INTERNATIONAL STANDARD

ISO 26262-1

Second edition
2018-12

Road vehicles — Functional safety —

Part 1: Vocabulary

Véhicules routiers — Sécurité fonctionnelle —
Partie 1: Vocabulaire

Reference number
ISO 26262-1:2018(E)

COPYRIGHT PROTECTED DOCUMENT

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

Published in Switzerland

Contents

Page

Foreword

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

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

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

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

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

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

This edition of ISO 26262 series of standards cancels and replaces the edition ISO 26262:2011 series of standards, which has been technically revised and includes the following main changes:

— requirements for trucks, buses, trailers and semi-trailers;

— extension of the vocabulary;

— more detailed objectives;

— objective oriented confirmation measures;

— management of safety anomalies;

— references to cyber security;

— updated target values for hardware architecture metrics;

— guidance on model based development and software safety analysis;

— evaluation of hardware elements;

— additional guidance on dependent failure analysis;

— guidance on fault tolerance, safety-related special characteristics and software tools;

— guidance for semiconductors;

— requirements for motorcycles; and

— general restructuring of all parts for improved clarity.

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

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

Introduction

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

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

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

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

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

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

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

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

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

e) provides requirements for relations between customers and suppliers.

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

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

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

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

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

— for motorcycles:

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

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

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

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

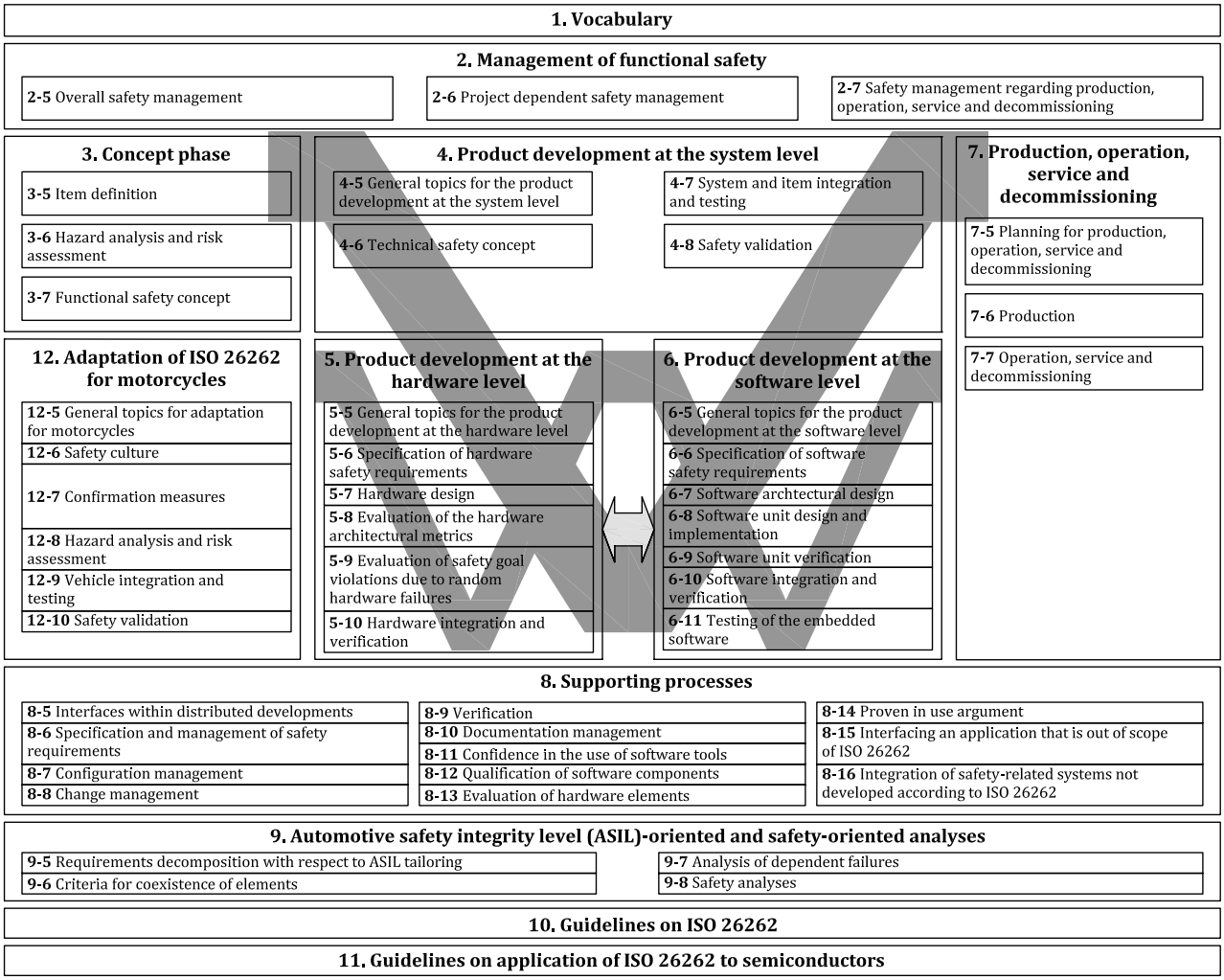

Figure 1 — Overview of the ISO 26262 series of standards

Road vehicles — Functional safety —

Part 1: Vocabulary

1 Scope

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

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

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

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

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

This document defines the vocabulary of terms used in the ISO 26262 series of standards.

2 Normative references

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

ISO 26262 (all parts), *Road vehicles — Functional safety*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 26262 (all parts) and the following apply.

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

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

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

3.1
architecture
representation of the structure of the *item* (3.84) or *element* (3.41) that allows identification of building blocks, their boundaries and interfaces, and includes the allocation of requirements to these building blocks

3.2
ASIL capability
capability of the *item* (3.84) or *element* (3.41) to meet assumed *safety* (3.132) requirements assigned with a given *ASIL* (3.6)

Note 1 to entry: As a part of hardware safety requirements, achievement of the corresponding random hardware target values for fault metrics (see ISO 26262-5:2018, Clauses 8 and 9) allocated to the *element* (3.41) is included, if needed.

3.3
ASIL decomposition
apportioning of redundant *safety* (3.132) requirements to *elements* (3.41), with sufficient *independence* (3.78), conducing to the same *safety goal* (3.139), with the objective of reducing the *ASIL* (3.6) of the redundant *safety* (3.132) requirements that are allocated to the corresponding *elements* (3.41)

Note 1 to entry: ASIL decomposition is a basis for methods of *ASIL* (3.6) tailoring during the design process (defined as requirements decomposition with respect to *ASIL* (3.6) tailoring in ISO 26262-9).

Note 2 to entry: ASIL decomposition does not apply to random hardware failure requirements per ISO 26262-9.

Note 3 to entry: Reducing the *ASIL* (3.6) of the redundant *safety* (3.132) requirements has some exclusions, e.g. *confirmation measures* (3.23) remain at the level of the *safety goal* (3.139).

3.4
assessment
examination of whether a characteristic of an *item* (3.84) or *element* (3.41) achieves the ISO 26262 objectives

3.5
audit
examination of an implemented process with regard to the process objectives

3.6
automotive safety integrity level
ASIL
one of four levels to specify the *item's* (3.84) or *element's* (3.41) necessary ISO 26262 requirements and *safety measures* (3.141) to apply for avoiding an *unreasonable risk* (3.176), with D representing the most stringent and A the least stringent level

Note 1 to entry: *QM* (3.117) is not an ASIL.

3.7
availability
capability of a product to provide a stated function if demanded, under given conditions over its defined lifetime

3.8
base failure rate
BFR
failure rate (3.53) of a hardware *element* (3.41) in a given application use case used as an input to *safety* (3.132) analyses

3.9
base vehicle
Original Equipment Manufacturer (OEM) *T&B vehicle configuration* (3.175) prior to installation of *body builder equipment* (3.12)

Note 1 to entry: *Body builder equipment* (3.12) may be installed on a base vehicle that consists of all driving relevant *systems* (3.163) (engine, driveline, chassis, steering, brakes, cabin and driver information).

EXAMPLE *Truck* (3.174) chassis with powertrain and cabin, rolling chassis with powertrain.

3.10
baseline
version of the approved set of one or more *work products* (3.185), *items* (3.84) or *elements* (3.41) that serves as a basis for change

Note 1 to entry: See ISO 26262-8:2018, Clause 8.

Note 2 to entry: A baseline is typically placed under configuration management.

Note 3 to entry: A baseline is used as a basis for further development through the change management process during the *lifecycle* (3.86).

3.11
body builder
BB
organization that adds *trucks* (3.174), *buses* (3.14), *trailers* (3.171) and *semi-trailers* (3.151) (T&B) bodies, cargo carriers, or equipment to a *base vehicle* (3.9)

Note 1 to entry: T&B bodies include *truck* (3.174) cabs, *bus* (3.14) bodies, walk-in vans, etc.

Note 2 to entry: Cargo carriers include cargo boxes, flat beds, car transport racks, etc.

Note 3 to entry: Equipment includes vocational devices and machinery, such as cement mixers, dump beds, snow blades, lifts, etc.

3.12
body builder equipment
machine, body, or cargo carrier installed on the T&B *base vehicle* (3.9)

3.13
branch coverage
percentage of branches of the control flow of a computer program executed during a test

Note 1 to entry: 100 % branch coverage implies 100 % *statement coverage* (3.160).

