BS ISO 26262-1:2011

BSI Standards Publication

Road vehicles — Functional safety

Part 1: Vocabulary

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of ISO 26262-1:2011.

The UK participation in its preparation was entrusted to Technical Committee AUE/16, Electrical and electronic equipment.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© BSI 2011

ISBN 978 0 580 62303 5

ICS 01.040.43; 43.040.10

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2011.

Amendments issued since publication

Date	Text affected

BS ISO 26262-1:2011

INTERNATIONAL STANDARD

ISO 26262-1

First edition
2011-11-15

Road vehicles — Functional safety —

Part 1: Vocabulary

Véhicules routiers — Sécurité fonctionnelle —

Partie 1: Vocabulaire

Reference number
ISO 26262-1:2011(E)

© ISO 2011

COPYRIGHT PROTECTED DOCUMENT

© ISO 2011

The reproduction of the terms and definitions contained in this International Standard is permitted in teaching manuals, instruction booklets, technical publications and journals for strictly educational or implementation purposes. The conditions for such reproduction are: that no modifications are made to the terms and definitions; that such reproduction is not permitted for dictionaries or similar publications offered for sale; and that this International Standard is referenced as the source document.

With the sole exceptions noted above, no other part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

Published in Switzerland

 © ISO 2011 – All rights reserved

Contents

Page

Foreword iv

Introduction....v

Scope....1

1 Terms and definitions....1

2 Abbreviated terms....18

Bibliography....21

Alphabetical index....22

© ISO 2011 – All rights reserved

Foreword

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

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

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

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

ISO 26262-1 was prepared by Technical Committee ISO/TC 22, Road vehicles, Subcommittee SC 3, Electrical and electronic equipment.

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

— Part 1: Vocabulary

— Part 2: Management of functional safety

— Part 3: Concept phase

— Part 4: Product development at the system level

— Part 5: Product development at the hardware level

— Part 6: Product development at the software level

— Part 7: Production and operation

— Part 8: Supporting processes

— Part 9: Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses

— Part 10: Guideline on ISO 26262

© ISO 2011 – All rights reserved

Introduction

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

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

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

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

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

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

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

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

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

e) provides requirements for relations with suppliers.

