DRAFT INTERNATIONAL STANDARD ISO/DIS 26262-1

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

Voting begins on:
2009-07-08

Voting terminates on:
2009-12-08

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

Road vehicles — Functional safety —

Part 1: **Vocabulary**

Véhicules routiers — Sécurité fonctionnelle —

Partie 1: Vocabulaire

ICS 01.040.43; 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.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

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 26262-1 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.

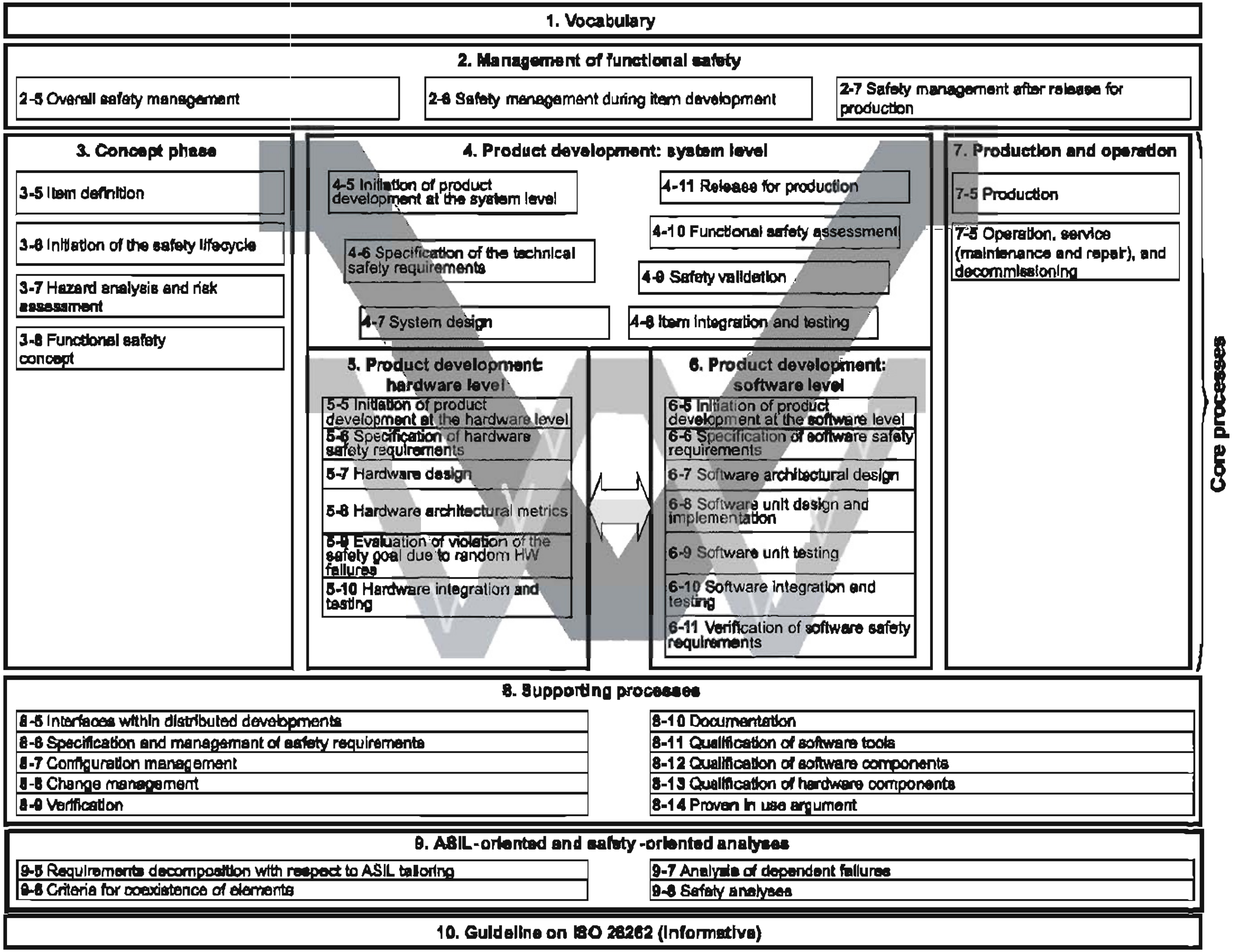
1. Vocabulary
2. Management of functional safety
2-5 Overall safety management
2-6 Safety management during item development
2-7 Safety management after release for production
3. Concept phase
3-5 Item definition
3-6 Initiation of the safety lifecycle
3-7 Hazard analysis and risk assessment
3-8 Functional safety concept
4. Product development: system level
4-5 Initiation of product development at the system level
4-6 Specification of the technical safety requirements
4-7 System design
4-8 Item integration and testing
4-9 Safety validation
4-10 Functional safety assessment
4-11 Release for production
7. Production and operation
7-5 Production
7-6 Operation, service (maintenance and repair), and decommissioning
5. Product development: hardware level
5-5 Initiation of product development at the hardware level
5-6 Specification of hardware safety requirements
5-7 Hardware design
5-8 Hardware architectural metrics
5-9 Evaluation of violation of the safety goal due to random HW failures
5-10 Hardware integration and testing
6. Product development: software level
6-5 Initiation of product development at the software level
6-6 Specification of software safety requirements
6-7 Software architectural design
6-8 Software unit design and implementation
6-9 Software unit testing
6-10 Software integration and testing
6-11 Verification of software safety requirements
Core processes
8. Supporting processes
8-5 Interfaces within distributed developments
8-6 Specification and management of safety requirements
8-7 Configuration management
8-8 Change management
8-9 Verification
8-10 Documentation
8-11 Qualification of software tools
8-12 Qualification of software components
8-13 Qualification of hardware components
8-14 Proven in use argument
9. ASIL-oriented and safety-oriented analyses
9-5 Requirements decomposition with respect to ASIL tailoring
9-6 Criteria for coexistence of elements
9-7 Analysis of dependent failures
9-8 Safety analyses
10. Guideline on ISO 26262 (informative)