Note 2 to entry: An if-statement always has two branches - condition true and condition false - independent of the existence of an else-clause.

3.14
bus
motor vehicle which, because of its design and appointments, is intended for carrying persons and luggage, and which has more than nine seating places, including the driving seat

Note 1 to entry: A bus may have one or two decks and may also tow a *trailer* (3.171).

3.15
calibration data
data that will be applied as software parameter values after the software build in the development process

EXAMPLE Parameters (e.g. value for low idle speed, engine characteristic diagrams); vehicle specific parameters (adaptation values, e.g., limit stop for throttle valve); variant coding (e.g. country code, left-hand/ right-hand steering).

Note 1 to entry: Calibration data does not contain executable or interpretable code.

3.16
candidate
item (3.84) or *element* (3.41) whose definition and conditions of use are identical to, or have a very high degree of commonality with, an *item* (3.84) or *element* (3.41) that is already released and in operation

Note 1 to entry: This definition applies where candidate is used in the context of a *proven in use argument* (3.115).

3.17
cascading failure
failure (3.50) of an *element* (3.41) of an *item* (3.84) resulting from a root cause [inside or outside of the *element* (3.41)] and then causing a *failure* (3.50) of another *element* (3.41) or *elements* (3.41) of the same or different *item* (3.84)

Note 1 to entry: Cascading failures are *dependent failures* (3.29) that could be one of the possible root causes of a *common cause failure* (3.18). See Figure 2.

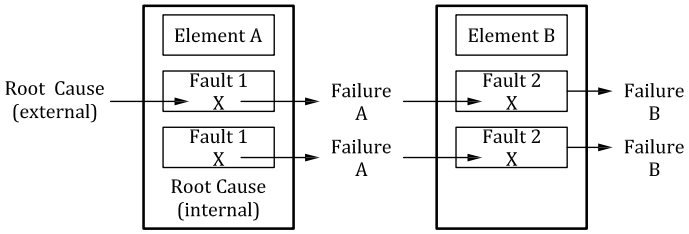

Figure 2 — Cascading failure

3.18
common cause failure
CCF
failure (3.50) of two or more *elements* (3.41) of an *item* (3.84) resulting directly from a single specific event or root cause which is either internal or external to all of these *elements* (3.41)

Note 1 to entry: Common cause failures are *dependent failures* (3.29) that are not *cascading failures* (3.17). See Figure 3.

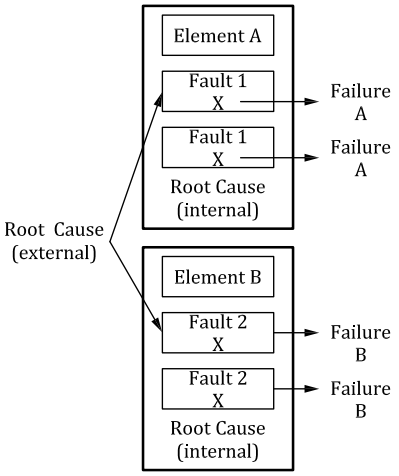

Figure 3 — Common cause failure

3.19
common mode failure
CMF
case of *CCF* (3.18) in which multiple *elements* (3.41) fail in the same manner

Note 1 to entry: *Failure* (3.50) in the same manner does not necessarily mean that they need to fail exactly the same. How close the *failure modes* (3.51) need to be in order to be classified as common mode failure depends on the context.

EXAMPLE 1 A *system* (3.163) has two temperature sensors which are compared with each other. If the difference between the two temperature sensors is larger than or equal to 5 °C it is handled as a *fault* (3.54) and the *system* (3.163) is switched into a *safe state* (3.131). A common mode failure lets both temperature sensors fail in such a way that the difference between the two sensors is smaller than 5 °C and therefore is not detected.

EXAMPLE 2 In a CPU lockstep *architecture* (3.1) where the outputs of both CPUs are compared cycle by cycle, both CPUs need to fail exactly the same way in order for the *failure* (3.50) to go undetected. In this context, a common mode failure lets both CPUs fail exactly the same way.

EXAMPLE 3 An over voltage *failure* (3.50) due to lots of parts not meeting their specification for over voltage is a common mode failure.

3.20
complete vehicle
fully assembled T&B *base vehicle* (3.9) with its *body builder equipment* (3.12)

EXAMPLE Refuse collector, dump *truck* (3.174).

3.21
component
non-system level *element* (3.41) that is logically or technically separable and is comprised of more than one *hardware part* (3.71) or one or more *software units* (3.159)

EXAMPLE A microcontroller.

Note 1 to entry: A component is a part of a *system* (3.163).

3.22
configuration data
data that is assigned during element build and that controls the element build process

EXAMPLE 1 Pre-processor variable settings which are used to derive compile time variants from the source code.

EXAMPLE 2 XML files to control the build tools or toolchain.

Note 1 to entry: Configuration data controls the software build. Configuration data is used to select code from existing code variants already defined in the code base. The functionality of selected code variant will be included in the executable code.

Note 2 to entry: Since configuration data is only used to select code variants, configuration data does not include code that is executed or interpreted during the use of the *item* (3.84).

3.23
confirmation measure
confirmation review (3.24), *audit* (3.5) or *assessment* (3.4) concerning *functional safety* (3.67)

3.24
confirmation review
confirmation that a *work product* (3.185) provides sufficient and convincing evidence of their contribution to the achievement of *functional safety* (3.67) considering the corresponding objectives and requirements of ISO 26262

Note 1 to entry: A complete list of confirmation reviews is given in ISO 26262-2.

Note 2 to entry: The goal of confirmation reviews is to ensure compliance with the ISO 26262 series of standards.

3.25
controllability
ability to avoid a specified *harm* (3.74) or damage through the timely reactions of the persons involved, possibly with support from *external measures* (3.49)

Note 1 to entry: Persons involved can include the driver, passengers or persons in the vicinity of the vehicle's exterior.

Note 2 to entry: The parameter C in *hazard analysis and risk assessment* (3.76) represents the potential for controllability.

3.26
coupling factors
common characteristic or relationship of *elements* (3.41) that leads to a dependence in their *failures* (3.50)

3.27
dedicated measure
measure to ensure the *failure rate* (3.53) claimed in the evaluation of the probability of violation of *safety goals* (3.139)

EXAMPLE Design feature such as *hardware part* (3.71) over-design (e.g. electrical or thermal stress rating) or physical separation (e.g. spacing of contacts on a printed circuit board); special sample test of incoming material to reduce the *risk* (3.128) of occurrence of *failure modes* (3.51) which contribute to the violation of *safety goals* (3.139); burn-in test; dedicated control plan.

3.28
degradation
state or transition to a state of the *item* (3.84) or *element* (3.41) with reduced functionality, performance, or both

3.29
dependent failures
failures (3.50) that are not statistically independent, i.e. the probability of the combined occurrence of the *failures* (3.50) is not equal to the product of the probabilities of occurrence of all considered independent *failures* (3.50)

Note 1 to entry: Dependent failures can manifest themselves simultaneously, or within a sufficiently short time interval, to have the effect of simultaneous *failures* (3.50).

Note 2 to entry: Dependent failures include *common cause failures* (3.18) and *cascading failures* (3.17).

Note 3 to entry: Whether a given *failure* (3.50) is a *cascading failure* (3.17) or a *common cause failure* (3.18) may depend on the hierarchical structure of the *elements* (3.41).

Note 4 to entry: Whether a given *failure* (3.50) is a *cascading failure* (3.17) or a *common cause failure* (3.18) may depend on the temporal behaviour of the *elements* (3.41).

Note 5 to entry: Dependent failures can include software *failures* (3.50) even if the probability of the *failure* (3.50) is not calculated.

3.30
dependent failure initiator
DFI
single root cause that leads multiple *elements* (3.41) to fail through *coupling factors* (3.26)

Note 1 to entry: *Coupling factors* (3.26) which are candidates for dependencies are identified during DFA.

Note 2 to entry: *Failure* (3.50) of *elements* (3.41) can happen simultaneously or sequentially.

EXAMPLE 1 *Coupling factor* (3.26): Two SW units using the same RAM. Root cause: One SW unit unintentionally corrupts data used by the second SW unit.

EXAMPLE 2 *Coupling factor* (3.26): Two ECUs operating in the same compartment of the car. Root cause: Unwanted/unexpected water intrusion into that particular compartment leads to flooding and to *failure* (3.50) of both ECUs.

EXAMPLE 3 *Coupling factor* (3.26): Two microcontrollers using the same 3,3 V power supply. Root cause: Overvoltage on the 3,3 V, damaging both microcontrollers.

3.31
detected fault
fault (3.54) whose presence is detected within a prescribed time by a *safety mechanism* (3.142)

Note 1 to entry: The prescribed time can be the *fault detection time interval* (3.55) or the *multiple-point fault detection time interva*l (3.98).

3.32
development interface agreement
DIA
agreement between customer and supplier in which the responsibilities for activities to be performed, evidence to be reviewed, or *work products* (3.185) to be exchanged by each party related to the development of *items* (3.84) or *elements* (3.41) are specified

Note 1 to entry: While DIA applies to the development phase, *supply agreement* (3.162) applies to production.

