
Road vehicles — Functional safety —

Part 10:
Guidelines on ISO 26262

Véhicules routiers — Sécurité fonctionnelle —

Partie 10: Lignes directrices relatives à l'ISO 26262



This document is a preview generated by EMS



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	vi
Introduction	viii
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Key concepts of ISO 26262	2
4.1 Functional safety for automotive systems (relationship with IEC 61508[1]).....	2
4.2 Item, system, element, component, hardware part and software unit.....	4
4.3 Relationship between faults, errors and failures.....	5
4.3.1 Progression of faults to errors to failures.....	5
4.4 FTTI and emergency operation tolerant time interval.....	6
4.4.1 Introduction.....	6
4.4.2 Timing model — Example control system.....	7
5 Selected topics regarding safety management	9
5.1 Work product.....	9
5.2 Confirmation measures.....	9
5.2.1 General.....	9
5.2.2 Functional safety assessment.....	10
5.3 Understanding of safety cases.....	12
5.3.1 Interpretation of safety cases.....	12
5.3.2 Safety case development lifecycle.....	13
6 Concept phase and system development	13
6.1 General.....	13
6.2 Example of hazard analysis and risk assessment.....	13
6.2.1 General.....	13
6.2.2 HARA example 1.....	13
6.2.3 HARA example 2.....	14
6.3 An observation regarding controllability classification.....	14
6.4 External measures.....	15
6.4.1 General.....	15
6.4.2 Example of vehicle dependent external measures 1.....	15
6.4.3 Example of vehicle dependent external measures 2.....	15
6.5 Example of combining safety goals.....	16
6.5.1 Introduction.....	16
6.5.2 General.....	16
6.5.3 Function definition.....	16
6.5.4 Safety goals applied to the same hazard in different situations.....	16
7 Safety process requirement structure — Flow and sequence of the safety requirements	17
8 Concerning hardware development	19
8.1 The classification of random hardware faults.....	19
8.1.1 General.....	19
8.1.2 Single-point fault.....	19
8.1.3 Residual fault.....	20
8.1.4 Detected dual-point fault.....	20
8.1.5 Perceived dual-point fault.....	20
8.1.6 Latent dual-point fault.....	21
8.1.7 Safe fault.....	21
8.1.8 Flow diagram for fault classification and fault class contribution calculation.....	21
8.1.9 How to consider the failure rate of multiple-point faults related to software-based safety mechanisms addressing random hardware failures.....	25
8.2 Example of residual failure rate and local single-point fault metric evaluation.....	25

8.2.1	General	25
8.2.2	Technical safety requirement for sensor A_Master	25
8.2.3	Description of the safety mechanism	26
8.2.4	Evaluation of example 1 described in Figure 12	29
8.3	Further explanation concerning hardware	37
8.3.1	How to deal with microcontrollers in the context of an ISO 26262 series of standards application	37
8.3.2	Safety analysis methods	37
8.4	PMHF units — Average probability per hour	44
9	Safety Element out of Context	47
9.1	Safety Element out of Context development	47
9.2	Use cases	48
9.2.1	General	48
9.2.2	Development of a system as a Safety Element out of Context example	49
9.2.3	Development of a hardware component as a Safety Element out of Context example	51
9.2.4	Development of a software component as a Safety Element out of Context example	53
10	An example of proven in use argument	55
10.1	General	55
10.2	Item definition and definition of the proven in use candidate	56
10.3	Change analysis	56
10.4	Target values for proven in use	56
11	Concerning ASIL decomposition	57
11.1	Objective of ASIL decomposition	57
11.2	Description of ASIL decomposition	57
11.3	An example of ASIL decomposition	57
11.3.1	General	57
11.3.2	Item definition	57
11.3.3	Hazard analysis and risk assessment	58
11.3.4	Associated safety goal	58
11.3.5	System architectural design	58
11.3.6	Functional safety concept	59
12	Guidance for system development with safety-related availability requirements	60
12.1	Introduction	60
12.2	Notes on concept phase when specifying fault tolerance	61
12.2.1	General	61
12.2.2	Vehicle operating states in which the availability of a functionality is safety-related	61
12.2.3	Prevention of hazardous events after a fault	61
12.2.4	Operation after fault reaction	62
12.2.5	Fault tolerant item example	63
12.2.6	ASIL decomposition of fault tolerant items	68
12.3	Availability considerations during hardware design phase	69
12.3.1	Random hardware fault quantitative analysis	69
12.4	Software development phase	71
12.4.1	Software fault avoidance and tolerance	71
12.4.2	Software fault avoidance	71
12.4.3	Software fault tolerance	71
13	Remark on “Confidence in the use of software tools”	72
14	Guidance on safety-related special characteristics	73
14.1	General	73
14.2	Identification of safety-related special characteristics	74
14.3	Specification of the control measures of safety-related special characteristics	74
14.4	Monitoring of the safety-related special characteristics	75

Annex A (informative) Fault tree construction and applications	76
Bibliography	79

This document is a preview generated by EVS

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.