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

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

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

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

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

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

© ISO 2011 – All rights reserved

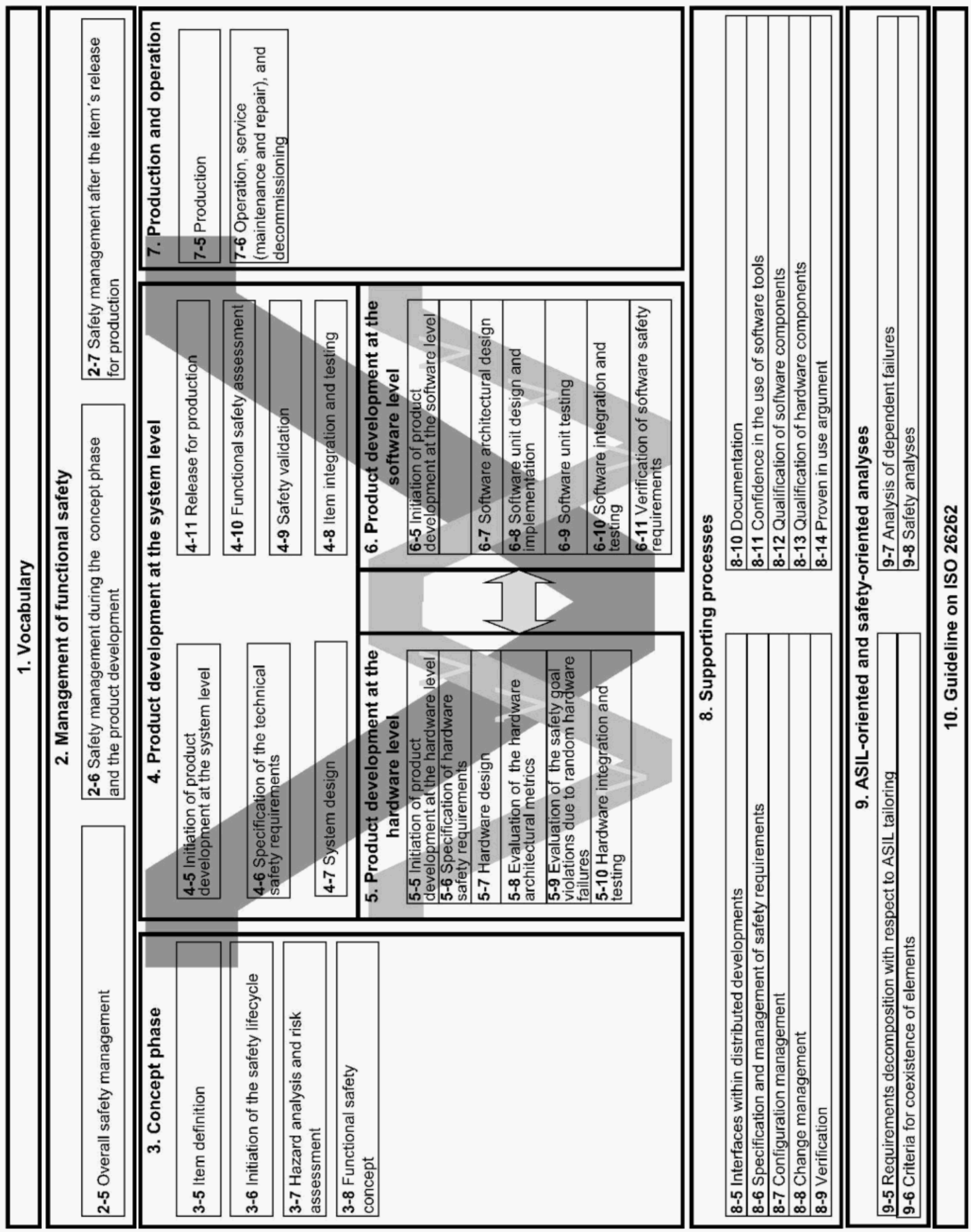

Figure 1 — Overview of ISO 26262

© ISO 2011 – All rights reserved

Road vehicles — Functional safety —

Part 1: Vocabulary

Scope

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

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

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

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

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

1 Terms and definitions

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

1.1
allocation
assignment of a requirement to an architectural element (1.32)

NOTE 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 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 2011 – All rights reserved

1.3

architecture

representation of the structure of the item (1.69) or functions or systems (1.129) or elements (1.32) that allows identification of building blocks, their boundaries and interfaces, and includes the allocation (1.1) of functions to hardware and software elements

1.4

assessment

examination of a characteristic of an item (1.69) or element (1.32)

NOTE A level of independence (1.61) of the party or parties performing the assessment is associated with each assessment.

1.5

audit

examination of an implemented process

1.6

Automotive Safety Integrity Level

ASIL

one of four levels to specify the item's (1.69) or element's (1.32) necessary requirements of ISO 26262 and safety measures (1.110) to apply for avoiding an unreasonable residual risk (1.97), with D representing the most stringent and A the least stringent level

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

availability

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

1.9

baseline

version of a set of one or more work products, items (1.69) or elements (1.32) that is under configuration management and used as a basis for further development through the change management process

NOTE See ISO 26262-8:2011, Clause 8.

1.10

branch coverage

percentage of branches of the control flow that have been executed

NOTE 1 100 % branch coverage implies 100 % statement coverage (1.127).

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

1.11

calibration data

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

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 Calibration data cannot contain executable or interpretable code.

© ISO 2011 – All rights reserved

1.12

candidate

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

NOTE This definition applies where candidate is used in the context of a proven in use argument (1.90).

1.13

cascading failure

failure (1.39) of an element (1.32) of an item (1.69) causing another element or elements of the same item to fail

NOTE Cascading failures are dependent failures (1.22) that are not common cause failures (1.14). See Figure 2, Failure A.

Figure 2 — Cascading failure

1.14

common cause failure

CCF

failure (1.39) of two or more elements (1.32) of an item (1.69) resulting from a single specific event or root cause

NOTE Common cause failures are dependent failures (1.22) that are not cascading failures (1.13). See Figure 3.

