
**Road vehicles — Functional safety —
Part 2:
Management of functional safety**

*Véhicules routiers — Sécurité fonctionnelle —
Partie 2: Gestion de la sécurité fonctionnelle*



Reference number
ISO 26262-2:2018(E)



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	v
Introduction	vii
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Requirements for compliance	2
4.1 Purpose	2
4.2 General requirements	2
4.3 Interpretations of tables	3
4.4 ASIL-dependent requirements and recommendations	3
4.5 Adaptation for motorcycles	3
4.6 Adaptation for trucks, buses, trailers and semi-trailers	3
5 Overall safety management	4
5.1 Objectives	4
5.2 General	4
5.2.1 Overview of the safety lifecycle	4
5.2.2 Explanatory remarks on the safety lifecycle	5
5.3 Inputs to this clause	9
5.3.1 Prerequisites	9
5.3.2 Further supporting information	9
5.4 Requirements and recommendations	9
5.4.1 General	9
5.4.2 Safety culture	9
5.4.3 Management of safety anomalies regarding functional safety	10
5.4.4 Competence management	11
5.4.5 Quality management system	11
5.4.6 Project-independent tailoring of the safety lifecycle	12
5.5 Work products	12
6 Project dependent safety management	12
6.1 Objectives	12
6.2 General	13
6.3 Inputs to this clause	14
6.3.1 Prerequisites	14
6.3.2 Further supporting information	14
6.4 Requirements and recommendations	14
6.4.1 General	14
6.4.2 Roles and responsibilities in safety management	14
6.4.3 Impact analysis at the item level	15
6.4.4 Reuse of an existing element	16
6.4.5 Tailoring of the safety activities	16
6.4.6 Planning and coordination of the safety activities	17
6.4.7 Progression of the safety lifecycle	19
6.4.8 Safety case	20
6.4.9 Confirmation measures	20
6.4.10 Confirmation reviews	23
6.4.11 Functional safety audit	24
6.4.12 Functional safety assessment	25
6.4.13 Release for production	27
6.5 Work products	28
7 Safety management regarding production, operation, service and decommissioning	28
7.1 Objective	28
7.2 General	28

7.3	Inputs to this clause.....	28
7.3.1	Prerequisites	28
7.3.2	Further supporting information.....	28
7.4	Requirements and recommendations.....	28
7.4.1	General.....	28
7.4.2	Responsibilities, planning and required processes	29
7.5	Work products.....	29
Annex A (informative) Overview of and workflow of functional safety management.....		30
Annex B (informative) Safety culture.....		33
Annex C (informative) Guidance for the confirmation measures.....		35
Annex D (informative) Example of a functional safety assessment agenda (for items that have an ASIL D safety goal)		40
Annex E (informative) Guidance on potential interaction of functional safety with cybersecurity.....		43
Bibliography		45

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.