3.33
diagnostic coverage
DC
percentage of the *failure rate* (3.53) of a hardware *element* (3.41), or percentage of the *failure rate* (3.53) of a *failure mode* (3.51) of a hardware *element* (3.41) that is detected or controlled by the implemented *safety mechanism* (3.142)

Note 1 to entry: Diagnostic coverage can be assessed with regard to *residual faults* (3.125) or with regard to latent *multiple-point faults* (3.97) that might occur in a hardware *element* (3.41).

Note 2 to entry: *Safety mechanisms* (3.142) implemented at different levels in the *architecture* (3.1) can be considered.

Note 3 to entry: Except when it is explicitly mentioned, the proportion of *safe faults* (3.130) of a safety-related hardware *element* (3.41) is not considered when determining the diagnostic coverage of the *safety mechanism* (3.142).

3.34
diagnostic points
output signals of an *element* (3.41) at which the detection or correction of a *fault* (3.54) is observed

Note 1 to entry: Diagnostic points are also referred to as "alarms" or "*error* (3.46) flags" or "correction flags".

EXAMPLE Read back information.

3.35
diagnostic test time interval
amount of time between the executions of online diagnostic tests by a *safety mechanism* (3.142) including duration of the execution of an online diagnostic test

Note 1 to entry: See Figure 5.

3.36
distributed development
development of an *item* (3.84) or *element* (3.41) with development responsibility divided between the customer and supplier(s) for the entire *item* (3.84) or *element* (3.41)

Note 1 to entry: Customer and supplier are roles of the cooperating parties.

3.37
diversity
different solutions satisfying the same requirement, with the goal of achieving *independence* (3.78)

Note 1 to entry: Diversity does not guarantee *independence* (3.78), but can deal with certain types of *common cause failures* (3.18).

Note 2 to entry: Diversity can be a technical solution [diverse hardware *components* (3.21), diverse SW *components* (3.21)] or a technical means (e.g. diverse compiler) to apply.

Note 3 to entry: Diversity is one way to realize *redundancy* (3.122).

EXAMPLE Diverse programming; diverse hardware.

3.38
dual-point failure
failure (3.50) resulting from the combination of two independent hardware *faults* (3.54) that leads directly to the violation of a *safety goal* (3.139)

Note 1 to entry: Dual-point failures are *multiple-point failures* (3.96) of order 2.

Note 2 to entry: Dual-point failures that are addressed in the ISO 26262 series of standards include those where one *fault* (3.54) affects a *safety-related element* (3.144) and another *fault* (3.54) affects the corresponding *safety mechanism* (3.142) intended to achieve or maintain a *safe state* (3.131).

3.39
dual-point fault
individual *fault* (3.54) that, in combination with another independent *fault* (3.54), leads to a *dual-point failure* (3.38)

Note 1 to entry: A dual-point fault can only be recognized after the identification of a *dual-point failure* (3.38), e.g. from cut set analysis of a fault tree.

Note 2 to entry: See also *multiple-point fault* (3.97).

3.40
electrical and/or electronic system
E/E system
system (3.163) that consists of electrical or electronic *elements* (3.41), including programmable electronic *elements* (3.41)

Note 1 to entry: An *element* (3.41) of an E/E system can also be another E/E system.

EXAMPLE Power supply; sensor or other input device; communication path; actuator or other output device.

3.41
element
system (3.163), *components* (3.21) (hardware or software), *hardware parts* (3.71), or *software units* (3.159)

Note 1 to entry: When “software element” or “hardware element” is used, this phrase denotes an element of software only or an element of hardware only, respectively.

Note 2 to entry: An element may also be a *SEooC* (3.138).

3.42
embedded software
fully-integrated software to be executed on a *processing element* (3.113)

3.43
emergency operation
operating mode (3.102) of an *item* (3.84), for providing *safety* (3.132) after the reaction to a *fault* (3.54) until the transition to a *safe state* (3.131) is achieved

Note 1 to entry: See Figure 4 and Figure 5.

Note 2 to entry: When a *safe state* (3.131) cannot be directly reached, or cannot be timely reached, or cannot be maintained after the detection of a *fault* (3.54), a *safety mechanism* (3.142) can transition the *item* (3.84) to emergency operation for providing *safety* (3.132) until the transition to a *safe state* (3.131) is achieved and maintained.

Note 3 to entry: Emergency operation and associated *emergency operation tolerance time interval* (3.45) are described in the *warning and degradation strategy* (3.183).

Note 4 to entry: *Degradation* (3.28) can be part of the concept for emergency operation.

EXAMPLE Emergency operation can be specified as part of the *error* (3.46) reaction of a fault tolerant *item* (3.84).

3.44
emergency operation time interval
EOTI
time-span during which *emergency operation* (3.43) is maintained

Note 1 to entry: See Figure 4 and Figure 5.

Note 2 to entry: *Emergency operation* (3.43) and associated *emergency operation tolerance time interval* (3.45) are described in the *warning and degradation strategy* (3.183).

Note 3 to entry: *Emergency operation* (3.43) is temporarily maintained for providing *safety* (3.132) until the transition to a *safe state* (3.131) is achieved.

3.45
emergency operation tolerance time interval
EOTTI
specified time-span during which *emergency operation* (3.43) can be maintained without an unreasonable level of *risk* (3.128)

Note 1 to entry: See Figure 4.

Note 2 to entry: Emergency operation tolerance time interval is the maximum value of the *emergency operation time interval* (3.44).

Note 3 to entry: *Emergency operation* (3.43) can be considered safe due to the limited operation time as defined in the emergency operation tolerance time interval.

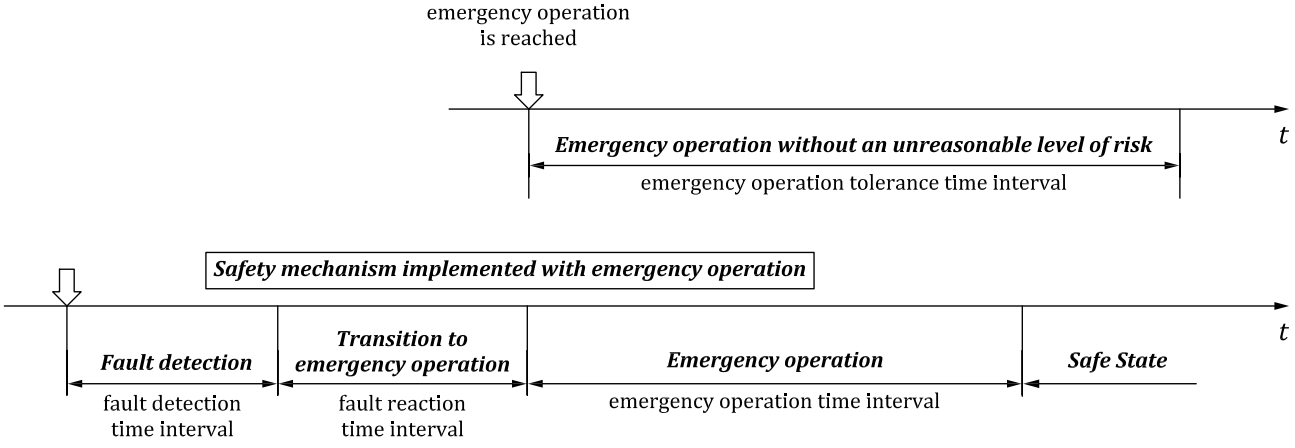

Figure 4 — Emergency operation tolerance time interval

3.46
error
discrepancy between a computed, observed or measured value or condition, and the true, specified or theoretically correct value or condition

Note 1 to entry: An error can arise as a result of a *fault* (3.54) within the *system* (3.163) or *component* (3.21) being considered.

3.47
expert rider
role filled by persons capable of evaluating *controllability* (3.25) classifications based on operation of actual *motorcycles* (3.93)

Note 1 to entry: An expert rider is a rider who has the:

— skill to evaluate *controllability* (3.25) including knowledge to evaluate;

— capability to conduct the vehicle test; and

— knowledge to evaluate *motorcycle* (3.93) *controllability* (3.25) characteristics with respect to a representative rider's riding capability.

Note 2 to entry: See ISO 26262-12:2018, Annex C for information relating to the use of expert riders.

3.48
exposure
state of being in an *operational situation* (3.104) that can be hazardous if coincident with the *failure mode* (3.51) under analysis

Note 1 to entry: The parameter "E" in *hazard analysis and risk assessment* (3.76) represents the potential exposure to the *operational situation* (3.104).

3.49
external measure
measure that is separate and distinct from the *item* (3.84) which reduces or mitigates the *risks* (3.128) resulting from the *item* (3.84)

3.50
failure
termination of an intended behaviour of an *element* (3.41) or an *item* (3.84) due to a *fault* (3.54) manifestation

Note 1 to entry: Termination can be permanent or transient.

3.51
failure mode
manner in which an *element* (3.41) or an *item* (3.84) fails to provide the intended behaviour

3.52
failure mode coverage
FMC
proportion of the *failure rate* (3.53) of a *failure mode* (3.51) of a hardware *element* (3.41) that is detected or controlled by the implemented *safety mechanism* (3.142)

3.53
failure rate
probability density of *failure* (3.50) divided by probability of survival for a hardware *element* (3.41)

Note 1 to entry: The failure rate is assumed to be constant and is generally denoted as "λ".

