INTERNATIONAL STANDARD

ISO 26262-10

First edition 2012-08-01

Road vehicles — Functional safety — Part 10:

Guideline on ISO 26262

ss ro. Véhicules routiers — Sécurité fonctionnelle —



Reference number ISO 26262-10:2012(E)



© ISO 2012

<text> 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.

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

Contents

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

52

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.

2. Management of functional selety 2. Management of functional selety 2. Solute management information 2. Solute management and many the accorate planes 2. Solute management and many the accorate planes 2. Solute management and many the accorate planes 2. Solute management information 3. Forduction 3. Production 3. Production 3. Production 3. Solute many sea of the many many sea of the management sea of the many s		1. Vocabulary	ıry	
2-6 Safety management during the corcept phase and the product development at the system level development at the system level 2-7 Safety management for production 4-5 Initiation of product development at the system level 4-1 Release for production 4-5 Specification of the technical development at the system level 4-1 Release for production 4-5 Specification of the technical development at the ardtery requirements 4-1 Release for production 4-5 Specification of the technical development at the ardtery requirements 4-1 Release for production 5-7 Finduct development at the ardtery requirements 4-8 Item integration at the ardtery requirements 5-7 Hardware development at the ardter requirements 4-8 Item integration at the ardtery requirements 5-7 Hardware development at the ardterural meterical setty requirements 6-8 Software level 5-7 Hardware development at the ardterural meterical setty requirements 6-8 Software level 5-7 Hardware development at the ardterural meterical setty requirements 6-10 Valuation of software level 5-7 Hardware development at the ardterural meterical setty requirements 6-10 Software level 5-7 Hardware development at the ardterural meterical setty requirements 6-10 Colourate and setty setty requirements 6-10 Laidware feating 6-10 Colourate and setty setty requirements 6-10 Colourate and setty setty requirements 6-10 Laid		2. Management of func	ctional safety	
4.5 Induct development at the system level 4.5 Induction of product 4.6 Specification of the technical safety assessment safety requirements 4.7 System design 4.7 System design 5. Product development at the hardware level between the software level bet	2-5 Overall safety management	2-6 Safety management during and the product development		anagement after the item 's release
4-5 Initiation of production 4-11 Release for production 4-6 Specification of the technical 4-10 Functional safety assessment 4-6 Specification of the technical 4-9 Safety validation 4-7 System design 4-9 Safety validation 4-7 System design 4-8 Safety validation 4-7 System design 4-8 Safety validation 4-7 System design 4-8 Safety validation 5-5 Friduct development at the landware level 5-7 Finitation of products 5-5 Friduct development at the bardware level 5-7 Finitation of products 5-5 Friduct development at the bardware level 5-7 Finitation of products 5-5 Friduct development at the bardware level 5-8 Finitation of products 5-6 Evaluation of the bardware level 5-7 Software level 5-7 Hardware design 5-7 Software level 5-7 Hardware design 6-7 Software unit design and broutents 5-7 Hardware design 6-7 Software unit design and broutents 5-8 Evaluation of the bardware level 6-7 Software unit design and broutents 5-9 Evaluation and the former at the software integration and testing 6-8 Software unit design and broutents 5-9 Evaluation and testing 6-9 Software unit design and broutents 5-9 Evaluation and testing	3. Concept phase	4. Product development	at the system level	7. Production and operation
4.6 Specification of the technical selety requirements 4-1 Cunctional safety assessment 4-7 System design 4-9 Early validation 4-7 System design 4-8 Item integration and testing 4-7 System design 4-8 Item integration and testing 5- Fooduct development at the hardware level 5- Forduct development at the software level 5- 5 Specification of hardware safety requirements 6- Forduct development at the software level 5-7 Hardware level 5- Specification of product development at the safety requirements 5-7 Hardware level 6- Software level 5-7 Hardware level 6- Software unit testing 6-10 Hardware 6- Software unit testing 6-10	3-5 Item definition	4-5 Initiation of product development at the system level	4-11 Release for production	7-5 Production
4-7 System design 4-9 Safety validation 7-7 System design 4-8 Item integration and testing 7-7 System design 4-8 Item integration and testing 7-7 System design 5-5 Initiation of product 5-5 Initiation of product 5-5 Initiation of product 6-5 Software level 5-5 Initiation of product 6-5 Software level 5-5 Initiation of software level 6-5 Software level 5-5 Software level 6-6 Software unit design and 5-7 Hardware 5-7 Hardware 5-7 Software level 5	3-6 Initiation of the safety lifecycle	4-6 Specification of the technical	4-10 Functional safety assessment	7-6 Operation, service (maintenance and repair), and
 Froduct development at the hardware level 5. Product development at the hardware level 5.5. Specification of hardware level 5.6 Specification of hardware level 5.6 Specification of the hardware level 5.6 Specification of the hardware level 5.6 Specification of the hardware level 5.7 Hardware design 5.8 Evaluation of the safety goan 5.10 Hardware integration and 5.10 Hardware integration and 5.10 Hardware integration and 8. Supporting procomments 9. ASIL-oriented and safety-oriented to ASIL tailoring 	3-7 Hazard analysis and risk assessment	safety requirements	4-9 Safety validation	decommissioning
hardware level 5-5 Initiation of product 6-6 Specification of hardware level 5-6 Specification of hardware level 5-7 Hardware design 5-8 Evaluation of the hardware level 5-9 Evaluation of the safety goat 5-9 Evaluation of the safety goat 5-9 Evaluation of the safety goat 5-9 Evaluation and 10 Hardware integration and 10 Hardware	3-8 Functional safety concept		6. Product development at the	
8. Supporting proc ments afety requirements 9. ASIL-oriented and safety-c espect to ASIL tailoring			 6. Product development at the software level 5. Software level 6.5 Initiation of product 6.5 Specification of software level 6.7 Software architectural design 6.8 Software unit design and 6.9 Software unit testing 6.10 Software integration and 6.11 Verification of software safety 	
8. Supporting proc ments afety requirements 9. ASIL-oriented and safety-c espect to ASIL tailoring			requirements	
ments afety requirements 9. ASIL-oriented and safety-c espect to ASIL tailoring	9	8. Supporting pro	ocesses	
afety requirements 9. ASIL-oriented and safety-cespect to ASIL tailoring	8-5 Interfaces within distributed develo	pments	8-10 Documentation	
9. ASIL-oriented and safety-cespect to ASIL tailoring	8-6 Specification and management of	safety requirements	8-11 Confidence in the use of software to	ools
9. ASIL-oriented and safety-cespect to ASIL tailoring	8-7 Configuration management		8-12 Qualification of software componen 8-13 Ourlification of hardware componen	lts are
9. ASIL-oriented and safety-cespect to ASIL tailoring	8-9 Verification		8-14 Proven in use argument	2
espect to ASIL tailoring		9. ASIL-oriented and safety.	-oriented analyses	
	9-5 Requirements decomposition with 9-6 Criteria for coexistence of element	espect to	 9-7 Analysis of dependent failures 9-8 Safetv analyses 	