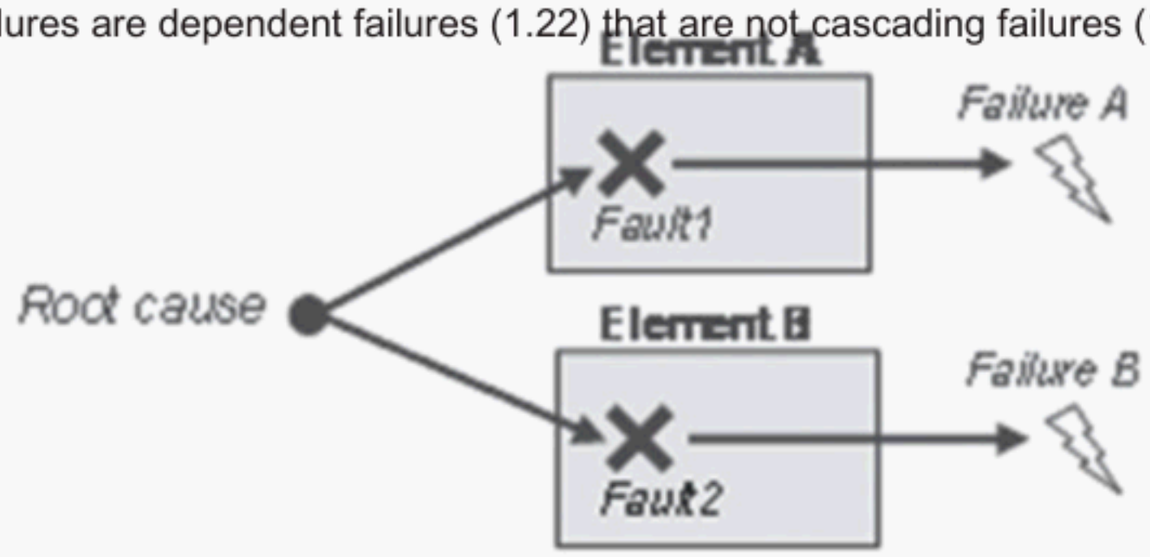

Figure 3 — Common cause failure

1.15

component

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

NOTE A component is a part of a system.

1.16

configuration data

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

EXAMPLE Pre-processor instructions; software build scripts (e.g. XML configuration files).

© ISO 2011 – All rights reserved

NOTE 1 Configuration data cannot contain executable or interpretable code.

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

1.17

confirmation measure
confirmation review (1.18), audit (1.5) or assessment (1.4) concerning functional safety (1.51)

1.18

confirmation review
confirmation that a work product meets the requirements of ISO 26262 with the required level of independence (1.61) of the reviewer

NOTE 1 A complete list of confirmation reviews is given in ISO 26262-2.

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

1.19

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

NOTE 1 Persons involved can include the driver, passengers or persons in the vicinity of the vehicle's exterior.

NOTE 2 The parameter C in hazard analysis and risk assessment (1.58) represents the potential for controllability.

1.20

dedicated measure
measure to ensure the failure rate (1.41) claimed in the evaluation of the probability of violation of safety goals (1.108)

EXAMPLE Design feature [such as hardware part (1.55) 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 (1.99) of occurrence of failure modes (1.40) which contribute to the violation of safety goals; burn-in test; dedicated control plan.

1.21

degradation
strategy for providing safety (1.103) by design after the occurrence of failures (1.39)

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

1.22

dependent failures
failures (1.39) whose probability of simultaneous or successive occurrence cannot be expressed as the simple product of the unconditional probabilities of each of them

NOTE 1 Dependent failures A and B can be characterized when

$P_{AB} \quad P_A \quad P_B$

where

P_{AB} is the probability of the simultaneous occurrence of failure A and failure B;

P_A is the probability of the occurrence of failure A;

P_B is the probability of the occurrence of failure B.

NOTE 2 Dependent failures include common cause failures (1.14) and cascading failures (1.13).

© ISO 2011 – All rights reserved

1.23

detected fault

fault (1.42) whose presence is detected within a prescribed time by a safety mechanism (1.111) that prevents the fault from being latent

EXAMPLE The fault can be detected by a dedicated safety mechanism (1.111) (e.g. detection of the error (1.36) and notifying the driver via an alerting device on the instrument panel) as defined in the functional safety concept (1.52).