3.54
fault
abnormal condition that can cause an *element* (3.41) or an *item* (3.84) to fail

Note 1 to entry: Permanent, intermittent, and *transient faults* (3.173) (especially soft errors) are considered.

Note 2 to entry: When a subsystem is in an *error* (3.46) state it could result in a fault for the *system* (3.163).

Note 3 to entry: An intermittent fault occurs from time to time and then disappears again. This type of fault can occur when a *component* (3.21) is on the verge of breaking down or, for example, due to an internal malfunction in a switch. Some *systematic faults* (3.165) (e.g. timing irregularities) could lead to intermittent faults.

3.55
fault detection time interval
FDTI
time-span from the occurrence of a *fault* (3.54) to its detection

Note 1 to entry: See Figure 5.

Note 2 to entry: Fault detection time interval is determined independently of *diagnostic test time interval* (3.35).

EXAMPLE The fault detection time interval of a diagnostic test can be longer than the *diagnostic test time interval* (3.35) due to implemented *error* (3.46) counters, i.e. the *fault* (3.54) must be detected more than once by the diagnostic test before triggering an *error* (3.46) reaction.

Note 3 to entry: Fault detection time interval, *diagnostic test time interval* (3.35), and *fault reaction time interval* (3.59) are relevant characteristics of a *safety mechanism* (3.142) based on *fault* (3.54) detection.

Note 4 to entry: A *fault* (3.54) is timely covered by the corresponding *safety mechanism* (3.142) if the fault detection time interval plus the *fault reaction time interval* (3.59) is lower than the relevant *fault tolerant time interval* (3.61).

3.56
fault handling time interval
FHTI
sum of *fault detection time interval* (3.55) and the *fault reaction time interval* (3.59)

Note 1 to entry: The FHTI is a property of a *safety mechanism* (3.142).

Note 2 to entry: See Figure 5.

3.57
fault injection
method to evaluate the effect of a *fault* (3.54) within an *element* (3.41) by inserting *faults* (3.54), *errors* (3.46), or *failures* (3.50) in order to observe the reaction by *observation points* (3.101)

Note 1 to entry: Fault injection can be performed at various levels of abstraction including *item* (3.84) or *element* (3.41) level depending on the scope, feasibility, observability and level of required detail. Depending on purpose, it can be performed at different stages of the safety lifecycle and by considering different *fault models* (3.58).

EXAMPLE 1 Injecting *faults* (3.54) during operation to verify that a *safety mechanism* (3.142) is working properly as part of a strategy to detect *latent faults* (3.85).

EXAMPLE 2 Injecting *faults* (3.54) during integration test through hardware debug ports or through dedicated software commands to test the hardware-software interface (HSI).

EXAMPLE 3 Simulating stuck-at *faults* (3.54) or transient faults at hardware component level to verify the *diagnostic coverage* (3.33) of a *safety mechanism* (3.142) or to identify *faults* (3.54) which may result in *errors* (3.46) or *failures* (3.50).

3.58
fault model
representation of *failure modes* (3.51) resulting from *faults* (3.54)

Note 1 to entry: Fault models are used to assess consequences of particular *faults* (3.54).

3.59
fault reaction time interval
FRTI
time-span from the detection of a *fault* (3.54) to reaching a *safe state* (3.131) or to reaching *emergency operation* (3.43)

Note 1 to entry: See Figure 4 and Figure 5.

3.60
fault tolerance
ability to deliver a specified functionality in the presence of one or more specified *faults* (3.54)

Note 1 to entry: Specified functionality can be *intended functionality* (3.83).

3.61
fault tolerant time interval
FTTI
minimum time-span from the occurrence of a *fault* (3.54) in an *item* (3.84) to a possible occurrence of a *hazardous event* (3.77), if the *safety mechanisms* (3.142) are not activated

Note 1 to entry: See Figure 5.

Note 2 to entry: The minimum time-span is to be evaluated over all *hazardous events* (3.77). It can depend on the characterization of the *hazards* (3.75).

Note 3 to entry: FTTI is related to a *hazard* (3.75) caused by a *malfunctioning behaviour* (3.88) of the *item* (3.84). FTTI is a relevant attribute for *safety goals* (3.139) derived from this *hazard* (3.75).

Note 4 to entry: A *fault* (3.54) is timely covered by a *safety mechanism* (3.142), if the *item* (3.84) is maintained in a *safe state* (3.131), or if the *item* (3.84) is transitioned to a *safe state* (3.131), or is transitioned to an *emergency operation* (3.43), within the relevant fault tolerant time interval.

Note 5 to entry: The occurrence of a *hazardous event* (3.77) is dependent on a *fault* (3.54) being present and a vehicle being in a scenario that allows the *fault* (3.54) to affect vehicle behaviour.

EXAMPLE A *failure* (3.50) in the brake *system* (3.163) may not result in a *hazardous event* (3.77) until the brakes are applied.

Note 6 to entry: While the FTTI is defined only at the *item* (3.84) level, at the *element* (3.41) level the maximum *fault handling time interval* (3.56) and the state to be achieved after fault handling to support the *functional safety concept* (3.68) can be specified.

Note 7 to entry: The *fault detection time interval* (3.55) may include multiple *diagnostic test time intervals* (3.35) to allow de-bouncing of *errors* (3.46) if the *diagnostic test time interval* (3.35) is sufficiently shorter than the *fault detection time interval* (3.55).

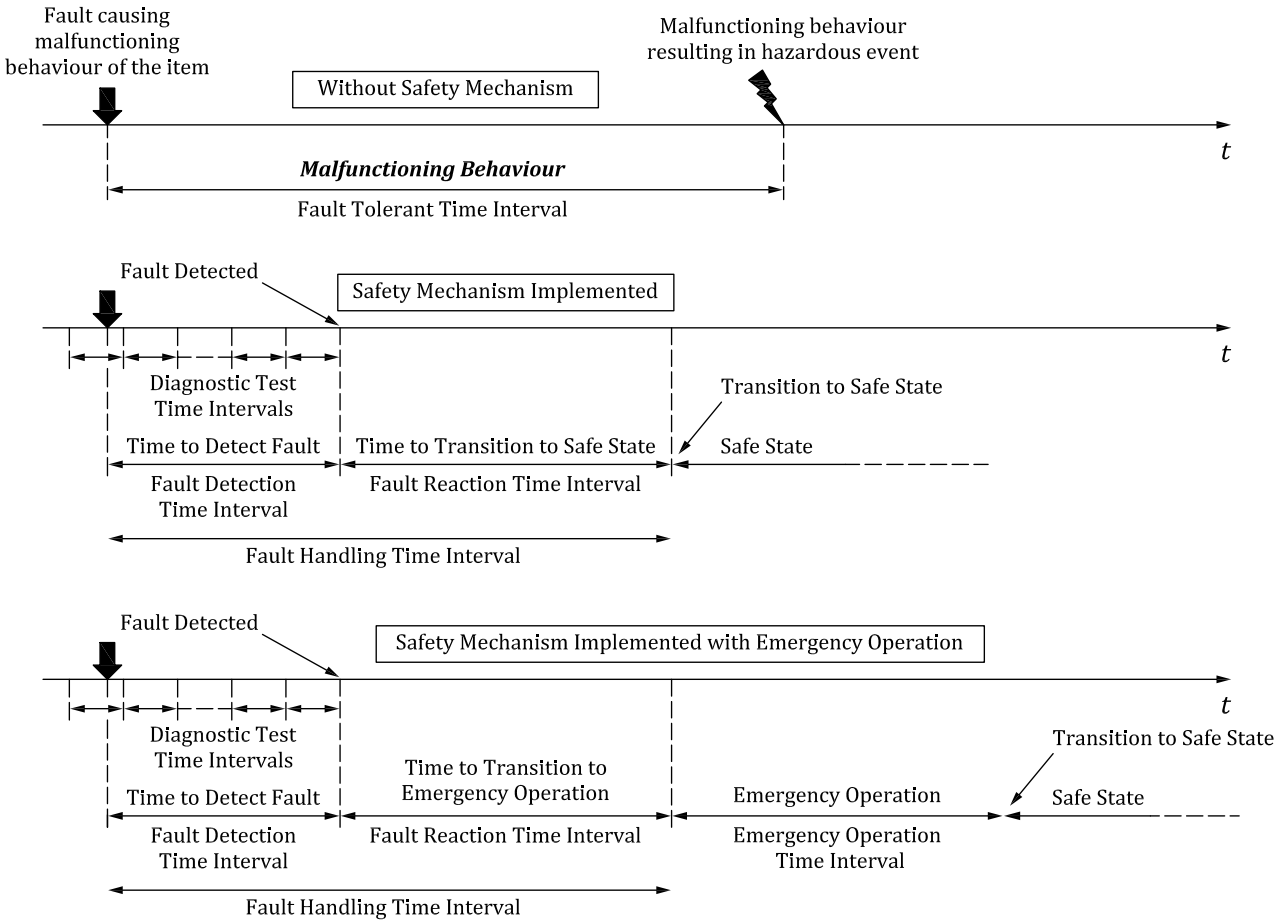

Figure 5 — Safety relevant time intervals

3.62
field data
data obtained from the use of an *item* (3.84) or *element* (3.41) including cumulative operating hours, all *failures* (3.50) and in-service *safety anomalies* (3.134)

Note 1 to entry: Field data normally comes from customer use.

