

SVENSK STANDARD

SS-ISO 26262-11:2018

Fastställt/Approved: 2018-12-23
Utgåva/Edition: 1
Språk/Language: engelska/English
ICS: 43.040.10



Vägfordon – Funktionssäkerhet i el- och elektroniksystem – Del 11: Tillämpning för halvledare (ISO 26262-11, IDT)

Road vehicles – Functional safety – Part 11: Guidelines on application of ISO 26262 to semiconductors (ISO 26262-11, IDT)

Denna standard är såld av
SEK Svensk Elstandard som även lämnar
allmänna upplysningar om svensk och utländsk standard.
Postadress: SEK, Box 1284, 164 29 Kista
Telefon: 08-444 14 00.
E-post: sek@elstandard.se Internet: www.elstandard.se

Standarder får världen att fungera

SIS (Swedish Standards Institute) är en fristående ideell förening med medlemmar från både privat och offentlig sektor. Vi är en del av det europeiska och globala nätverk som utarbetar internationella standarder. Standarder är dokumenterad kunskap utvecklad av framstående aktörer inom industri, näringsliv och samhälle och befrämjar handel över gränser, bidrar till att processer och produkter blir säkrare samt effektiviserar din verksamhet.

Delta och påverka

Som medlem i SIS har du möjlighet att påverka framtida standarder inom ditt område på nationell, europeisk och global nivå. Du får samtidigt tillgång till tidig information om utvecklingen inom din bransch.

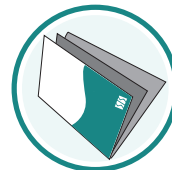
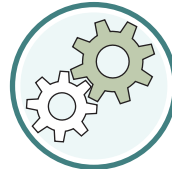
Ta del av det färdiga arbetet

Vi erbjuder våra kunder allt som rör standarder och deras tillämpning. Hos oss kan du köpa alla publikationer du behöver – allt från enskilda standarder, tekniska rapporter och standardpaket till handböcker och onlinetjänster. Genom vår webbtjänst e-nav får du tillgång till ett lättnavigerat bibliotek där alla standarder som är aktuella för ditt företag finns tillgängliga. Standarder och handböcker är källor till kunskap. Vi säljer dem.

Utveckla din kompetens och lyckas bättre i ditt arbete

Hos SIS kan du gå öppna eller företagsinterna utbildningar kring innehåll och tillämpning av standarder. Genom vår närhet till den internationella utvecklingen och ISO får du rätt kunskap i rätt tid, direkt från källan. Med vår kunskap om standarders möjligheter hjälper vi våra kunder att skapa verklig nytta och lönsamhet i sina verksamheter.

Vill du veta mer om SIS eller hur standarder kan effektivisera din verksamhet är du välkommen in på www.sis.se eller ta kontakt med oss på tel 08-555 523 00.



Standards make the world go round

SIS (Swedish Standards Institute) is an independent non-profit organisation with members from both the private and public sectors. We are part of the European and global network that draws up international standards. Standards consist of documented knowledge developed by prominent actors within the industry, business world and society. They promote cross-border trade, they help to make processes and products safer and they streamline your organisation.

Take part and have influence

As a member of SIS you will have the possibility to participate in standardization activities on national, European and global level. The membership in SIS will give you the opportunity to influence future standards and gain access to early stage information about developments within your field.

Get to know the finished work

We offer our customers everything in connection with standards and their application. You can purchase all the publications you need from us - everything from individual standards, technical reports and standard packages through to manuals and online services. Our web service e-nav gives you access to an easy-to-navigate library where all standards that are relevant to your company are available. Standards and manuals are sources of knowledge. We sell them.

Increase understanding and improve perception

With SIS you can undergo either shared or in-house training in the content and application of standards. Thanks to our proximity to international development and ISO you receive the right knowledge at the right time, direct from the source. With our knowledge about the potential of standards, we assist our customers in creating tangible benefit and profitability in their organisations.

If you want to know more about SIS, or how standards can streamline your organisation, please visit www.sis.se or contact us on phone +46 (0)8-555 523 00



Den internationella standarden ISO 26262-11:2018 gäller som svensk standard. Detta dokument innehåller den officiella engelska versionen av ISO 26262-11:2018.

The International Standard ISO 26262-11:2018 has the status of a Swedish Standard. This document contains the official English version of ISO 26262-11:2018.

© Copyright/Upphovsrätten till denna produkt tillhör SIS, Swedish Standards Institute, Stockholm, Sverige. Användningen av denna produkt regleras av slutanvändarlicensen som återfinns i denna produkt, se standardens sista sidor.

© Copyright SIS, Swedish Standards Institute, Stockholm, Sweden. All rights reserved. The use of this product is governed by the end-user licence for this product. You will find the licence in the end of this document.