Figure 1 — Overview of ISO 26262

DRAFT INTERNATIONAL STANDARD ISO/DIS 26262-1

Road vehicles — Functional safety — Part 1: Vocabulary

Scope

ISO 26262 is intended to be applied to safety-related systems that include one or more E/E systems and that are installed in series production passenger cars with a max gross weight up to 3,5 t. ISO 26262 does not address unique E/E systems in special purpose vehicles such as vehicles designed for drivers with disabilities. Systems developed prior to the publication date of ISO 26262 are exempted from the scope.

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

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

This part of the International Standard specifies the terms, definitions and abbreviated terms for application in all parts of ISO°26262.

1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

1.1 allocation

assignment of all or part of a requirement to architectural elements

NOTE Intent is not to divide an atomic requirement into multiple requirements. Tracing of an atomic system level requirement to multiple lower level atomic requirements is allowed.

EXAMPLE allocation of system time between hardware and software components

1.2 anomaly

condition that deviates from expectations based on requirements specifications, design documents, user documents, standards, etc., or from someone’s perceptions or experiences

Note: Anomalies might be found during, but not limited to, the review, test, analysis, compilation, or use of software products or applicable documentation.

1.3 architecture

representation of the structure of the item or systems or elements that allows identification of building blocks, their boundaries and interfaces, and includes the allocation of functions to hardware and software elements

1.4 ASIL decomposition

apportioning of safety requirements redundantly to sufficiently independent elements with the objective of reducing the ASIL of the elements

NOTE See ISO 26262-9:-- Clause 5.

1.5 assessment

examination of a characteristic of an item or element

NOTE A level of independence is associated with each assessment.

1.6 audit

examination of implemented process

1.7 Automotive Safety Integrity Level (ASIL)

one of four levels to specify the item's or element's necessary requirements of ISO 26262 and safety measures for avoiding an unreasonable residual risk with D representing the most stringent and A the least stringent level

1.8 availability

capability of a product to be in a state to execute the function required under given conditions, at a certain time or in a given period, supposing the required external resources are available

1.9 baseline

released version of one or more work products, hardware or software items or elements, that is under configuration management and used as a basis for further development through change management process

NOTE see ISO 26262-8:-- Clause 7

1.10 branch coverage

percentage of branches of the control flow that have been executed

NOTE 1 100 % branch coverage implies 100 % statement coverage.

NOTE 2 An if-statement always has 2 branches - condition true and condition false - independent of the existence of an else-clause.

1.11 calibration data

data that will be applied after the software build in the development process

NOTE: Calibration data cannot contain executable or interpretable code.