3.63
formal notation
description technique that has both its syntax and semantics completely defined

EXAMPLE Z notation (Zed); NuSMV (symbolic model checker); Prototype Verification System (PVS); Vienna Development Method (VDM); mathematical formulae.

3.64
formal verification
method used to prove the correctness of an *item* (3.84) or *element* (3.41) against the specification of its function or properties in *formal notation* (3.63)

3.65
freedom from interference
absence of *cascading failures* (3.17) between two or more *elements* (3.41) that could lead to the violation of a *safety* (3.132) requirement

EXAMPLE 1 *Element* (3.41) 1 is free of interference from *element* (3.41) 2 if no *failure* (3.50) of *element* (3.41) 2 can cause *element* (3.41) 1 to fail.

EXAMPLE 2 *Element* (3.41) 3 interferes with *element* (3.41) 4 if there exists a *failure* (3.50) of *element* (3.41) 3 that causes *element* (3.41) 4 to fail.

3.66
functional concept
specification of the intended functions and their interactions necessary to achieve the desired behaviour

Note 1 to entry: The functional concept is developed during the concept *phase* (3.110).

3.67
functional safety
absence of *unreasonable risk* (3.176) due to *hazards* (3.75) caused by *malfunctioning behaviour* (3.88) of *E/E systems* (3.40)

3.68
functional safety concept
specification of the *functional safety requirements* (3.69), with associated information, their allocation to *elements* (3.41) within the *architecture* (3.1), and their interaction necessary to achieve the *safety goals* (3.139)

3.69
functional safety requirement
specification of implementation-independent *safety* (3.132) behaviour or implementation-independent *safety measure* (3.141) including its safety-related attributes

Note 1 to entry: A functional safety requirement can be a *safety* (3.132) requirement implemented by a safety-related *E/E system* (3.40), or by a safety-related *system* (3.163) of *other technologies* (3.105), in order to achieve or maintain a *safe state* (3.131) for the *item* (3.84) taking into account a determined *hazardous event* (3.77).

Note 2 to entry: The functional safety requirements might be specified independently of the technology used in the concept *phase* (3.110) of product development.

Note 3 to entry: Safety-related attributes include information about the *ASIL* (3.6).

3.70
hardware architectural metrics
metrics for the *evaluation* of the effectiveness of the hardware *architecture* (3.1) with respect to *safety* (3.132)

Note 1 to entry: The *single-point fault* (3.156) metric and the *latent fault* (3.85) metric are the hardware architectural metrics.

3.71
hardware part
portion of a hardware *component* (3.21) at the first level of hierarchical decomposition

EXAMPLE The CPU of a microcontroller, a resistor, flash array of a microcontroller.

3.72
hardware elementary subpart
smallest portion of a *hardware subpart* (3.73) considered in *safety* (3.132) analysis

EXAMPLE A flip-flop of the ALU with its logic cone, a register.

3.73
hardware subpart
portion of a *hardware part* (3.71) that can be logically divided and represents second or greater level of hierarchical decomposition

EXAMPLE ALU of a CPU of a microcontroller, register bank of a CPU.

3.74
harm
physical injury or damage to the health of persons

3.75
hazard
potential source of *harm* (3.74) caused by *malfunctioning behaviour* (3.88) of the *item* (3.84)

Note 1 to entry: This definition is restricted to the scope of the ISO 26262 series of standards; a more general definition is potential source of *harm* (3.74).

3.76
hazard analysis and risk assessment
HARA
method to identify and categorize *hazardous events* (3.77) of *items* (3.84) and to specify *safety goals* (3.139) and *ASILs* (3.6) related to the prevention or mitigation of the associated *hazards* (3.75) in order to avoid *unreasonable risk* (3.176)

3.77
hazardous event
combination of a *hazard* (3.75) and an *operational situation* (3.104)

3.78
independence
absence of *dependent failures* (3.29) between two or more *elements* (3.41) that could lead to the violation of a *safety* (3.132) requirement, or organizational separation of the parties performing an action

Note 1 to entry: *ASIL decomposition* (3.3) or *confirmation measures* (3.23) include requirements on independence.

3.79
independent failures
failures (3.50) whose probability of simultaneous or successive occurrence can be expressed as the simple product of their unconditional probabilities

Note 1 to entry: Independent failures can include software *failures* (3.50) even if their probability of failure is not calculated.

3.80
informal notation
description technique that does not have its syntax completely defined

Note 1 to entry: An incomplete syntax definition implies that the semantics are also not completely defined.

3.81
inheritance
conveyance of attributes of requirements in an unchanged manner to the next level of detail during the development process

3.82
inspection
examination of *work products* (3.185), following a formal procedure, in order to detect *safety anomalies* (3.134)

Note 1 to entry: Inspection is a means of *verification* (3.180).

Note 2 to entry: Inspection differs from *testing* (3.169) in that it does not normally involve the operation of the associated *item* (3.84) or *element* (3.41).

Note 3 to entry: A formal procedure normally includes a previously defined procedure, checklist, moderator and *review* (3.127) of the results.

3.83
intended functionality
behaviour specified for an *item* (3.84), excluding *safety mechanisms* (3.142)

Note 1 to entry: The specified behaviour is at the vehicle level.

3.84
item
system (3.163) or combination of *systems* (3.163), to which ISO 26262 is applied, that implements a function or part of a function at the vehicle level

Note 1 to entry: See *vehicle function* (3.178).

3.85
latent fault
multiple-point fault (3.97) whose presence is not detected by a *safety mechanism* (3.142) nor perceived by the driver within the *multiple-point fault detection time interval* (3.98)

3.86
lifecycle
entirety of *phases* (3.110) from concept through decommissioning of the *item* (3.84)

3.87
management system
policies, procedures and processes an organization uses to meet its objectives

3.88
malfunctioning behaviour
failure (3.50) or unintended behaviour of an *item* (3.84) with respect to its design intent

3.89
maximum time to repair time interval
specified time-span during which a *safe state* (3.131) can be maintained

Note 1 to entry: Maximum time to repair is a relevant characteristic when a *safe state* (3.131) cannot be maintained until the end of the remaining vehicle service life.

Note 2 to entry: The conditions for recovering from the *safe state* (3.131) are described in the *warning and degradation strategy* (3.183).

Note 3 to entry: If relevant, maximum time to repair time interval is described in the *warning and degradation strategy* (3.183).

3.90
model-based development
MBD
development that uses models to describe the behaviour or properties of an *element* (3.41) to be developed

Note 1 to entry: Depending on the level of abstraction used for such a model, the model can be used for simulation or code generation or both.

3.91
modification
Creation of a new *item* (3.84) from an existing *item* (3.84)

Note 1 to entry: Modification is used in the ISO 26262 series of standards with respect to re-use for *lifecycle* (3.86) tailoring. A change is applied during the *lifecycle* (3.86) of an *item* (3.84), while a modification is applied to create a new *item* (3.84) from an existing one.

3.92
modified condition/decision coverage
MC/DC
percentage of all single condition outcomes that independently affect a decision outcome that have been exercised in the control flow

Note 1 to entry: MC/DC is a type of code coverage analysis. It builds on top of *branch coverage* (3.13), and as such, it too requires that all code blocks and all execution paths have been tested.

3.93
motorcycle
two-wheeled motor-driven vehicle, or three-wheeled motor-driven vehicle whose unladen weight does not exceed 800 kg, excluding mopeds as defined in ISO 3833

3.94
motorcycle safety integrity level
MSIL
one of four levels that specify the *item's* (3.84) or *element's* (3.41) necessary ISO 26262 *risk* (3.128) reduction requirements and convert to ASIL (3.6) for *safety measures* (3.141) to apply for avoiding unreasonable *residual risk* (3.126) for *items* (3.84) and *elements* (3.41) used specifically in *motorcycle* (3.93) applications, with D representing the most stringent and A the least stringent level

3.95
multi-core
hardware *component* (3.21) which includes two or more hardware *processing elements* (3.113) which can operate independently from each other

3.96
multiple-point failure
failure (3.50), resulting from the combination of several independent hardware *faults* (3.54), which leads directly to the violation of a *safety goal* (3.139)

3.97
multiple-point fault
individual *fault* (3.54) that, in combination with other independent *faults* (3.54), if undetected and not perceived, could lead to a *multiple-point failure* (3.96)

Note 1 to entry: A multiple-point fault can only be recognized after the identification of a *multiple-point failure* (3.96), e.g. from cut set analysis of a fault tree.

3.98
multiple-point fault detection time interval
time-span to detect a *multiple-point fault* (3.97) before it can contribute to a *multiple-point failure* (3.96)

3.99
new development
process of creating an *item* (3.84) or *element* (3.41) having a previously unspecified functionality, or a novel implementation of an existing functionality, or both

3.100
non-functional hazard
hazard (3.75) that arises due to factors other than *malfunctioning behaviour* (3.88) of the *E/E system* (3.40), safety-related *systems* (3.163) of *other technologies* (3.105), or *external measures* (3.49)

3.101
observation points
output signals of an *element* (3.41) at which the potential effect of a *fault* (3.54) is observed

EXAMPLE Output of a memory.

3.102
operating mode
conditions of functional state that arise from the use and application of an *item* (3.84) or *element* (3.41)

EXAMPLE *System* (3.163) off; *system* (3.163) active; *system* (3.163) passive; degraded operation; *emergency operation* (3.43); *safe state* (3.131).

