

Redline version
compares Second edition to
First edition



Road vehicles — Functional safety —
Part 1:
Vocabulary

Véhicules routiers — Sécurité fonctionnelle —
Partie 1: Vocabulaire

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO 26262-1:2018

<https://standards.iteh.ai/catalog/standards/iso/c1a72b85-fd93-4952-bc1e-38aedd5d0742/iso-26262-1-2018>






Reference number
ISO 26262-1:redline:2018(E)

© ISO 2018

IMPORTANT

This marked-up version uses the following colour-coding in the marked-up text:

- | | |
|--|---|
|  Text example 1 | — Text has been added (in green) |
| Text example 2 | — Text has been deleted (in red) |
|  | — Graphic figure has been added |
|  | — Graphic figure has been deleted |
| 1.x ... | — If there are changes in a clause/subclause, the corresponding clause/subclause number is highlighted in yellow in the Table of contents |

iTeh Standards

(<https://standards.iteh.ai>)

DISCLAIMER

This marked-up version highlights the main changes in this edition of the document compared with the previous edition. It does not focus on details (e.g. changes in punctuation).

ISO 26262-1:2018

This marked-up version does not constitute the official ISO document and is not intended to be used for implementation purposes.



COPYRIGHT PROTECTED DOCUMENT

© ISO 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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	iv
Introduction	vi
1 Scope	1
2 Normative references	1
13 Terms and definitions	2
24 Abbreviated terms	32
Bibliography	37
Alphabetical index	37

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO 26262-1:2018

<https://standards.iteh.ai/catalog/standards/iso/c1a72b85-fd93-4952-bc1e-38aedd5d0742/iso-26262-1-2018>

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~~ 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 ~~rules given in~~ editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

~~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. 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.

~~ISO 26262-1~~ This document was prepared by Technical Committee ISO/TC 22, Road vehicles Subcommittee, Subcommittee SC 332, Electrical and electronic equipment components and general system aspects.

This edition of ISO 26262 series ~~consists of the following parts~~ of standards cancels and replaces the edition ISO 26262:2011, under the general title series of standards, which has been technically revised and includes the ~~Road vehicles Functional safety~~ following main changes:

- ~~Part 1: Vocabulary~~ requirements for trucks, buses, trailers and semi-trailers;
- ~~Part 2: Management of functional safety~~ extension of the vocabulary;
- ~~Part 3: Concept phase~~ more detailed objectives;
- ~~Part 4: Product development at the system level~~ objective oriented confirmation measures;
- ~~Part 5: Product development at the hardware level~~ management of safety anomalies;
- references to cyber security;
- updated target values for hardware architecture metrics;
- ~~Part 6: Product development at the software level~~ guidance on model based development and software safety analysis;
- ~~Part 7: Production and operation~~ evaluation of hardware elements;

- ~~Part 8. Supporting processes~~ additional guidance on dependent failure analysis;
- ~~Part 9. Automotive Safety Integrity Level (ASIL) oriented and safety oriented analyses~~ guidance on fault tolerance, safety-related special characteristics and software tools;
- ~~Part 10. Guideline on ISO 26262~~ 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.

iTeh Standards (<https://standards.iteh.ai>) Document Preview

ISO 26262-1:2018

<https://standards.iteh.ai/catalog/standards/iso/c1a72b85-fd93-4952-bc1e-38aedd5d0742/iso-26262-1-2018>

Introduction

The ISO 26262 series of standards is the adaptation of IEC 61508 series to comply with needs specific to the application sector 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 of future automobile development. New functionalities not only in areas such as driver assistance, propulsion, in vehicle dynamics control and active and passive safety systems increasingly touch the domain of system safety engineering in the development of road vehicles. Development and integration of these automotive functionalities will strengthen the need for safe system development processes, functional safety and the need to provide evidence that all reasonable system 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 avoid mitigate these risks by providing appropriate requirements and processes.

