

This is a preview of "ISO 26262-10:2012". [Click here to purchase the full version from the ANSI store.](#)

First edition
2012-08-01

Road vehicles — Functional safety — Part 10: Guideline on ISO 26262

Véhicules routiers — Sécurité fonctionnelle —

Partie 10: Lignes directrices relatives à l'ISO 26262



Reference number
ISO 26262-10:2012(E)

© ISO 2012

This is a preview of "ISO 26262-10:2012". Click [here](#) to purchase the full version from the ANSI store.



COPYRIGHT PROTECTED DOCUMENT

© ISO 2012

All rights reserved. Unless otherwise specified, no 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

This is a preview of "ISO 26262-10:2012". Click [here](#) to purchase the full version from the ANSI store.

Contents

Page

Foreword	iv
Introduction.....	v
1 Scope	1
2 Normative references	1
3 Terms, definitions and abbreviated terms	2
4 Key concepts of ISO 26262.....	2
4.1 Functional safety for automotive systems (relationship with IEC 61508)	2
4.2 Item, system, element, component, hardware part and software unit.....	4
4.3 Relationship between faults, errors and failures	5
5 Selected topics regarding safety management.....	6
5.1 Work product	6
5.2 Confirmation measures	6
5.3 Understanding of safety cases	9
6 Concept phase and system development.....	10
6.1 General	10
6.2 Example of hazard analysis and risk assessment	10
6.3 An observation regarding controllability classification	11
6.4 External measures.....	12
6.5 Example of combining safety goals	13
7 Safety process requirement structure - Flow and sequence of safety requirements	14
8 Concerning hardware development	17
8.1 The classification of random hardware faults	17
8.2 Example of residual failure rate and local single-point fault metric evaluation	22
8.3 Further explanation concerning hardware	34
9 Safety element out of context	36
9.1 Safety element out of context development	36
9.2 Use cases	37
10 An example of proven in use argument	45
10.1 General	45
10.2 Item definition and definition of the proven in use candidate	46
10.3 Change analysis	46
10.4 Target values for proven in use	46
11 Concerning ASIL decomposition.....	47
11.1 Objective of ASIL decomposition	47
11.2 Description of ASIL decomposition	47
11.3 An example of ASIL decomposition	47
Annex A (informative) ISO 26262 and microcontrollers	51
Annex B (informative) Fault tree construction and applications	73
Bibliography.....	89

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 26262-10 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*

This is a preview of "ISO 26262-10:2012". [Click here to purchase the full version from the ANSI store.](#)

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.

This is a preview of "ISO 26262-10:2012". Click here to purchase the full version from the ANSI store.

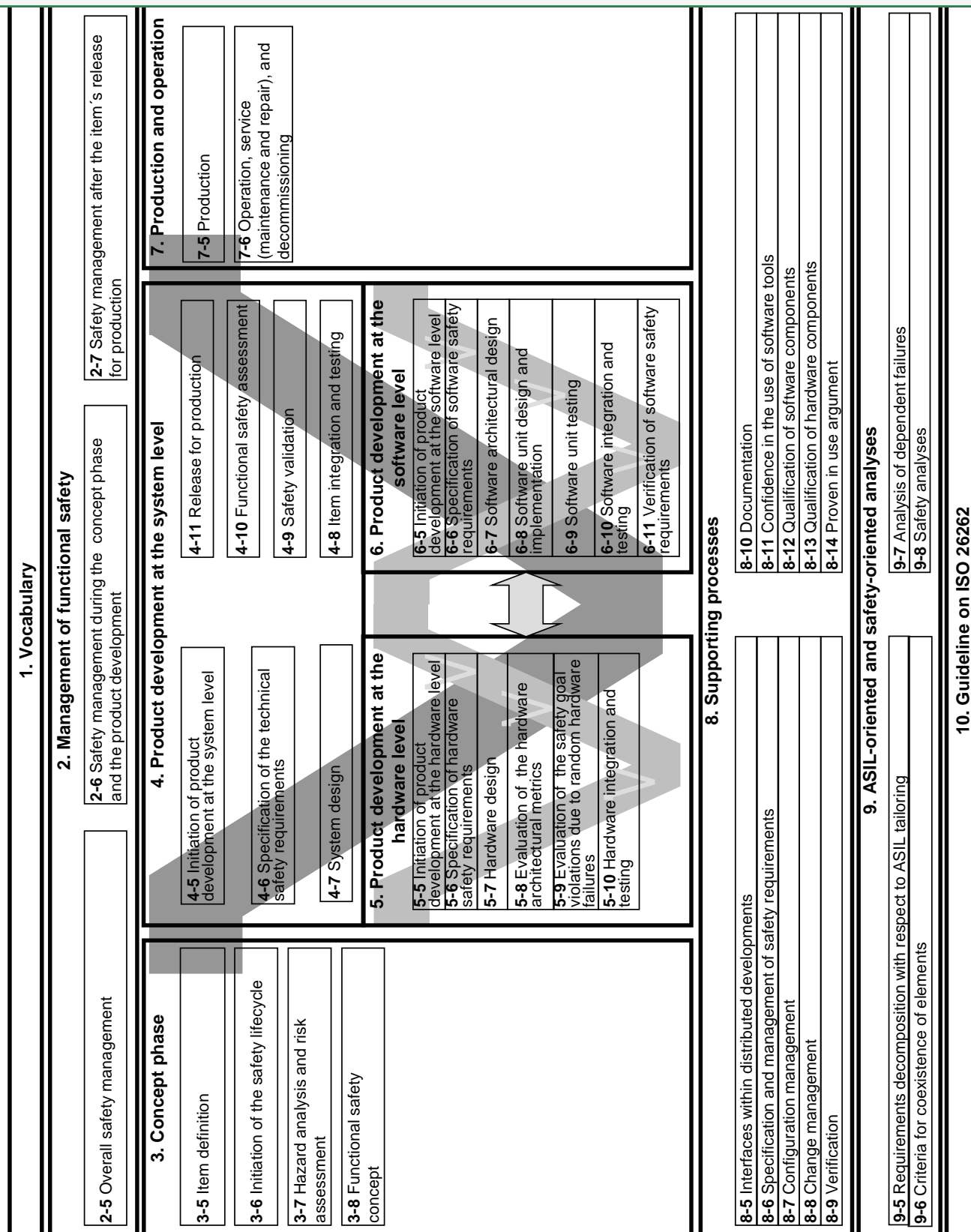


Figure 1 — Overview of ISO 26262