NOTE The first edition of this document was published in 2012, therefore this document cancels and replaces ISO 26262-10:2012.

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.

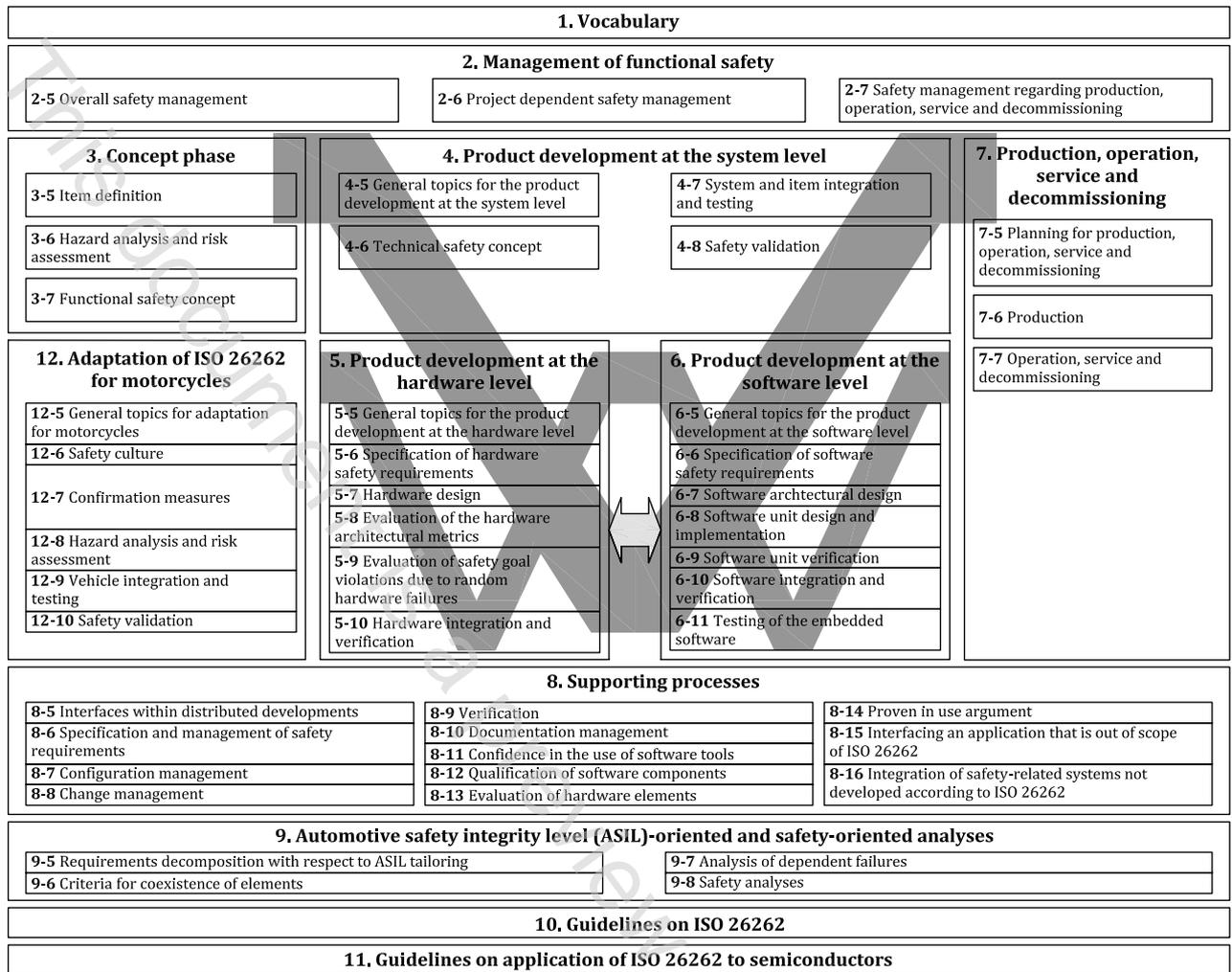


Figure 1 — Overview of the ISO 26262 series of standards

Road vehicles — Functional safety —

Part 10: Guidelines on ISO 26262

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 does not address the nominal performance of E/E systems.

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

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

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