EXAMPLE Calibration data can include:

- Parameters: e.g. value for low idle speed, engine characteristic diagrams;
- Vehicle specific parameter (adaptation values): e.g. limit stop for throttle valve; and
- Variant coding: e.g. country code, left-hand / right-hand steering

1.12 candidate

item or element whose definition and conditions of use are identical to, or have a very high degree of commonality with, an item or element that is already released and in operation

1.13 cascading failure

failure of an element of an item causing other elements of the same item to fail

NOTE: Cascading failures are dependent failures that are not common cause failures (see Figure 2).

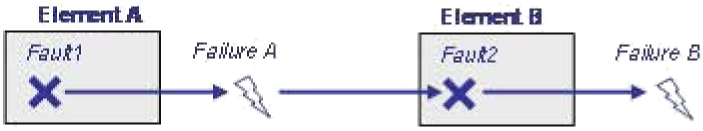

Figure 2 — Cascading failure

1.14 common cause failure (CCF)

failure of two or more elements of an item resulting from a single specific event or root cause

NOTE: Common cause failures are dependent failures that are not cascading failures (see Figure 3).

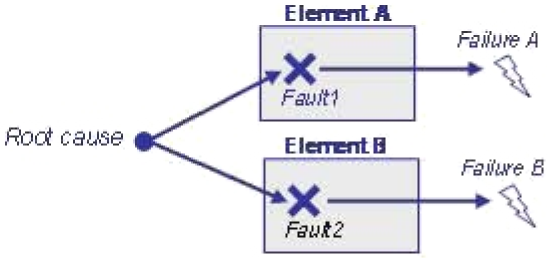

Figure 3 — Common cause failure

1.15 component

non-system level, non-elementary, logically and technically separable element

NOTE: A component is a part of a system and consists of software units or hardware parts.

1.16 configuration data

data that is assigned during software build and controls the software build process

NOTE 1: Configuration data cannot contain executable or interpretable code.

NOTE 2: Configuration data controls the software build. Only code and/or data being selected by configuration data can be included in the executable code.

EXAMPLE: Configuration data can include:

- Pre-processor instructions; and

— Software build scripts (e.g. XML configuration files).

1.17 confirmation measure

confirmation review, audit or assessment concerning functional safety

1.18 confirmation review

confirmation that a work product meets the requirements of ISO 26262 with the required level of independence

NOTE 1 Complete List of confirmation reviews is given in ISO 26262-2.

NOTE 2 The goal of confirmation reviews is compliance with ISO 26262.

1.19 controllability

avoidance of the specified harm or damage through the timely reactions of the persons involved

NOTE: The parameter C in hazard analysis and risk assessment represents the potential for controllability.

1.20 dedicated measures

measures to ensure the failure rate claimed in the evaluation of the probability of violation of safety goals

EXAMPLE: Dedicated measures can include:

a) design features such as hardware part over-design (e.g. electrical or thermal stress rating) or physical separation (e.g. spacing of contacts on a printed circuit board);

b) a special sample test of incoming material to reduce the risk of occurrence of this failure mode;

c) a burn-in test;

d) a dedicated control plan.

1.21 dependent failures

failures whose probability of simultaneous or successive occurrence cannot be expressed as the simple product of the unconditional probabilities of each of them

NOTE 1 Strict mathematical definition gives P (Failure A AND Failure B) $\neq$ P (Failure A) * P (Failure B) where P denotes the probability, but the case where P (Failure A AND Failure B) < P (Failure A) * P (Failure B) is not meaningful in the context of functional safety.

Where:

P (Failure A AND Failure B) is the probability of the simultaneous occurrence of failure a and failure B;

P (Failure A) is the probability of the occurrence of failure A;

P (Failure B) is the probability of the occurrence of failure B.

NOTE 2 Dependent failures include common cause failures and cascading failures.

1.22 degradation

strategy for providing safety by design after the occurrence of failures

NOTE Degradation can include reduced functionality, reduced performance, or both reduced functionality and performance.

1.23 detected fault

fault whose presence is detected by a safety mechanism within a prescribed time

NOTE The fault can be detected by a dedicated safety mechanism (such as a detection of the error and signalling the driver via an alerting device on the instrument panel) as defined in the functional safety concept.