3.103
operating time
cumulative time that an *item* (3.84) or *element* (3.41) is functioning, including degraded modes

3.104
operational situation
scenario that can occur during a vehicle's life

EXAMPLE Driving at high speed; parking on a slope; maintenance.

3.105
other technology
technology different from E/E technologies that are within the scope of ISO 26262

EXAMPLE Mechanical technology; hydraulic technology.

Note 1 to entry: Other technologies can either be considered in the specification of the *functional safety concept* (3.68) (see ISO 26262-3:2018, Clause 7 and Figure 2), during the allocation of *safety* (3.132) requirements (see ISO 26262-3 and ISO 26262-4), or as an *external measure* (3.49).

3.106
partitioning
separation of functions or *elements* (3.41) to achieve a design

Note 1 to entry: Partitioning can be used for *fault* (3.54) containment to avoid *cascading failures* (3.17). To achieve *freedom from interference* (3.65) between partitioned design *elements* (3.41), additional non-functional requirements can be introduced.

3.107
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

3.108
perceived fault
fault (3.54) that may be perceived indirectly (through deviating behaviour on vehicle level)

3.109
permanent fault
fault (3.54) that occurs and stays until removed or repaired

Note 1 to entry: Direct current (d.c.) *faults* (3.54), e.g. stuck-at, and bridging *faults* (3.54) are permanent faults.

3.110
phase
stage in the *safety* (3.132) *lifecycle* (3.86) that is specified in ISO 26262-3, ISO 26262-4, ISO 26262-5, ISO 26262-6, and ISO 26262-7

Note 1 to entry: The distinct parts ISO 26262-3, ISO 26262-4, ISO 26262-5, ISO 26262-6 and ISO 26262-7 specify, respectively, the phases of:

— concept,

— product development at the *system* (3.163) level,

— product development at the hardware level,

— product development at the software level, and

— production, operation, service and decommissioning.

3.111
physics of failure https://www.kekaoxing.com
PoF
science-based approach to reliability based on *failure* (3.50) mechanism research

Note 1 to entry: PoF is typically applied using durability simulations performed in a Computer Aided Engineering (CAE) environment.

Note 2 to entry: PoF analysis may have an advantage when assessing reliability of new technologies and designs since years of field *failure* (3.50) history are not needed to make the reliability prediction.

3.112
power take-off
PTO
interface which enables a *truck* (3.174) or *tractor* (3.170) power source to operate equipment

EXAMPLE Interface to operate hydraulic pump, vacuum, lift, dump bed, cement mixer.

3.113
processing element
PE
hardware part (3.71) providing a set of functions for data processing, normally consisting of a register set, an execution unit, and a control unit

EXAMPLE 1 A hardware *component* (3.21) consisting of four cores can be described as having four PEs.

EXAMPLE 2 The streaming multi-processors in a GPU can be considered PEs.

3.114
programmable logic device
PLD
hardware *component* (3.21) or *hardware part* (3.71) which has an undefined circuit function at the time of manufacture and is configured during integration into a higher level *element* (3.41)

3.115
proven in use argument
evidence that, based on analysis of *field data* (3.62) resulting from use of a *candidate* (3.16), the probability of any *failure* (3.50) of this candidate that could impair a *safety goal* (3.139) of an *item* (3.84), meets the requirements for the applicable *ASIL* (3.6)

3.116
proven in use credit
substitution of a given set of *lifecycle* (3.86) *sub-phases* (3.161) with corresponding *work products* (3.185) by a *proven in use argument* (3.115)

3.117
quality management
QM
coordinated activities to direct and control an organization with regard to quality

Note 1 to entry: QM is not an *ASIL* (3.6), but may be specified in the *hazard analysis and risk assessment* (3.76).

3.118
random hardware failure
failure (3.50) that can occur unpredictably during the lifetime of a hardware *element* (3.41) and that follows a probability distribution

Note 1 to entry: Random hardware failure rates can be predicted with reasonable accuracy.

Note 2 to entry: Physical hardware *failures* (3.50) as defined by the *PoF* (3.111) methodology (SAE J1211, JEDEC JEP122, or similar) can be considered as random hardware failures for the purpose of this document.

3.119
random hardware fault
hardware *fault* (3.54) with a probabilistic distribution

3.120
reasonably foreseeable
technically possible and with a credible or measurable rate of occurrence

Note 1 to entry: Expected misuse can be understood as a sub-class of reasonably foreseeable event.

3.121
rebuilding
altering a T&B from its original configuration in order to perform a different task

Note 1 to entry: Rebuilding can include *modification* (3.91) of *T&B vehicle configuration* (3.175).

3.122
redundancy
existence of means in addition to the means that would be sufficient to perform a required function or to represent information

Note 1 to entry: Redundancy is used in ISO 26262 series of standards with respect to achieving a *safety goal* (3.139) or a specified *safety* (3.132) requirement, or to representing safety-related information.

Note 2 to entry: The redundancy could be implemented homogenously or with *diversity* (3.37).

EXAMPLE 1 Duplicated functional *components* (3.21) can be an instance of redundancy for the purpose of increasing *availability* (3.7) or allowing *fault* (3.54) detection.

EXAMPLE 2 The addition of parity bits to data representing safety-related information provides redundancy for the purpose of allowing *fault* (3.54) detection.

3.123
regression strategy
strategy to verify that an implemented change did not affect the unchanged, existing and previously verified parts or properties of an *item* (3.84) or *element* (3.41)

3.124
remanufacturing
dismantling and retrofitting a T&B vehicle with new or restored parts after a period of service according to the original specifications

3.125
residual fault
portion of a *random hardware fault* (3.119) that by itself leads to the violation of a *safety goal* (3.139), occurring in a hardware *element* (3.41), where that portion of the *random hardware fault* (3.119) is not controlled by a *safety mechanism* (3.142)

Note 1 to entry: This presumes that the hardware *element* (3.41) has *safety mechanism* (3.142) coverage for only a portion of its *faults* (3.54).

EXAMPLE If a set of *faults* (3.54) which is safety-relevant and not safe has a subset with 60 % coverage, then the remaining 40 % of the set of *faults* (3.54) are residual faults.

3.126
residual risk
risk (3.128) remaining after the deployment of *safety measures* (3.141)

3.127
review
examination of a *work product* (3.185), for achievement of its intended work product (3.185) goal, according to the purpose of the review

Note 1 to entry: From a development *phase* (3.110) perspective, *verification review* (3.181) and *confirmation review* (3.24).

3.128
risk
combination of the probability of occurrence of *harm* (3.74) and the *severity* (3.154) of that *harm* (3.74)

3.129
robust design
design that can function correctly in the presence of invalid inputs or stressful environmental conditions

Note 1 to entry: 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 the service life within design limits; and

— in the context of the ISO 26262 series of standards, robustness is the ability to provide safe behaviour at boundaries.

3.130
safe fault
fault (3.54) whose occurrence will not significantly increase the probability of violation of a *safety goal* (3.139)

Note 1 to entry: As shown in ISO 26262-5:2018, Annex B, both non-safety and *safety-related elements* (3.144) can have safe faults.

Note 2 to entry: *Single-point faults* (3.156), *residual faults* (3.125) and *dual-point faults* (3.39) do not constitute safe faults.

Note 3 to entry: Unless shown relevant in the *safety* (3.132) concept, *multiple-point faults* (3.97) with higher order than 2 can be considered as safe faults.

3.131
safe state
operating mode (3.102), in case of a *failure* (3.50), of an *item* (3.84) without an unreasonable level of *risk* (3.128)

Note 1 to entry: See Figure 5.

Note 2 to entry: While normal operation can be considered safe, the definition of safe state is only in the case of *failure* (3.50) in the context of the ISO 26262 series of standards.

EXAMPLE Switched-off mode (for *systems* (3.163) that are not fault tolerant).

3.132
safety
absence of *unreasonable risk* (3.176)

3.133
safety activity
activity performed in one or more *phases* (3.110) or *sub-phases* (3.161) of the *safety* (3.132) *lifecycle* (3.86)

3.134
safety anomaly
conditions that deviate from expectations and that can lead to *harm* (3.74)

Note 1 to entry: Safety anomalies can be discovered, among other times, during the *review* (3.127), *testing* (3.169), analysis, compilation, or use of *components* (3.21) or applicable documentation.

EXAMPLE Deviation can be on requirements, specifications, design documents, user documents, standards, or on experience.

3.135
safety architecture
set of *elements* (3.41) and their interaction to fulfil the *safety* (3.132) requirements

3.136
safety case
argument that *functional safety* (3.67) is achieved for *items* (3.84), or *elements* (3.41), and satisfied by evidence compiled from *work products* (3.185) of activities during development.

Note 1 to entry: Safety case can be extended to cover *safety* (3.132) issues beyond the scope the ISO 26262 series of standards.

3.137
safety culture
enduring values, attitudes, motivations and knowledge of an organization in which *safety* (3.132) is prioritized over competing goals in decisions and behaviour

Note 1 to entry: See ISO 26262-2:2018, Annex B.