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

- a) provides a reference for the automotive safety lifecycle (management, and supports the tailoring of the activities to be performed during the lifecycle phases, i.e., development, production, operation, service, decommissioning) and supports tailoring the necessary activities during these lifecycle phases and decommissioning;
- b) provides an automotive-specific risk-based approach to determine integrity levels [Automotive Safety Integrity Levels (ASIL ASILs)];
- c) uses ASILs to specify applicable which of the requirements of ISO 26262 so as are applicable to avoid unreasonable residual risk;
- d) provides requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety being achieved, functional safety management, design, implementation, verification, validation and confirmation measures; and
- e) provides requirements for relations with 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.

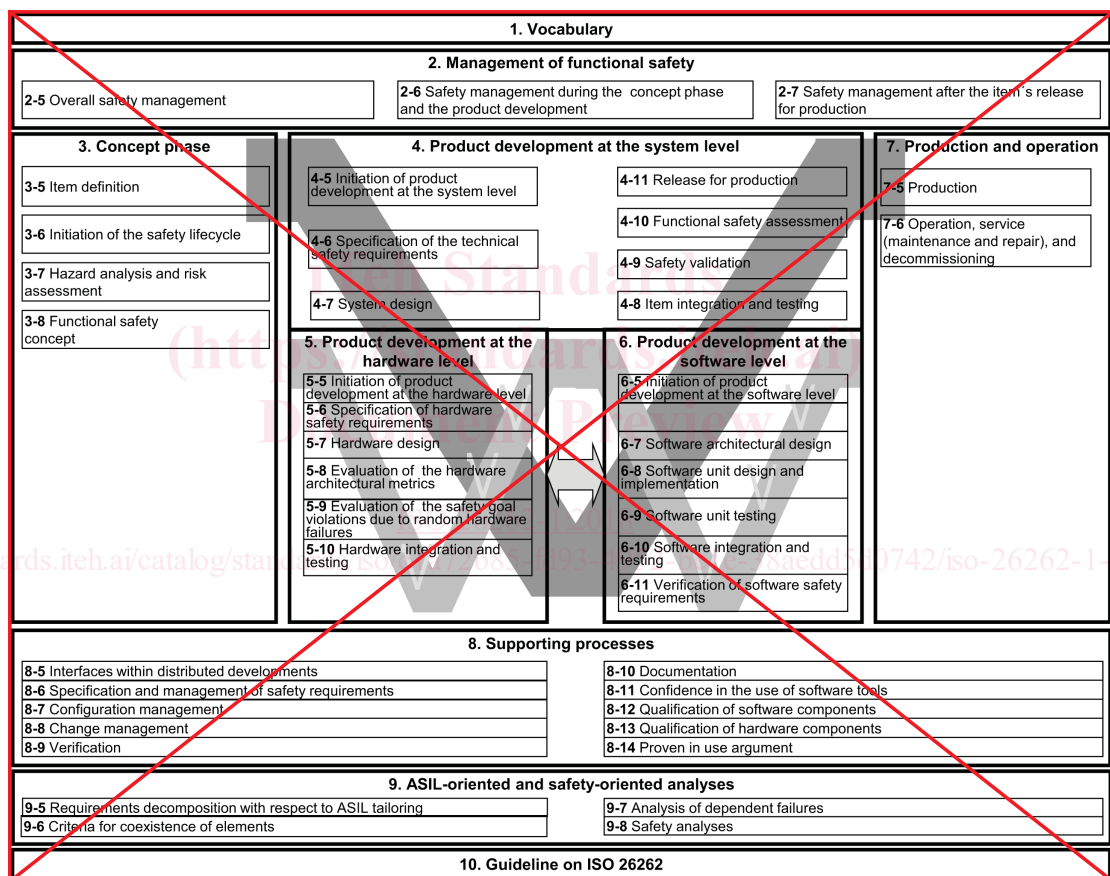
Functional The achievement of functional safety is influenced by the development process (including such activities as requirements specification, design, implementation, integration, verification, validation and configuration), the production and service processes and by the management processes.

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

Figure 1 shows the overall structure of this edition 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 between 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 Clause 6 of ISO 26262-2:2018, Clause 6.