1.24 development interface agreement (DIA)

agreement between customer and supplier in which the responsibilities for activities, evidence, or work products to be exchanged by each party are specified

1.25 diagnostic coverage

proportion of a hardware element failure rate that is covered by the safety mechanisms implemented

NOTE 1 Diagnostic coverage can be assessed with regard to residual faults or with regard to latent multiple point faults that might occur in a hardware element.

NOTE 2 The definition may be represented in terms of the equations given in ISO 26262-5.

NOTE 3 Safety mechanisms implemented at different levels in the architecture can be considered.

1.26 diagnostic test interval

amount of time between the executions of online diagnostic tests of a safety mechanism

1.27 distributed development

development of an item or element with development responsibility divided between customer and supplier for the entire item or element, or for subsystems

NOTE: Customer and supplier are roles of the cooperating parties.

1.28 diversity

different solutions satisfying the same requirement with the aim of independence

EXAMPLE diverse programming or diverse hardware

1.29 dual point failure

failure, resulting from the combination of two independent faults, that leads directly to the violation of a safety goal

NOTE Dual point failures that are addressed in ISO 26262 include at least those where one fault affects a safety-related element and another fault affects the corresponding safety mechanism intended to achieve or maintain a safe state.

1.30 dual point fault

individual fault that, in combination with another independent fault, leads to a dual point failure

NOTE 1 A dual point fault can only be recognized after the identification of dual point failure e.g. from cut set analysis of a fault tree.

NOTE 2 See also **multiple point fault** (1.77).

1.31 E/E system

system that consists of electrical and/or electronic elements, including programmable electronic elements

EXAMPLE E/E systems include power supplies, sensors and other input devices, data highways and other communication paths, actuators and other output devices

1.32 element

system or part of a system including components, hardware, software, hardware part, and software units

1.33 embedded software

fully-integrated software to be executed on a processing element

EXAMPLE Normally the processing element is a micro controller, an FPGA or an ASIC.

1.34 emergency operation

functionality to transition to a safe-state as defined in the fail-safe concept

1.35 emergency operation interval

time-span between the occurrence of a fault and transition to a safe state as defined in the fail-safe concept, in which at least the functionality specified as an emergency operation is supported

1.36 error

discrepancy between a computed, observed or measured value or condition and the true, specified, or theoretically correct value or condition

NOTE 1 An error can arise as a result of unforeseen operating conditions or due to a fault within the system, subsystem or component being considered.

NOTE 2 A fault can manifest itself as an error within the considered element and, at the end of its latency, the error can cause a failure.

1.37 exposure

state of being in an operational situation that can be hazardous if coincident with the failure mode under analysis

1.38 external measure

measure separate and distinct from the item that reduces or mitigates the risks resulting from the item

1.39 failure

termination of the ability of an element or an item to perform a function as required

NOTE 1 Termination is a reduction in, or loss of, ability of an element or an item to perform a function as required.

NOTE 2 There is a difference between “to perform a function as required” (stronger definition, use-oriented) and ”to perform a function as specified”, so a failure can result from an incorrect specification.

1.40 failure mode

manner in which an element or an item fails

1.41 failure rate

density of probability of failure divided by probability of survival for a hardware element

NOTE The failure rate is generally denoted as "λ".

1.42 fault

abnormal condition that can cause an element or an item to fail

1.43 fault model

representation of failure modes resulting from faults

NOTE Fault models are generally based on field experience or reliability handbooks.

1.44 fault reaction time

time-span to perform the specified action necessary to achieve a successful transition to a safe state

1.45 fault tolerant time interval

time-span in which the vehicle function can be stressed with faults before a hazardous event develops

1.46 field data

data obtained from the use of an item or element including cumulative operating hours, all failures and in-service problems

NOTE Field data normally comes from customer use.

1.47 formal notation

description technique that has both its syntax and semantics completely defined

1.48 formal verification

method used to prove the correctness of a system against the formal specification of its required behavior

1.49 freedom from interference

absence of cascading failures between two or more elements that could lead to the violation of a safety requirement

EXAMPLE 1: Element 1 is interference-free of element 2 if no failure of element 2 can cause element 1 to fail.

EXAMPLE 2: Element 3 interferes with element 4 if there exists a failure of element 3 that causes element 4 to fail.

1.50 functional concept

specification of the intended functions and their interactions necessary to achieve the desired behavior

NOTE The functional concept is developed during the concept phase.