Upplysningar om sakinnehållet i standarden lämnas av SIS, Swedish Standards Institute, telefon 08-555 520 00. Standarder kan beställas hos SIS som även lämnar allmänna upplysningar om svensk och utländsk standard.

Information about the content of the standard is available from the Swedish Standards Institute (SIS), telephone +46 8 555 520 00. Standards may be ordered from SIS, who can also provide general information about Swedish and foreign standards.

Denna standard är framtagen av kommittén för Funktionssäkerhet i elektronisksystem, SIS/TK 240/AG 08.

Har du synpunkter på innehållet i den här standarden, vill du delta i ett kommande revideringsarbete eller vara med och ta fram andra standarder inom området? Gå in på www.sis.se - där hittar du mer information.

Contents

Page

Foreword	vi
Introduction	vii
1 Scope.....	9
2 Normative references	9
3 Terms and definitions.....	9
4 A semiconductor component and its partitioning	10
4.1 How to consider semiconductor components	10
4.1.1 Semiconductor component development	10
4.2 Dividing a semiconductor component in parts.....	10
4.3 About hardware faults, errors and failure modes.....	11
4.3.1 Fault models.....	11
4.3.2 Failure modes	12
4.3.3 The distribution of base failure rate across failure modes	12
4.4 About adapting a semiconductor component safety analysis to system level.....	13
4.5 Intellectual Property (IP).....	14
4.5.1 About IP.....	14
4.5.2 Category and safety requirements for IP.....	15
4.5.3 IP lifecycle.....	17
4.5.4 Work products for IP	19
4.5.5 Integration of black-box IP.....	22
4.6 Base failure rate for semiconductors	23
4.6.1 General notes on base failure rate estimation.....	23
4.6.2 Permanent base failure rate calculation methods	28
4.7 Semiconductor dependent failure analysis	50
4.7.1 Introduction to DFA.....	50
4.7.2 Relationship between DFA and safety analysis.....	51
4.7.3 Dependent failure scenarios	51
4.7.4 Distinction between cascading failures and common cause failures	54
4.7.5 Dependent failure initiators and mitigation measures.....	54
4.7.6 DFA workflow	60
4.7.7 Examples of dependent failures analysis.....	63
4.7.8 Dependent failures between software element and hardware element.....	64
4.8 Fault injection.....	64
4.8.1 General.....	64
4.8.2 Characteristics or variables of fault injection	64
4.8.3 Fault injection results.....	66
4.9 Production and Operation	66
4.9.1 About Production.....	66
4.9.2 Production Work Products.....	67
4.9.3 About service (maintenance and repair), and decommissioning	67
4.10 Interfaces within distributed developments	67
4.11 Confirmation measures.....	68
4.12 Clarification on hardware integration and verification	68
5 Specific semiconductor technologies and use cases.....	69
5.1 Digital components and memories.....	69
5.1.1 About digital components	69
5.1.2 Fault models of non-memory digital components.....	69
5.1.3 Detailed fault models of memories	70
5.1.4 Failure modes of digital components	71
5.1.5 Example of failure mode definitions for common digital blocks.....	71
5.1.6 Qualitative and quantitative analysis of digital component	75
5.1.7 Notes on quantitative analysis of digital components	76

5.1.8	Example of quantitative analysis.....	78
5.1.9	Example of techniques or measures to detect or avoid systematic failures during design of a digital component.....	79
5.1.10	Verification using fault injection simulation	83
5.1.11	Example of safety documentation for a digital component	84
5.1.12	Examples of safety mechanisms for digital components and memories	85
5.1.13	Overview of techniques for digital components and memories.....	86
5.2	Analogue/mixed signal components.....	89
5.2.1	About analogue and mixed signal components	89
5.2.2	Analogue and mixed signal components and failure modes	91
5.2.3	Notes about safety analysis.....	100
5.2.4	Examples of safety mechanisms	103
5.2.5	Avoidance of systematic faults during the development phase	106
5.2.6	Example of safety documentation for an analogue/mixed-signal component.....	110
5.3	Programmable logic devices.....	111
5.3.1	About programmable logic devices.....	111
5.3.2	Failure modes of PLD.....	115
5.3.3	Notes on safety analyses for PLDs	116
5.3.4	Examples of safety mechanisms for PLD	121
5.3.5	Avoidance of systematic faults for PLD.....	122
5.3.6	Example of safety documentation for a PLD	125
5.3.7	Example of safety analysis for PLD.....	126
5.4	Multi-core components.....	126
5.4.1	Types of multi-core components.....	126
5.4.2	Implications of ISO 26262 series of standards for multi-core components.....	126
5.5	Sensors and transducers	128
5.5.1	Terminology of sensors and transducers	128
5.5.2	Sensors and transducers failure modes	130
5.5.3	Safety analysis for sensors and transducers	134
5.5.4	Examples of safety measures for sensors and transducers	136
5.5.5	About avoidance of systematic faults for sensors and transducers	140
5.5.6	Example of safety documentation for sensors and transducers.....	140
Annex A (informative) Example on how to use digital failure modes for diagnostic coverage evaluation.....		142
Annex B (informative) Examples of dependent failure analysis.....		146
Annex C (informative) Examples of quantitative analysis for a digital component.....		160
Annex D (informative) Examples of quantitative analysis for analogue component		165
Annex E (informative) Examples of quantitative analysis for PLD component.....		179
Bibliography		185

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.