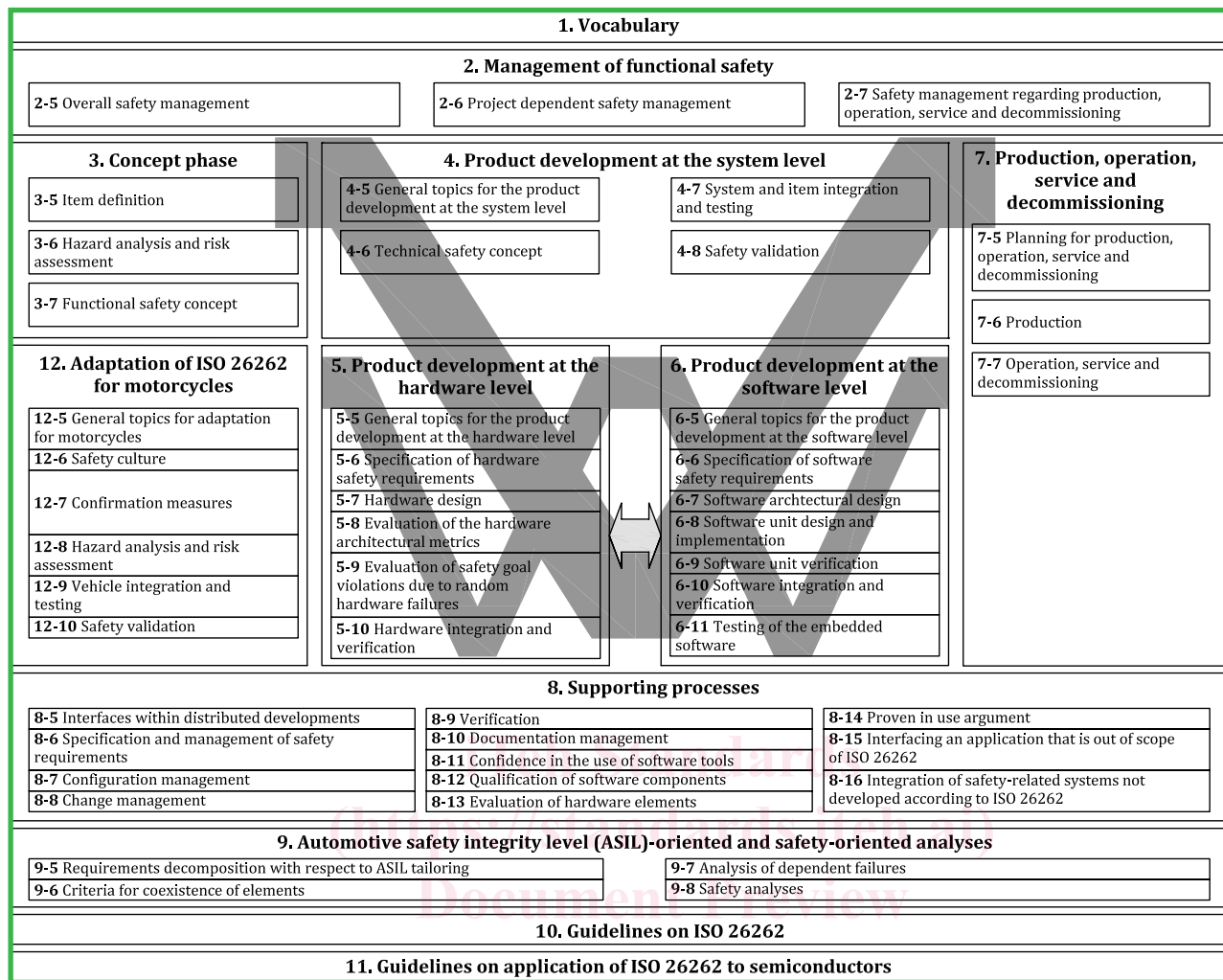


Figure 1 — Overview of the ISO 26262 series of standards

Road vehicles — Functional safety —

Part 1: Vocabulary

1 Scope

~~ISO 26262~~ 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 ~~passenger cars with a maximum gross vehicle mass up to 3 500 kg~~ road vehicles, excluding mopeds. ~~ISO 26262~~ This document does not address unique E/E systems in special purpose vehicles such as ~~vehicles~~ 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 ~~ISO 26262~~ this document, are exempted from the scope: ~~For further development or alterations based on~~ of this edition. This document addresses alterations to existing systems and their components released for production prior to the publication of ~~ISO 26262~~; ~~only the modifications will be developed in accordance with~~ this document by tailoring the safety lifecycle depending on the alteration. This document addresses integration of existing systems not developed ~~ISO 26262~~ according to this document and systems developed according to this document by tailoring the safety lifecycle.

~~ISO 26262~~ This document addresses possible hazards caused by malfunctioning behaviour of ~~E/E~~ 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 ~~E/E~~ safety-related E/E systems.

~~ISO 26262 does not address the nominal performance of~~ This document describes a framework for functional safety to assist the development of safety-related E/E systems; ~~even if dedicated functional performance standards exist for these systems (e.g. active and passive safety systems, brake systems, Adaptive Cruise Control).~~ This 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 ~~part~~ document defines the vocabulary of ~~ISO 26262~~ specifies the terms, definitions and abbreviated terms for application in all ~~parts~~ terms used in the ISO 26262 series of ~~ISO 26262~~ 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 following terms and definitions given in ISO 26262 (all parts) and the following apply.

1.1 allocation

~~assignment of a requirement to an architectural element (1.32)~~

~~Note 1 to entry. Intent is not to divide an atomic requirement into multiple requirements. Tracing of an atomic system (1.129) level requirement to multiple lower level atomic requirements is allowed.~~

1.2 anomaly

~~condition that deviates from expectations, based, for example, on requirements, specifications, design documents, user documents, standards, or on experience~~