1.51 functional safety

absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems

1.52 functional safety concept

specification of the functional safety requirements, with associated information, their assignment to architectural elements, and their interaction necessary to achieve the safety goals

1.53 functional safety requirement

specification of implementation-independent safety behavior, or implementation-independent safety measure, including its safety-related attributes

NOTE 1 A functional safety requirement can be a safety requirement implemented by a safety-related E/E system, or by a safety-related system of other technologies, in order to achieve or maintain a safe state for the item taking into account a determined hazardous event.

NOTE 2 The functional safety requirements might be specified independently of the used technology in the concept phase of product development. They are detailed into the technical safety requirements after concept phase.

1.54 hardware architectural metrics

metrics for the assessment of the effectiveness of the hardware architecture with respect to safety

NOTE The single point faults metric and the latent faults metric are the hardware architectural metrics.

1.55 hardware part

hardware element whose function cannot be further sub-divided

EXAMPLE Resistor, integrated circuit, microcontroller, capacitor, bus, cable, connector

1.56 harm

physical injury or damage to the health of people

1.57 hazard

potential source of harm

1.58 hazard analysis and risk assessment

method to identify and categorize hazardous events of items and to specify safety goals and ASILs related to the prevention or mitigation of these hazards in order to avoid unreasonable risk

1.59 hazardous event

combination of a hazard and an operational situation

1.60 homogeneous redundancy

multiple and identical implementations of a requirement

1.61 independence

absence of dependent failure between two or more elements that could lead to the violation of a safety requirement; or organizational separation of the parties performing an action

NOTE Independence is a characteristic associated with ASIL decomposition.

1.62 independent failures

failures whose probability of simultaneous or successive occurrence can be expressed as the simple product of their unconditional probabilities

1.63 informal notation

description technique that does not have its syntax completely defined

NOTE: An incomplete syntax definition implies that the semantics are also not completely defined.

EXAMPLE: descriptions in figures and diagrams

1.64 informal verification

verification methods not considered as semi-formal or formal verification techniques

EXAMPLE: design and model reviews

1.65 inheritance

passing attributes of requirements in an unchanged manner to the next level of detail during the development process

1.66 initial ASIL

ASIL resulting from the hazard analysis or the ASIL resulting from a preceding ASIL decomposition

NOTE: The initial ASIL is the starting point for ASIL decomposition or further ASIL decomposition.

1.67 inspection

systematic examination of work products, following a formal procedure, in order to detect anomalies

NOTE 1 Inspection is a means of verification.

NOTE 2 Inspection differs from testing in that it does not normally involve the operation of the items inspected.

NOTE 3 Any anomalies that are detected are usually addressed by rework, following which the reworked products are re-inspected.

EXAMPLE The inspection is organized by a “moderator” who chairs the inspection meeting. The material to be inspected is read by two independent inspectors. The author of the material attends the meeting and carries out the rework, but does not participate in the inspection. An inspection is divided into six obligatory phases:

— Planning: The moderator chooses the material to be inspected, ensures that inspectors are available and have adequate preparation time, and

— Kick-off: The inspection team meets and the author of the material briefs the moderator and inspectors.

— Preparation: The inspectors read the material independently in private and note any instances of nonconformity.

— Inspection meeting: The moderator chairs the meeting and assigns one of the inspectors to be the reader, who reads through the entire material out loud. Either inspector will draw attention to any discrepancies that were found, and these are documented by a secretary on a standard form;

— Rework: The author is given a list of discrepancies and revises the material to remove these.

— Final check: The moderator checks that the discrepancies have been removed, and schedules a re-inspection if necessary.

1.68 intended functionality

basic behavior specified for an item, system, or element

1.69 item

system or array of systems or a function to which ISO 26262 is applied

1.70 item development

entirety of the process of creating an E/E safety related system to which ISO 26262 is applied

1.71 latent fault

multiple point fault whose presence is not detected by a safety mechanism nor perceived by the driver within the multiple point fault detection interval

1.72 lifecycle

entirety of phases from concept through decommissioning of the item

1.73 malfunctioning behavior

failure or unintended behavior of the item with respect to the design intent for this item

1.74 model-based development

development that uses models to describe the functional behavior of the elements which are to be developed

NOTE Depending on the level of abstraction used for such a model it can be used for simulation or code generation or both.