3.138
safety element out of context
SEooC
safety-related element (3.144) which is not developed in the context of a specific *item* (3.84)

Note 1 to entry: A SEooC can be a *system* (3.163), a combination of *systems* (3.163), a *software component* (3.157), a *software unit* (3.159), a hardware *component* (3.21) or a *hardware part* (3.71).

EXAMPLE A generic wiper *system* (3.163) with assumed safety requirements to be integrated in different OEM *systems* (3.163).

3.139
safety goal
top-level *safety* (3.132) requirement as a result of the *hazard analysis and risk assessment* (3.76) at the vehicle level

Note 1 to entry: One safety goal can be related to several *hazards* (3.75), and several safety goals can be related to a single *hazard* (3.75).

3.140
safety manager
person or organization responsible for overseeing and ensuring the execution of activities necessary to achieve *functional safety* (3.67)

Note 1 to entry: At different levels of the *item's* (3.84) development, each company involved can appoint one or more different persons by splitting assignment in accordance with the internal matrix organization.

3.141
safety measure
activity or technical solution to avoid or control *systematic failures* (3.164) and to detect or control *random hardware failures* (3.118), or mitigate their harmful effects

Note 1 to entry: Safety measures include *safety mechanisms* (3.142).

EXAMPLE FMEA, or software without the use of global variables.

3.142
safety mechanism
technical solution implemented by E/E functions or *elements* (3.41), or by *other technologies* (3.105), to detect and mitigate or tolerate *faults* (3.54) or control or avoid *failures* (3.50) in order to maintain *intended functionality* (3.83) or achieve or maintain a *safe state* (3.131)

Note 1 to entry: Safety mechanisms are implemented within the *item* (3.84) to prevent *faults* (3.54) from leading to *single-point failures* (3.155) and to prevent *faults* (3.54) from being *latent faults* (3.85).

Note 2 to entry: The safety mechanism is either:

a) able to transition to, or maintain the *item* (3.84) in a *safe state* (3.131), or

b) able to alert the driver such that the driver is expected to control the effect of the *failure* (3.50), as defined in the *functional safety concept* (3.68).

3.143
safety plan
plan to manage and guide the execution of the *safety activities* (3.133) of a project including dates, milestones, tasks, deliverables, responsibilities and resources

3.144
safety-related element
element (3.41) that has the potential to contribute to the violation of or achievement of a *safety goal* (3.139)

Note 1 to entry: Fail-safe *elements* (3.41) are considered safety-related if they can contribute to at least one *safety goal* (3.139).

3.145
safety-related function
function that has the potential to contribute to the violation of or achievement of a *safety goal* (3.139)

3.146
safety-related incident
occurrence of a safety-related *failure* (3.50)

3.147
safety-related special characteristic
characteristic of an *item* (3.84) or *element* (3.41), or their production process, for which reasonably foreseeable deviation could impact, contribute to, or cause any potential reduction of *functional safety* (3.67)

Note 1 to entry: IATF 16949 defines the term special characteristics.

Note 2 to entry: Safety-related special characteristics are derived during the development *phase* (3.110) of the *item* (3.84) or *elements* (3.41).

Note 3 to entry: A safety related special characteristic is different from and should not be confused with a *safety mechanism* (3.142).

EXAMPLE Temperature range; expiration date; fastening torque; production tolerance; configuration.

3.148
safety validation
assurance, based on examination and tests, that the *safety goals* (3.139) are adequate and have been achieved with a sufficient level of integrity

Note 1 to entry: ISO 26262-4 provides suitable methods for safety validation.

3.149
semi-formal notation
description technique whose syntax is completely defined but whose semantics definition can be incomplete

EXAMPLE Structured And Design Techniques (SADT); Unified Modeling Language (UML).

3.150
semi-formal verification
verification (3.180) that is based on a description given in *semi-formal notation* (3.149)

EXAMPLE Use of test vectors generated from a semi-formal model to test that the *system* (3.163) behaviour matches the model.

3.151
semi-trailer
trailer (3.171) that is designed to be towed by means of a kingpin coupled to a *tractor* (3.170) that imposes a substantial vertical load on the towing vehicle

3.152
series production road vehicle
road vehicle that is intended to be used for public roads and is not a prototype

Note 1 to entry: Vehicle type classification may vary between regions.

EXAMPLE 1 A vehicle that is sold for use by the general public.

EXAMPLE 2 A vehicle that is sold to be used amongst the general public.

3.153
service note
documentation of *safety* (3.132) information to be considered when performing maintenance procedures for the *item* (3.84)

EXAMPLE *Safety-related special characteristic* (3.147); *safety* (3.132) operation that can be required.

3.154
severity
estimate of the extent of *harm* (3.74) to one or more individuals that can occur in a potentially *hazardous event* (3.77)

Note 1 to entry: The parameter "S" in *hazard analysis and risk assessment* (3.76) represents the potential severity of *harm* (3.74).

3.155
single-point failure
failure (3.50) that results from a *single-point fault* (3.156)

3.156
single-point fault
hardware *fault* (3.54) in an *element* (3.41) that leads directly to the violation of a *safety goal* (3.139) and no *fault* (3.54) in that *element* (3.41) is covered by any *safety mechanism* (3.142)

Note 1 to entry: See also *single-point failure* (3.155).

Note 2 to entry: If at least one *safety mechanism* (3.142) is defined for a hardware *element* (3.41) (e.g. a watchdog for a microcontroller), then no *faults* (3.54) of the considered hardware *element* (3.41) are single-point faults.

3.157
software component
one or more *software units* (3.159)

3.158
software tool
computer program used in the development of an *item* (3.84) or *element* (3.41)

3.159
software unit
atomic level *software component* (3.157) of the software *architecture* (3.1) that can be subjected to stand-alone *testing* (3.169)

3.160
statement coverage
percentage of statements within the software that have been executed

3.161
sub-phase
subdivision of a *phase* (3.110) in the *safety* (3.132) *lifecycle* (3.86) that is specified in a clause of ISO 26262

EXAMPLE *hazard analysis and risk assessment* (3.76) is a sub-phase of the *safety* (3.132) *lifecycle* (3.86) specified in ISO 26262-3:2018, Clause 6.

3.162
supply agreement
agreement between customer and supplier in which the responsibilities for activities, evidence or *work products* (3.185) to be performed and/or exchanged by each party related to the production of *items* (3.84) and *elements* (3.41), are specified

Note 1 to entry: While *DIA* (3.32) applies to the development phase, supply agreement applies to production.

3.163
system
set of *components* (3.21) or subsystems that relates at least a sensor, a controller and an actuator with one another

Note 1 to entry: The related sensor or actuator can be included in the system, or can be external to the system.

3.164
systematic failure
failure (3.50) related in a deterministic way to a certain cause, that can only be eliminated by a change of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

3.165
systematic fault
fault (3.54) whose *failure* (3.50) is manifested in a deterministic way that can only be prevented by applying process or design measures

3.166
target environment
environment on which specific software is intended to be executed

Note 1 to entry: For application software the target environment is the microcontroller with basic software and operating system. For *embedded software* (3.42) the target environment is the ECU in the *system* (3.163) context.

3.167
technical safety concept
specification of the *technical safety requirements* (3.168) and their allocation to *system* (3.163) *elements* (3.41) with associated information providing a rationale for *functional safety* (3.67) at the *system* (3.163) level

3.168
technical safety requirement
requirement derived for implementation of associated *functional safety requirements* (3.69)

Note 1 to entry: The derived requirement includes requirements for mitigation.

3.169
testing
process of planning, preparing, and operating or exercising an *item* (3.84) or *element* (3.41) to verify that it satisfies specified requirements, to detect *safety anomalies* (3.134), to validate that requirements are suitable in the given context and to create confidence in its behaviour

3.170
tractor
truck (3.174) that is designed to tow a *semi-trailer* (3.151)

3.171
trailer
road vehicle which is designed to be towed such that no substantial part of the total weight is supported by the towing vehicle

Note 1 to entry: A trailer can be designed to transport goods, equipment, or persons.

3.172
transducer
hardware part (3.71) that converts one form of energy into another and has a sensitivity that determines the magnitude of its output energy form relative to the magnitude of its input energy form

3.173
transient fault
fault (3.54) that occurs once and subsequently disappears

Note 1 to entry: Transient faults can appear due to electromagnetic interference, which can lead to bit-flips. Soft *errors* (3.46) such as Single Event Upset (SEU) and Single Event Transient (SET) are transient faults.

3.174
truck
motor vehicle designed to transport goods, or equipment on-board the chassis

Note 1 to entry: It may also tow a *trailer* (3.171).

3.175
T&B vehicle configuration
technical characteristics of a T&B *base vehicle* (3.9) and *body builder equipment* (3.12) that do not change during operation

Note 1 to entry: Changes may occur during *rebuilding* (3.121).

EXAMPLE Wheel base, axle load distribution, wheels (number of axles, driven axles, steered axles).

3.176
unreasonable risk
risk (3.128) judged to be unacceptable in a certain context according to valid societal moral concepts

3.177
variance in T&B vehicle operation
use of a T&B vehicle with different dynamic characteristics influenced by cargo or towing during the service life of the vehicle

EXAMPLE T&B with or without load, T&B with variations in load distribution, *truck* (3.174) with or without *trailer* (3.171), *tractor* (3.170) with or without *semi-trailer* (3.151) (*tractor* (3.170) solo).