1.24

development interface agreement

DIA

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

1.25

diagnostic coverage

proportion of the hardware element (1.32) failure rate (1.41) that is detected or controlled by the implemented safety mechanisms (1.111)

NOTE 1 Diagnostic coverage can be assessed with regard to residual faults (1.96) or with regard to latent multiple-point faults (1.77) that might occur in a hardware element.

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

NOTE 3 Safety mechanisms implemented at different levels in the architecture (1.3) can be considered.

1.26

diagnostic test interval

amount of time between the executions of online diagnostic tests by a safety mechanism (1.111)

1.27

distributed development

development of an item (1.69) or element (1.32) with development responsibility divided between the customer and supplier(s) for the entire item or element, or for subsystems

NOTE Customer and supplier are roles of the cooperating parties.

1.28

diversity

different solutions satisfying the same requirement with the aim of independence (1.61)

EXAMPLE Diverse programming; diverse hardware.

NOTE Diversity does not guarantee independence, but addresses certain types of common cause failures (1.14).

1.29

dual-point failure

failure (1.39) resulting from the combination of two independent faults (1.42) that leads directly to the violation of a safety goal (1.108)

NOTE 1 Dual-point failures are multiple-point failures (1.76) of order 2.

NOTE 2 Dual-point failures that are addressed in ISO 26262 include those where one fault affects a safety-related element (1.113) and another fault affects the corresponding safety mechanism (1.111) intended to achieve or maintain a safe state (1.102).

NOTE 3 For a dual-point failure to directly violate a safety goal, the presence of both independent faults is necessary, i.e. the violation of a safety goal due to a combination of a residual fault (1.96) with a safe fault (1.101) is not considered a dual-point failure since the residual fault leads to a violation of a safety goal with or without the presence of a second independent fault.

© ISO 2011 – All rights reserved

AIS	Abbreviated Injury Scale
ASIC	Application-Specific Integrated Circuit
ASIL	Automotive Safety Integrity Level (see definition 1.6)
BIST	Built-In Self-Test
CAN	Controller Area Network
CCF	Common Cause Failure (see definition 1.14)
COTS	Commercial Off The Shelf
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DC	Diagnostic Coverage (see definition 1.25)
d.c.	Direct Current
DIA	Development Interface Agreement (see definition 1.24)
DSC	Dynamic Stability Control
ECU	Electronic Control Unit
EDC	Error Detection and Correction
E/E system	Electrical and/or Electronic system (see definition 1.31)
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESD	Electrostatic Discharge
ESC	Electronic Stability Control
ETA	Event Tree Analysis
FPGA	Field Programmable Gate Array
FIT	Failures In Time
FMEA	Failure Mode and Effects Analysis
FTA	Fault Tree Analysis
HAZOP	HAZard and Operability analysis
HSI	Hardware-Software Interface
HW	Hardware
H&R	Hazard analysis and Risk assessment (see definition 1.58)
IC	Integrated Circuit
I/O	Input – Output
MC/DC	Modified Condition/Decision Coverage
MMU	Memory Management Unit
MPU	Memory Protection Unit

© ISO 2011 – All rights reserved

MUX	MUltipleXer
OS	Operating System
PLD	Programmable Logic Device
PMHF	Probabilistic Metric for random Hardware Failures
QM	Quality Management
RAM	Random Access Memory
ROM	Read Only Memory
RFQ	Request For Quotation
SIL	Safety Integrity Level
SOP	Start Of Production
SRS	System Requirements Specification
SW	Software
UML	Unified Modeling Language
V&V	Verification and Validation
XML	eXtensible Markup Language

© ISO 2011 – All rights reserved

Bibliography

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

[2] ISO/TS 16949, Quality management systems — Particular requirements for the application of ISO 9001:2008 for automotive production and relevant service part organizations

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

[4] ISO 26262-3:2011, Road vehicles — Functional safety — Part 3: Concept phase

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

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

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

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

[9] ISO 26262-8:2011, Road vehicles — Functional safety — Part 8: Supporting processes