1.75 modification

authorized alteration of an item

NOTE Modification is used in ISO 26262 with respect to re-use for lifecycle tailoring.

1.76 multiple point failure

failure, resulting from the combination of several independent faults, which leads directly to the violation of a safety goal

1.77 multiple point fault

individual fault that, in combination with other independent faults, leads to a multiple point failure

NOTE A “multiple point fault” can only be recognized after the identification of “multiple point failure” e.g. from cut set analysis of a fault tree.

1.78 multiple point fault detection interval

time span to detect **multiple point fault (1.77)** before it may contribute to a multiple point failure

NOTE An undetected **multiple point fault (1.77)** may be regarded as a latent fault.

1.79 new development

process of creating an item having previously unspecified functionality, a novel implementation of an existing functionality, or both

1.80 non-functional hazard

hazard that arises due to factors other than malfunction or incorrect functioning of the E/E system, safety-related systems of other technologies, or external risk reduction measures

1.81 operating mode

perceivable functional state of an item

EXAMPLE system off, system active, system passive, degraded operation, emergency operation

1.82 operating time

cumulative time that an item or element is functioning

1.83 operational situation

scenario that may occur during a vehicle’s life

EXAMPLE Operational situations can include driving, parking, and maintenance.

1.84 partitioning

separation of functions or elements

EXAMPLE Partitioning may be used for fault containment or ease of verification and validation.

1.85 passenger car

Vehicle designed and constructed primarily for the carriage of persons and their luggage, their goods, or both, having not more than a seating capacity of eight, in addition to the driver, and without space for standing passengers.

1.86 perceived fault

fault whose presence is deduced by the driver within a prescribed time interval

EXAMPLE The fault may be directly perceived through obvious limitation of system behavior or performance.

1.87 phase

stage in the safety lifecycle that is specified in a distinct part of ISO 26262

NOTE The phases in ISO 26262 are specified in distinct parts, i.e. ISO26262-3, ISO26262-4, ISO26262-5, ISO26262-6 and ISO26262-7 specify the concept phase, the phase "product development: system level", the phase "product development: hardware level", the phase "product development: software level", and the "production and operation" phase, respectively.

1.88 proven in use argument

evidence, based on analysis of field data resulting from use of a given version of a candidate, that the likelihood of any failure of this candidate that could impair a safety goal of an item that uses it is low enough according to the applicable ASIL

1.89 proven in use credit

set of safety lifecycle subphases or activities with corresponding work products that can be substituted by proven in use argument provided the candidate fulfils the proven in use criteria

1.90 random hardware failure

failure that may occur unpredictably during the lifetime of a hardware element and that follows a probability distribution

NOTE: Random hardware failure rates can be predicted with reasonable accuracy.

1.91 reasonably foreseeable event

event that is technically possible and has a credible or measurable rate of occurrence

NOTE Credibility is normally determined by a group of knowledgeable people.

1.92 redundancy

existence of means in addition to the means that would be sufficient for an element to perform a required function or to represent information

NOTE Redundancy is used in ISO 26262 with respect to achieving a safety goal, a specified safety requirement, or representing safety-related information.

EXAMPLE 1: Duplicated functional components can be an instance of redundancy for the purpose of increasing availability or allowing fault detection.

EXAMPLE 2: The addition of parity bits to data representing safety-related information provides redundancy for the purpose of allowing fault detection.

1.93 regression strategy

verification strategy to assure that change of an element or item has not affected existing and previously verified elements or items

1.94 residual fault

portion of a fault that by itself leads to the violation of a safety goal, occurring in a hardware element, where that portion of the fault is not covered by safety mechanisms

1.95 residual risk

risk remaining after the deployment of safety measures

1.96 review

examination of a work product, where the level of detail is up to the reviewer

NOTE: Reviews may be supported by checklists.

1.97 risk

combination of the probability of occurrence of harm and the severity of that harm

1.98 robust design

design that has the ability to function correctly in the presence of invalid inputs or stressful environment conditions

NOTE Robustness can be understood as follows:

- for software, robustness is the ability to respond to abnormal inputs and conditions,
- for hardware, robustness is the ability to be immune to environmental stress and stable over service life within design limits,
- for system, robustness is the ability to provide safe behavior at boundaries.