~~Note 1 to entry. Anomalies can be discovered, among other times, during the review (1.98), testing (1.134), analysis, compilation, or use of components (1.15) or applicable documentation.~~

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/>

1.3.1 architecture

representation of the structure of the *item* (1.693.84) or functions or systems (1.129) *element* (3.41) or *elements* (1.32) that allows identification of building blocks, their boundaries and interfaces, and includes the *allocation* (1.1) *allocation* of functions to hardware and software elements *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), conducting 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).

1.4.3.4 assessment

examination of whether a characteristic of an *item* (1.693.84) or *element* (1.323.41) achieves the ISO 26262 objectives

~~Note 1 to entry. A level of independence (1.61) of the party or parties performing the assessment is associated with each assessment.~~

1.5.3.5**audit**

examination of an implemented process with regard to the process objectives

1.6.3.6**automotive safety integrity level**

ASIL

one of four levels to specify the *item's* (1.6.3.84) or *element's* (1.6.3.41) necessary requirements of ISO 26262 requirements and safety measures (1.6.3.141) to apply for avoiding an unreasonable residualunreasonable risk (1.6.3.176), with D representing the most stringent and A the least stringent level

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

1.7**ASIL decomposition**

apportioning of safety requirements redundantly to sufficiently independent elements (1.32), with the objective of reducing the ASIL (1.6) of the redundant safety requirements that are allocated to the corresponding elements

1.8.3.7**availability**

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

1.9.3.10**baseline**

version of a the approved set of one or more work productswork products (3.185), items (1.6.3.84) or elements (1.6.3.41) that is under configuration management and usedserves as a basis for further development through the change management processchange

Note 1 to entry: See ISO 26262-8:2011 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)

~~1.10~~ 3.13

branch coverage

percentage of branches of the control flow ~~that have been executed~~ of a computer program executed during a test

Note 1 to entry: 100 % branch coverage implies 100 % ~~statement~~statement coverage (~~1.12~~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).

~~1.11~~ 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 ~~cannot~~does not contain executable or interpretable code.