Figure 1 — Overview of ISO 26262

Road vehicles — Functional safety —

Part 10: Guideline on ISO 26262

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

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

2 Normative references

The following referenced documents are indispensable for the application 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 26262-1:2011, Road vehicles — Functional safety — Part 1: Vocabulary

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

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

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

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

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

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

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

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

3 Terms, definitions and abbreviated terms

For the purposes of this document, the terms, definitions and abbreviated terms given in ISO 26262-1:2011 apply.

4 Key concepts of ISO 26262

4.1 Functional safety for automotive systems (relationship with IEC 61508)

IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems*, is designated by IEC as a generic standard and a basic safety publication. This means that industry sectors will base their own standards for functional safety on the requirements of IEC 61508.

In the automotive industry, there are a number of issues with applying IEC 61508 directly. Some of these issues and corresponding differences in ISO 26262 are described below.

IEC 61508 is based upon the model of "equipment under control", for example an industrial plant that has an associated control system as follows:

- a) A hazard analysis identifies the hazards associated with the equipment under control (including the equipment control system), to which risk reduction measures will be applied. This can be achieved through E/E/PE systems, or other technology safety-related systems (e.g. a safety valve), or external measures (e.g. a physical containment of the plant). ISO 26262 contains a normative automotive scheme for hazard classification based on severity, probability of exposure and controllability.
- b) Risk reduction allocated to E/E/PE systems is achieved through safety functions, which are designated as such. These safety functions are either part of a separate protection system or can be incorporated into the plant control. It is not always possible to make this distinction in automotive systems. The safety of a vehicle depends on the behaviour of the control systems themselves.

ISO 26262 uses the concept of safety goals and a safety concept as follows:

- a hazard analysis and risk assessment identifies hazards and hazardous events that need to be prevented, mitigated or controlled;
- a safety goal is formulated for each hazardous event;
- an Automotive Safety Integrity Level (ASIL) is associated with each safety goal;
- the functional safety concept is a statement of the functionality to achieve the safety goal(s);
- the technical safety concept is a statement of how this functionality is implemented on the system level by hardware and software; and
- software safety requirements and hardware safety requirements state the specific safety requirements which will be implemented as part of the software and hardware design.

EXAMPLE

- The airbag system: one of the hazards is unintended deployment.
- An associated safety goal is that the airbag does not deploy unless a crash occurs that requires the deployment.