1.99 safe fault

fault whose occurrence will not significantly increase the probability of violation of a safety goal

NOTE A single point fault, a residual fault or a multiple point fault are not safe faults.

1.100 safe state

operating mode of an item without an unreasonable level of risk

EXAMPLE intended operating mode, degraded operating mode or switched-off modes

1.101 safety

absence of unreasonable risk

1.102 safety architecture

set of elements and their interaction to fulfill the safety requirements, including redundancy and independence concepts

1.103 safety case

argument that the safety goals for an item are complete and satisfied by evidence compiled from work products of the safety activities during development

NOTE Safety case can be extended to cover safety issues beyond the scope of this standard.

1.104 safety culture

policy and strategy used within an organization to support the development, production, and operation of safety related systems

1.105 safety goal

top-level safety requirement as a result of the hazard analysis and risk assessment

NOTE 1 The negation of a safety goal leads to the top event of further safety analyses (e.g. FTA).

NOTE 2 The existence of several safety goals for one item is possible. One safety goal can be related to several hazardous events.

1.106 safety measure

activity or technical solution to avoid or control systematic failures and to detect random hardware failures or control random hardware failures,, or mitigate their harmful effects

1.107 safety mechanism

measure implemented by a E/E functions or element, or in other technologies, to detect or control failures in order to achieve a safe state of the item, or maintain a safe state of the item, or both

NOTE 1 Safety mechanisms are implemented within the item to prevent faults from leading to single point failures or residual failures and to prevent faults from being latent.

NOTE 2 The safety mechanism is either

a) able to switch to, or maintain, the item in a safe state; or

b) able to alert the driver such that the driver is expected to control the effect of the failure;

as defined in the functional safety concept.

1.108 safety plan

plan to control and guide the safety activities of a project including dates, milestones, tasks, deliverables, responsibilities and resources

NOTE The objective of a safety plan is to ensure that a developed item will fulfill the safety goals.

1.109 safety-related element

element which has the potential to contribute to the violation of a safety goal

NOTE Fail-safe elements are considered safety-related if they contribute to the safety goal.

1.110 safety-related special characteristic

product or production process characteristic for which reasonably foreseeable deviation could impact, contribute to, or cause any potential reduction of functional safety

NOTE These safety-related special characteristics are derived during the development phase.

EXAMPLE Temperature range, expiry date, fastening torque, production tolerance, and configuration.

1.111 safety validation

assurance, based on examination and tests, that the safety goals are sufficient and have been achieved

NOTE ISO 26262-4 provides suitable methods for validation.

1.112 semi-formal notation

description technique that has its syntax completely defined, but its semantics definition may be incomplete

EXAMPLE Graphical modelling approaches such as UML use case diagrams, UML class diagrams, block diagrams and state charts.

1.113 semi-formal verification

verification that is based on a description using semi-formal notation

1.114 service note

documentation of safety information to be considered when performing maintenance procedures for the item

EXAMPLE safety-related special characteristic, safety operation that may be required

1.115 severity

measure of the extent of harm to an individual in a specific situation

1.116 single point failure

failure that results from a single point fault and leads directly to the violation of a safety goal

1.117 single point fault

fault in an element that is not covered by a safety mechanism and that leads directly to the violation of a safety goal

1.118 software component

Implementation of one or more logically and technically separable functions in software

NOTE A software component consists of one or more software components, or software units, or both. Within the software architecture software components are realised by partitions and tasks.

1.119 software tool

computer program used in the development of an item and its corresponding elements

1.120 software unit

lowest level software component of the software architecture that can be subjected to stand-alone testing

1.121 special purpose vehicle

vehicle intended to perform a function that requires special body arrangements, equipment or both

EXAMPLE motor caravan, armoured vehicles, ambulances, hearses, trailer caravans, mobile cranes

NOTE ECE TRANS/WP. 29/78/Rev. 1/Amend.2 provides definitions for special purpose vehicles.

1.122 statement coverage

percentage of statements within the software that have been executed

NOTE Execute an IF-statement within a source code with one test case.

1.123 sub-phase

subdivision of a stage in the safety lifecycle that is specified in a distinct clause of ISO 26262

NOTE Hazard analysis & risk assessment is specified in ISO-26262-3—, Clause 6.