3.178
vehicle function
behaviour of the vehicle, intended by the implementation of one or more *items* (3.84), that is observable by the customer

EXAMPLE An "automatic cruise control" is a vehicle function that can be implemented, using different ECUs and a variety of sensor technology (e.g. Radar, Lidar, Camera).

3.179
vehicle operating state
operating mode (3.102) in combination with the *operational situation* (3.104)

Note 1 to entry: The vehicle operating state is determined by the currently provided performance of the specified functionality (e.g. highly automated driving) within the current driving situation (e.g. on the highway at 120 km/h). The *ASIL (*3.6) rating of the *hazardous event* (3.77) (e.g. sudden loss of the specified functionality) is dependent on the current vehicle operating state (e.g. sudden loss of highly automated driving capability is more critical at high speeds than at very low speeds); sudden loss of highly automated driving capability at high speeds is not an issue if the *system* (3.163) is not in operation, i.e. the *system* (3.163) fails while the driver is in control.

3.180
verification
determination whether or not an examined object meets its specified requirements

EXAMPLE The typical verification activities can be classified as follows:

— *verification review* (3.181), *walk-through* (3.182), *inspection* (3.82);

— verification *testing* (3.169);

— simulation;

— prototyping; and

— analysis (*safety* (3.132) analysis, control flow analysis, data flow analysis, etc.).

3.181
verification review
verification (3.180) activity to ensure that the result of a development activity fulfils the project requirements, or technical requirements, or both

Note 1 to entry: Individual requirements on verification reviews are given in specific clauses of individual parts of the ISO 26262 series of standards.

Note 2 to entry: The goal of verification reviews is technical correctness and completeness of the *item* (3.84) or *element* (3.41).

EXAMPLE Verification review types can be technical *review* (3.127), *walk-through* (3.182) or *inspection* (3.82).

3.182
walk-through
systematic examination of *work products* (3.185) in order to detect *safety anomalies* (3.134)

Note 1 to entry: Walk-through is a means of *verification* (3.180).

Note 2 to entry: Walk-through differs from *testing* (3.169) in that it does not normally involve the operation of the associated *item* (3.84) or *element* (3.41).

Note 3 to entry: Any anomalies that are detected are usually addressed by rework, followed by a walk-through of the reworked *work products* (3.185).

EXAMPLE During a walk-through, the developer explains the *work product* (3.185) step-by-step to one or more reviewers. The objective is to create a common understanding of the *work product* (3.185) and to identify any *safety anomalies* (3.134) within the *work product* (3.185). Both *inspections* (3.82) and walk-throughs are types of peer *review* (3.127), where a walk-through is a less stringent form of peer *review* (3.127) than an *inspection* (3.82).

3.183
warning and degradation strategy
specification of how to alert the driver of potentially reduced functionality and of how to provide this reduced functionality to reach a *safe state* (3.131)

Note 1 to entry: The warning and degradation strategy includes:

— the specification of haptic, audio or visual cues to alert the driver for upcoming *degradation* (3.28);

— the description of one or more *safe states* (3.131) associated with the corresponding *safety goals* (3.139);

— the conditions for transitioning to a *safe state* (3.131);

— the conditions for recovering from a *safe state* (3.131) and, if applicable, the corresponding *maximum time to repair time interval* (3.89); and

— if applicable, *emergency operation* (3.43) and associated *emergency operation tolerance time interval* (3.45).

3.184
well-trusted
previously used without known *safety anomalies* (3.134) in a comparable application

EXAMPLE Well-trusted design principle; well-trusted tool; well-trusted hardware *component* (3.21).

3.185
work product
documentation resulting from one or more associated requirements of ISO 26262

Note 1 to entry: The documentation can be in the form of a single document containing the complete information for the work product or a set of documents that together contain the complete information for the work product.

4 Abbreviated terms

ACC	Adaptive Cruise Control
ADC	Analogue to Digital Converter
AEC	Automotive Electronics Council
AIS	Abbreviated Injury Scale
ALU	Arithmetic Logic Unit
ASIC	Application-Specific Integrated Circuit
ASIL	Automotive Safety Integrity Level (see definition 3.6)
BB	Body Builder (see definition 3.11)
BFR	Base Failure Rate (see definition 3.8)
BIST	Built-In Self-Test
CAN	Controller Area Network

CCF	Common Cause Failure (see definition 3.18)
CCP	Controllability Classification Panel (see ISO 26262-12:2018, Annex C)
CMOS	Complementary Metal Oxide Semiconductor
COTS	Commercial Off The Shelf
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DC	Diagnostic Coverage (see definition 3.33)
DAC	Digital to Analogue Converter
DFA	Dependent Failure Analysis
DFI	Dependent Failure Initiator (see definition 3.30)
DIA	Development Interface Agreement (see definition 3.32)
DMA	Direct Memory Access
DMOS	Double diffused Metal Oxide Semiconductor (HV MOS)
DSP	Digital Signal Processor
ECC	Error Correction Code
ECU	Electronic Control Unit
EDC	Error Detection Code
E/E system	Electrical and/or Electronic system (see definition 3.40)
EEC	Evaluation of Each Cause of safety goal violation
EMC	ElectroMagnetic Compatibility
EMI	ElectroMagnetic Interference
EOTI	Emergency Operation Time Interval (see definition 3.44)
EOTTI	Emergency Operation Tolerance Time Interval (see definition 3.45)
ESD	ElectroStatic Discharge
ESC	Electronic Stability Control
ETA	Event Tree Analysis
EVR	Embedded Voltage Regulator
FDTI	Fault Detection Time Interval (see definition 3.55)
FET	Field Effect Transistor
FHTI	Fault Handling Time Interval (see definition 3.56)
FIT	Failures In Time (in this standard a FIT is 10E-9 failures per operational hour)

FMC	Failure Mode Coverage (see definition 3.52)
FMEA	Failure Mode and Effects Analysis
FPGA	Field Programmable Gate Array
FRTI	Fault Reaction Time Interval (see definition 3.59)
FTA	Fault Tree Analysis
FTTI	Fault Tolerant Time Interval (see definition 3.61)
GPU	Graphics Processing Unit
HARA	Hazard Analysis and Risk Assessment (see definition 3.76)
HAZOP	HAZard and OPerability analysis
HSI	Hardware-Software Interface
HS/LS	High Side / Low Side
HW	HardWare
IC	Integrated Circuit
I/O	Input – Output
ISA	Instruction Set Architecture
LDO	Low Drop Output regulator
LFM	Latent-Fault Metric
LS	Low Side
LSB	Least Significant Bit
MBD	Model Based Development
MC/DC	Modified Condition/Decision Coverage (see definition 3.92)
MCU	Multi-point Control Unit
MMU	Memory Management Unit
MPU	Memory Protection Unit
MSIL	Motorcycle Safety Integrity Level (see definition 3.94)
MUX	MUltipleXer
OEM	Original Equipment Manufacturer
OS	Operating System
OV	Over Voltage
PAL	Programmable Array Logic
PE	Processing Element (see definition 3.113)

PLD	Programmable Logic Device (see definition 3.114)
PLL	Phase Locked Loop
PMHF	Probabilistic Metric for random Hardware Failures
PoF	Physics of Failure (see definition 3.111)
PPAP	Production Part Approval Process
PTO	Power Take-Off (see definition 3.112)
QM	Quality Management
RAM	Random Access Memory
RF	Residual Fault (see definition 3.125)
RFQ	Request For Quotation
ROM	Read Only Memory
RTL	Register Transfer Level
SEB	Single Event Burnout
SEE	Single Event Effect
SEGR	Single Event Gate Rupture
SEooC	Safety Element out of Context (see definition 3.138)
SET	Single Event Transient
SEU	Single Event Upset
SG	Safety Goal (see definition 3.139)
SMPS	Switched Mode Power Supply
SoC	System on Chip
SOP	Start Of Production
SPFM	Single-Point Fault Metric
SPI	Serial Peripheral Interface
SW	SoftWare
T&B	Trucks, Buses, trailers and semi-trailers (see definitions 3.174, 3.14, 3.171, and 3.151)
TCL	Tool Confidence Level
TD	Tool error Detection
TI	Tool Impact

UML	Unified Modeling Language
UV	Under Voltage
XML	eXtensible Markup Language

Bibliography

[1] ISO 3779, *Road vehicles — Vehicle identification number (VIN) — Content and structure*

[2] IATF 16949, *Quality management system requirements for automotive production and relevant service parts organizations*

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

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

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

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

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

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

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

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

[11] ISO 26262-10:2018, *Road vehicles — Functional safety — Part 10: Guideline on ISO 26262*

[12] ISO 26262-11:2018, *Road vehicles — Functional safety — Part 11: Guideline on application of ISO 26262 to semiconductors*

[13] ISO 26262-12:2018, *Road vehicles — Functional safety — Part 12: Adaptation of ISO 26262 for motorcycles*

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

[15] ECE/TRANS/WP *.29/78/Rev.3+Amend.1 (Consolidated Resolution on the Construction of Vehicles (R.E.3))*

[16] TRANS/WP. *29/1045+Amend.1&2*

[17] SAE J1211, *Physics of Failure methodology*

[18] ISO 3833, *Road vehicles — Types — Terms and definitions*

[19] ISO 9000:2015, *Quality management systems — Fundamentals and vocabulary*

ICS 01.040.43; 43.040.10
Price group A