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.

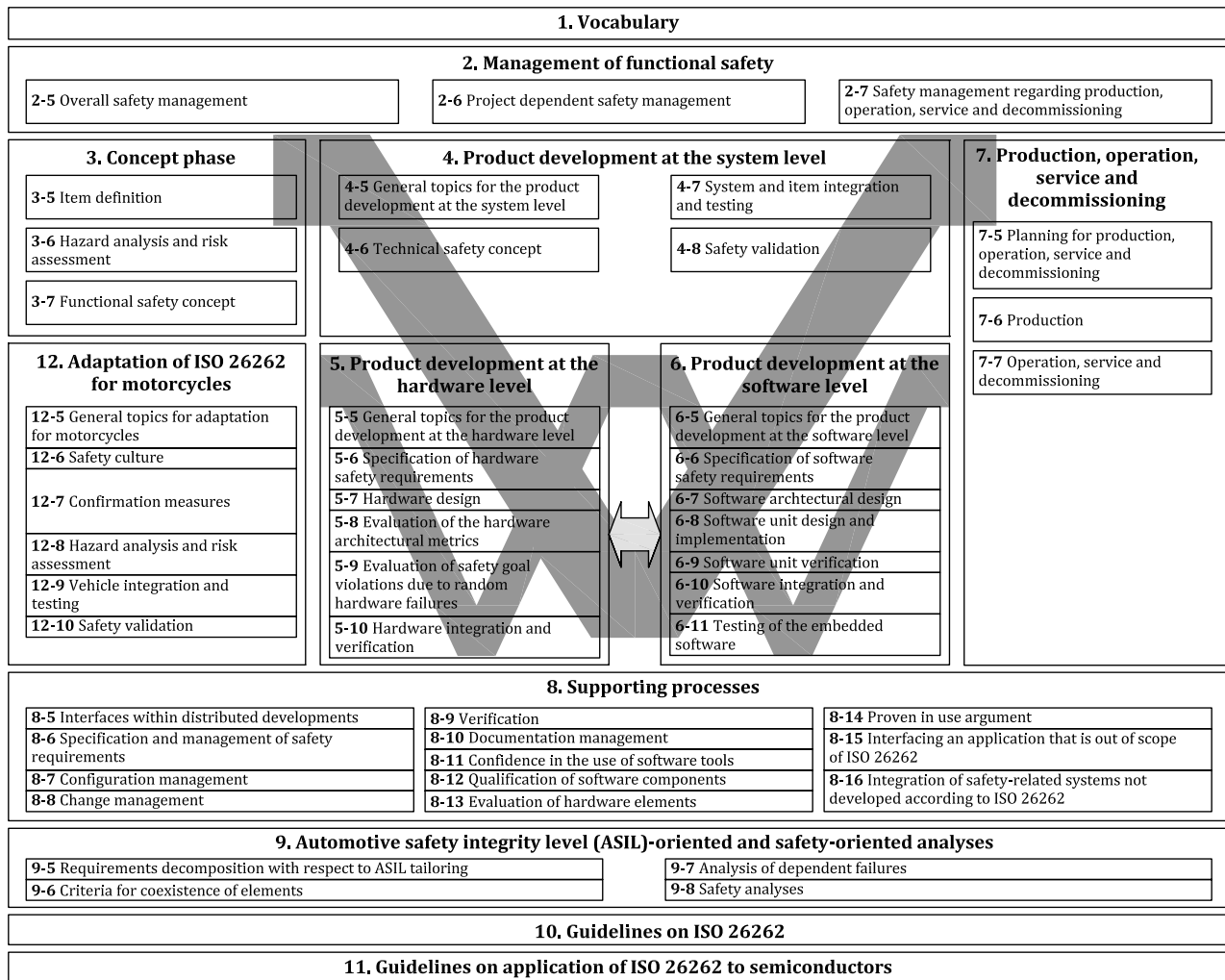


Figure 1 — Overview of the ISO 26262 series of standards

Road vehicles — Functional safety —

Part 11: Guidelines on application of ISO 26262 to semiconductors

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 has an informative character only. It contains possible interpretations of other parts of ISO 26262 with respect to semiconductor development. The content is not exhaustive with regard to possible interpretations, i.e., other interpretations can also be possible in order to fulfil the requirements defined in other parts of ISO 26262.

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*