1.124 system

set of elements, at least sensor, controller, and actuator, in relation with each other in accordance with a design

NOTE An element of a system can be another system at the same time.

1.125 systematic failure

failure of an element or item that is caused in a deterministic way during development, manufacturing, or maintenance

NOTE Systematic failures can be prevented by applying design measures or production process changes on this element or item.

1.126 technical safety concept

specification of the technical safety requirements to implement and to allocate them to the system design

1.127 technical safety requirement

requirements derived from the associated functional safety requirements to provide their technical implementation

1.128 testing

process of planning, preparing and executing or exercising a system or system component to verify that it satisfies specified requirements, to detect errors, and to create confidence in the system behaviour

1.129 unreasonable risk

risk judged to be unacceptable in a certain context according to valid societal moral concepts

1.130 verification

determination of completeness and correct specification or implementation of requirements from a previous phase

1.131 verification review

verification activity to ensure that the result of a development activity fulfils the project requirements, or, technical requirements, or both

NOTE 1 Individual requirements on "Verification Reviews" are given in dedicated clauses of ISO 26262.

NOTE 2 Goal of "Verification Reviews" is "technical" correctness and completeness of the item with respect to use cases and failure modes

EXAMPLE technical review, walkthrough, and inspections

1.132 walkthrough

systematic examination of work products in order to detect anomalies

NOTE 1 Walkthrough is a means of verification.

NOTE 2 Walkthrough differs from testing in that it does not normally involve the operation of the items inspected.

NOTE 3 Any anomalies that are detected are usually addressed by rework, following which the reworked products are walked through again.

EXAMPLE During a walkthrough the developer explains the work product step by step to one or more assessors. The objective is to create a common understanding of the work product and to identify any errors, defects, discrepancies or problems within the work product. A walkthrough is a less stringent form of an inspection.

1.133 warning and degradation concept

specification for how to alert the driver of potentially reduced functionality and specification how to provide this reduced functionality

1.134 well-trusted design principle

design principle that has been previously used with positive experience and without known safety problems

1.135 work product

reference to the complete information concerning the results of associated requirements

NOTE A reference can be an independent document containing the complete information of a work product or a list of references to the complete information of a work product.

2 Abbreviated terms

ACC	Adaptive Cruise Control

AEC	Automotive Electronics Council
AIS	Abbreviated Injury Scale
ASIC	Application-Specific Integrated Circuit
ASIL	Automotive Safety Integrity Level
BIST	Built-In Self-Test
CAN	Controller Area Network
CCF	Common Cause Failure
COTS	Commercial Off The Shelf
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DC	Diagnostic Coverage
D.C.	Direct Current
DIA	Development Interface Agreement
DSC	Dynamic Stability Control
ECU	Electronic Control Unit
EDC	Error Detection and Correction
E/E-System	Electrical and/or Electronic system
EMC	ElectroMagnetic Compatibility
ESD	ElectroStatic Discharge
ESP	Electronic Stability Program
ETA	Event Tree Analysis
FPGA	Field Programmable Gate Array
FHA	Functional Hazard Analysis
FMEA	Failure Mode and Effects Analysis
FTA	Fault Tree Analysis
HALT	Highly Accelerated Life Testing
HAZOP	HAZard and OPerability analysis
HSI	Hardware Software Interface
HW	Hardware

H&R	Hazard analysis and Risk assessment
IC	Integrated Circuit
I/O	Input – Output
MC/DC	Modified Condition/Decision Coverage
MMU	Memory Management Unit
MPU	Memory Protection Unit
MUX	MUltipleXer
OS	Operating System
PD	Product Development
PLD	Programmable Logic Device
QM	Quality Management
RAM	Random Access Memory
ROM	Read Only Memory
RFQ	Request For Quotation
SIL	Safety Integrity Level
SOP	Start Of Production
SRS	System Requirements Specification
SW	SoftWare
UML	Universal Modeling Language
V&V	Verification and Validation
XML	eXtensible Markup Language

Bibliography

[1] ISO 3779, Road vehicles – Vehicle identification number (VIN)

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

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

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

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

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

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

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

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

[10] ISO 26262-10: —[1] Road vehicles – Functional Safety — Part 10: Guideline on ISO 26262 (informative)

[11] ECE TRANS/WP. 29/78/Rev. 1/Amend.2 provides definitions for special purpose vehicles