
**Road vehicles — Functional safety —
Part 4:
Product development at the system
level**

Véhicules routiers — Sécurité fonctionnelle —

Partie 4: Développement du produit au niveau du système



Reference number
ISO 26262-4:2018(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	2
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	4
4.6 Adaptation for trucks, buses, trailers and semi-trailers	4
5 General topics for the product development at the system level	4
5.1 Objectives	4
5.2 General	4
6 Technical safety concept	5
6.1 Objectives	5
6.2 General	6
6.3 Inputs to this clause	6
6.3.1 Prerequisites	6
6.3.2 Further supporting information	6
6.4 Requirements and recommendations	6
6.4.1 Specification of the technical safety requirements	6
6.4.2 Safety mechanisms	7
6.4.3 System architectural design specification and technical safety concept	9
6.4.4 Safety Analyses and avoidance of systematic failures	9
6.4.5 Measures for control of random hardware failures during operation	11
6.4.6 Allocation to hardware and software	11
6.4.7 Hardware-software interface (HSI) specification	12
6.4.8 Production, operation, service and decommissioning	12
6.4.9 Verification	13
6.5 Work products	14
7 System and item integration and testing	14
7.1 Objectives	14
7.2 General	15
7.3 Inputs to this clause	15
7.3.1 Prerequisites	15
7.3.2 Further supporting information	15
7.4 Requirements and recommendations	15
7.4.1 Specification of integration and test strategy	15
7.4.2 Hardware-software integration and testing	17
7.4.3 System integration and testing	19
7.4.4 Vehicle integration and testing	21
7.5 Work products	24
8 Safety validation	24
8.1 Objectives	24
8.2 General	24
8.3 Inputs to this clause	25
8.3.1 Prerequisites	25
8.3.2 Further supporting information	25
8.4 Requirements and recommendations	25

8.4.1	Safety validation environment.....	25
8.4.2	Specification of safety validation.....	25
8.4.3	Execution of safety validation.....	26
8.4.4	Evaluation.....	26
8.5	Work products.....	27
Annex A (informative) Overview of and workflow of product development at the system level		28
Annex B (informative) Example contents of hardware-software interface (HSI)		30
Bibliography		34

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.