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

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

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

[13] ECE TRANS/WP.29/78/Rev.1/Amend.2, Consolidated Resolution on the construction of vehicles (R.E.3)

© ISO 2011 – All rights reserved

Alphabetical index

A

allocation 1.1
anomaly 1.2
architecture 1.3
ASIL 1.6
ASIL decomposition 1.7
assessment 1.4
audit 1.5
Automotive Safety Integrity Level 1.6
availability 1.8

B

baseline 1.9
branch coverage 1.10

C

calibration data 1.11
candidate 1.12
cascading failure 1.13
CCF 1.14
common cause failure 1.14
component 1.15
configuration data 1.16
confirmation measure 1.17
confirmation review 1.18
controllability 1.19

D

dedicated measure 1.20
degradation 1.21
dependent failures 1.22
detected fault 1.23
development interface agreement 1.24
DIA 1.24
diagnostic coverage 1.25
diagnostic test interval 1.26
distributed development 1.27
diversity 1.28
dual-point failure 1.29
dual-point fault 1.30

E

E/E system 1.31
electrical and/or electronic system 1.31
element 1.32
embedded software 1.33
emergency operation 1.34
emergency operation interval 1.35
error 1.36
exposure 1.37
external measure 1.38

F

failure 1.39
failure mode 1.40
failure rate 1.41
fault 1.42
fault model 1.43
fault reaction time 1.44
fault tolerant time interval 1.45
field data 1.46
formal notation 1.47
formal verification 1.48
freedom from interference 1.49
functional concept 1.50
functional safety 1.51
functional safety concept 1.52
functional safety requirement 1.53

H

hardware architectural metrics 1.54
hardware part 1.55
harm 1.56
hazard 1.57
hazard analysis and risk assessment 1.58
hazardous event 1.59
homogeneous redundancy 1.60

I

independence 1.61
independent failures 1.62
informal notation 1.63
informal verification 1.64
inheritance 1.65
initial ASIL 1.66
inspection 1.67
intended functionality 1.68
item 1.69
item development 1.70

L

latent fault 1.71
lifecycle 1.72

M

malfunctioning behaviour 1.73
model-based development 1.74
modification 1.75
multiple-point failure 1.76
multiple-point fault 1.77
multiple-point fault detection interval 1.78

N

new development 1.79
non-functional hazard 1.80

O

operating mode 1.81
operating time 1.82
operational situation 1.83
other technology 1.84

P

partitioning 1.85
passenger car 1.86
perceived fault 1.87
permanent fault 1.88
phase 1.89
proven in use argument 1.90
proven in use credit 1.91

R

random hardware failure 1.92
reasonably foreseeable event 1.93
redundancy 1.94
regression strategy 1.95
residual fault 1.96
residual risk 1.97
review 1.98
risk 1.99
robust design 1.100

S

safe fault 1.101
safe state 1.102
safety 1.103
safety activity 1.104
safety architecture 1.105
safety case 1.106
safety culture 1.107
safety goal 1.108

© ISO 2011 – All rights reserved

safety manager 1.109
safety measure 1.110
safety mechanism 1.111
safety plan 1.112 safety validation 1.116
safety-related element 1.113
safety-related function 1.114
safety-related special characteristic 1.115 semi-formal notation 1.117
semi-formal verification 1.118
service note 1.119 severity 1.120
single-point failure 1.121
single-point fault 1.122
software component 1.123
software tool 1.124
software unit 1.125
special-purpose vehicle 1.126
statement coverage 1.127
subphase 1.128 system 1.129
systematic failure 1.130
systematic fault 1.131

T

technical safety concept 1.132
technical safety requirement 1.133
testing 1.134
transient fault 1.135

U

unreasonable risk 1.136

V

verification 1.137
verification review 1.138

W

walk-through 1.139
warning and degradation concept 1.140
well-trusted 1.141
work product 1.142

© ISO 2011 – All rights reserved

BS ISO 26262-1:2011
ISO 26262-1:2011(E)

ICS 01.040.43; 43.040.10

Price based on 23 pages

© ISO 2011 – All rights reserved

This page deliberately left blank

This page deliberately left blank