~~1.12~~ 3.16

candidate

item (~~1.69~~3.84) or *element* (~~1.32~~3.41) whose definition and conditions of use are identical to, or have a very high degree of commonality with, an ~~item~~item (3.84) or ~~element~~element (3.41) that is already released and in operation

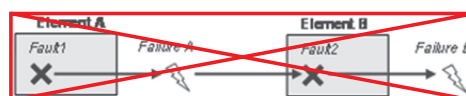
Note 1 to entry: This definition applies where candidate is used in the context of a *proven in use argument* (~~1.20~~3.115).

~~1.13~~ 3.17

cascading failure

failure (~~1.39~~3.50) of an *element* (~~1.32~~3.41) of an *item* (~~1.69~~3.84) resulting from a root cause [inside or outside of the *element* (3.41) ~~causing~~] and then causing a *failure* (3.50) of another ~~element~~element (3.41) or ~~elements~~elements (3.41) of the same ~~item~~ or different *item* (3.84)

Note 1 to entry: Cascading failures are *dependent failures* (~~1.22~~3.29) that ~~are not~~ could be one of the possible root causes of a *common cause failures* (1.14*failure* (3.18). See Figure 2, Failure A.



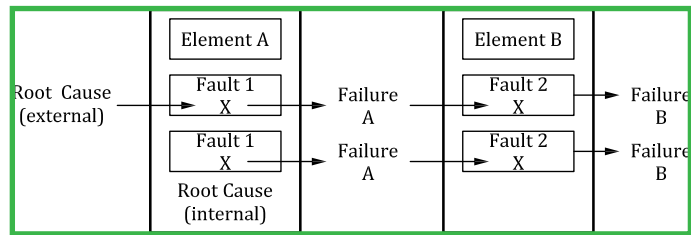


Figure 2 — Cascading failure

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.

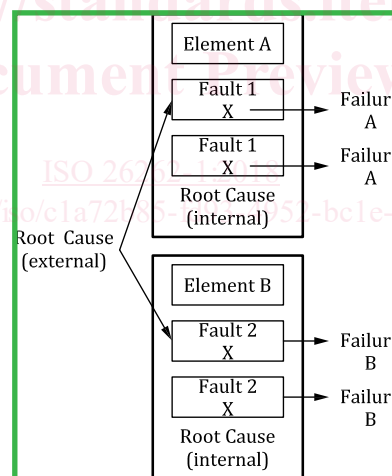
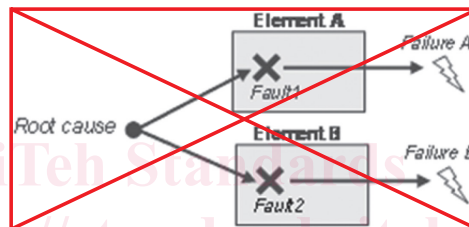


Figure 3 — Common cause failure

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).

1.15 3.21

component

non-~~system~~ (1.129) *system* level *element* (1.32 3.41) that is logically ~~and~~ or technically separable and is comprised of more than one *hardware part* (1.55 3.71) or ~~of~~ one or more *software units* (1.125 3.159)

EXAMPLE A microcontroller.

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

1.16 3.22

configuration data

data that is assigned during ~~software~~ *element* build and that controls the ~~software~~ *element* build process

EXAMPLE 1 Pre-processor ~~instructions, software build scripts (e.g. XML configuration files)~~ *variable settings* which are used to derive compile time variants from the source code.

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

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

NOTE 2 ~~Note 1 to entry: Configuration data controls the software build. Only code, or data selected by configuration data can~~ 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).

1.17 3.23

confirmation measure

confirmation review (1.18 3.24), *audit* (1.53.5) or *assessment* (1.43.4) concerning *functional safety* (1.51 3.67)

1.18 3.24

confirmation review

confirmation that a ~~work product meets~~ *work product* (3.185) ~~the requirements~~ provides sufficient and convincing evidence of their contribution to the achievement of ~~ISO 26262 with~~ *functional safety* (3.67) ~~the required level of considering the~~ *independence* (1.61) of the reviewer ~~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.

1.19 3.25

controllability

ability to avoid a specified *harm* (1.56 3.74) or damage through the timely reactions of the persons involved, possibly with support from *external measures* (1.38 3.49)

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