 26262-2, certain aspects of a functional safety assessment are described separately, i.e. the functional safety audit and the confirmation reviews.

A functional safety assessment includes:

a) a review of the appropriateness and effectiveness of the implemented safety measures that can be assessed during the item development;

b) an evaluation of the work products that are required by the safety plan. The review of selected work products is emphasised. These are coined as confirmation reviews and aim to confirm the compliance of such work products with the corresponding requirements of ISO 26262; and

c) one or more functional safety audits to evaluate the implementation of the processes required for functional safety.

A functional safety assessment can be repeated or updated.

EXAMPLE 1 A functional safety assessment update because of a change of the item, or element(s) of the item, that is identified by the change management as having an impact on the functional safety of the item [see ISO 26262-8:2011, Clause 8 (Change management)].

EXAMPLE 2 An iteration of a functional safety assessment triggered by the follow-up of a functional safety assessment report that included a recommendation for a conditional acceptance or rejection of the item's functional safety. In this case, the iteration includes a follow-up of the recommendations resulting from the previous functional safety assessment(s), including an evaluation of the performed corrective actions, if applicable.

If the highest ASIL of the item's safety goals is ASIL B, a functional safety assessment can be omitted or performed less rigorously. However, even if the functional safety assessment is not performed, other confirmation measures are still performed, i.e. the confirmation reviews of the hazard analysis and risk assessment, the safety plan, the item integration and testing plan, the validation plan, the applicable safety analyses, the proven in use arguments (if applicable), and the completeness of the safety case (see ISO 26262-2:2011, Table 1).

If the highest ASIL of the item's safety goals is ASIL A, there is no requirement or recommendation in ISO 26262 for or against performing a functional safety assessment. However, confirmation reviews of the hazard analysis and risk assessment and of the applicable safety analyses are still performed.

In the case of a distributed development, the scope of a functional assessment includes the work products generated, and the processes and safety measures implemented, by a vehicle manufacturer and the suppliers in the item's supply chain [see ISO 26262-2 and ISO 26262-8:2011, Clause 5 (Interfaces within distributed developments)].

The purpose of a functional safety assessment is to evaluate an item's achievement of functional safety, which is only possible at the item level. Therefore, a functional safety assessment at the premises of a supplier (that develops elements of the item) refers only to an assessment with a limited scope, which essentially serves as an input for the subsequent functional safety assessment activities (at the customer level). As the final customer in the item development, the vehicle manufacturer appoints person(s) to perform a functional safety assessment in its full scope, so as to judge an item's achievement of functional safety. This judgement includes providing a recommendation for acceptance, conditional acceptance, or rejection of the item's functional safety.

NOTE For the case where a Tier 1 supplier is responsible for the item development including vehicle integration, this supplier takes over the aforementioned role of the vehicle manufacturer.

In a practical manner, a functional safety assessment in the case of a distributed development can thus be broken down into:

— functional safety assessments with a limited scope at the supplier's premises, concerning the suppliers in the supply chain. The applicable ASIL is the highest inherited ASIL (of the item's safety goals) across the elements, of the item, that are developed by the supplier (see also ISO 26262-8:2011, 5.4.5); and

— a final functional safety assessment that includes a judgement of the functional safety achieved by the integrated item, e.g. performed by the vehicle manufacturer. The applicable ASIL is the highest ASIL of the item's safety goals (see also ISO 26262-2).

EXAMPLE A vehicle manufacturer develops an item with an ASIL D Safety Goal (SG1) and an ASIL A Safety Goal (SG2), and will perform a functional safety assessment regarding this item. It is possible that, for example, a Tier 2 or Tier 3 supplier only develops ASIL A elements of the item, i.e. only elements that inherit the ASIL of SG2 [however, refer to ISO 26262-9:2011, Clause 6 (Criteria for coexistence of elements), if applicable]. There is no requirement or recommendation (for or against) in ISO 26262 to perform a functional safety assessment at this supplier's premises regarding this item development.

The scope, procedure (e.g. work products to be made available by the supplier, work products to be reviewed by the customer) and execution of a functional safety assessment concerning the interface between a customer and a supplier are specified in the corresponding Development Interface Agreement [see ISO 26262-8:2011, Clause 5 (Interfaces within distributed developments)].

EXAMPLE DIA between a vehicle manufacturer (customer) and a Tier 1 supplier. DIA between a Tier 1 supplier (customer) and a Tier 2 supplier.

A possible manner to perform a functional safety assessment in the case of a distributed development is that the vehicle manufacturer and the suppliers in the supply chain each address those aspects of the assessment activities [see bullets a), b) and c) above] for which the respective party is responsible for, as follows:

— a supplier reviews the safety measures implemented in the developed elements including their appropriateness and effectiveness to comply with the corresponding safety goals or safety requirements (provided by the customer or developed by the supplier), and evaluates its implemented processes and the applicable work products. A supplier also evaluates the potential impacts of the developed elements on the item's functional safety, e.g. identifies whether implemented safety measures can lead to new hazards; and

— the vehicle manufacturer evaluates the functional safety of the integrated item. A part of the evaluation can be based on the work products or information provided by one or more suppliers, including reports of the functional safety assessments performed at supplier's premises.

NOTE A customer can evaluate the safety measures implemented by a supplier and the work products made available by a supplier. A customer can also evaluate the processes implemented by a supplier at the supplier's premises (see ISO 26262-8:2011, 5.4.4.8)

5.3 Understanding of safety cases

5.3.1 Interpretation of safety cases

The purpose of a safety case is to provide a clear, comprehensive and defensible argument, supported by evidence, that an item is free from unreasonable risk when operated in an intended context.

The guidance given here focuses on the scope of ISO 26262.

There are three principal elements of a safety case, namely:

— the requirements;

— the argument; and

— the evidence, i.e. ISO 26262 work products.

The relationship between these three elements, in the context of ISO 26262, is depicted in Figure 6.

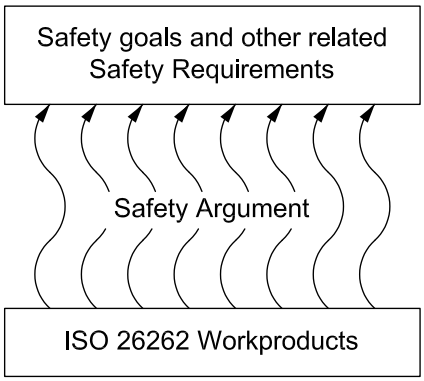


Figure 6 — Key elements of a safety case (see [2])

The safety argument communicates the relationship between the evidence and the objectives. The role of the safety argument is often neglected. It is possible to present many pages of supporting evidence without clearly explaining how this evidence relates to the safety objectives. Both the argument and the evidence are crucial elements of the safety case and go hand-in-hand. An argument without supporting evidence is unfounded, and therefore unconvincing. Evidence without an argument is unexplained, resulting in a lack of clarity as to