
**Road vehicles — Functional safety —
Part 11:
Guidelines on application of ISO
26262 to semiconductors**

Véhicules routiers — Sécurité fonctionnelle —

Partie 11: Lignes directrices sur l'application de l'ISO 26262 aux semi-conducteurs

(<https://standards.iteh.ai>)
Document Preview

ISO 26262-11:2018

<https://standards.iteh.ai/catalog/standards/iso/28846afb-9d19-4e1e-b00c-2c35b74a475b/iso-26262-11-2018>



iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO 26262-11:2018

<https://standards.iteh.ai/catalog/standards/iso/28846af6-9d19-4e1e-b00c-2c35b74a475b/iso-26262-11-2018>



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 | vi |
| 1 Scope | 1 |
| 2 Normative references | 1 |
| 3 Terms and definitions | 1 |
| 4 A semiconductor component and its partitioning | 2 |
| 4.1 How to consider semiconductor components | 2 |
| 4.1.1 Semiconductor component development | 2 |
| 4.2 Dividing a semiconductor component in parts | 2 |
| 4.3 About hardware faults, errors and failure modes | 3 |
| 4.3.1 Fault models | 3 |
| 4.3.2 Failure modes | 4 |
| 4.3.3 The distribution of base failure rate across failure modes | 4 |
| 4.4 About adapting a semiconductor component safety analysis to system level | 5 |
| 4.5 Intellectual Property (IP) | 6 |
| 4.5.1 About IP | 6 |
| 4.5.2 Category and safety requirements for IP | 7 |
| 4.5.3 IP lifecycle | 9 |
| 4.5.4 Work products for IP | 11 |
| 4.5.5 Integration of black-box IP | 14 |
| 4.6 Base failure rate for semiconductors | 15 |
| 4.6.1 General notes on base failure rate estimation | 15 |
| 4.6.2 Permanent base failure rate calculation methods | 20 |
| 4.7 Semiconductor dependent failure analysis | 41 |
| 4.7.1 Introduction to DFA | 41 |
| 4.7.2 Relationship between DFA and safety analysis | 42 |
| 4.7.3 Dependent failure scenarios | 42 |
| 4.7.4 Distinction between cascading failures and common cause failures | 45 |
| 4.7.5 Dependent failure initiators and mitigation measures | 45 |
| 4.7.6 DFA workflow | 51 |
| 4.7.7 Examples of dependent failures analysis | 54 |
| 4.7.8 Dependent failures between software element and hardware element | 55 |
| 4.8 Fault injection | 55 |
| 4.8.1 General | 55 |
| 4.8.2 Characteristics or variables of fault injection | 55 |
| 4.8.3 Fault injection results | 57 |
| 4.9 Production and Operation | 57 |
| 4.9.1 About Production | 57 |
| 4.9.2 Production Work Products | 58 |
| 4.9.3 About service (maintenance and repair), and decommissioning | 58 |
| 4.10 Interfaces within distributed developments | 58 |
| 4.11 Confirmation measures | 59 |
| 4.12 Clarification on hardware integration and verification | 59 |
| 5 Specific semiconductor technologies and use cases | 60 |
| 5.1 Digital components and memories | 60 |
| 5.1.1 About digital components | 60 |
| 5.1.2 Fault models of non-memory digital components | 60 |
| 5.1.3 Detailed fault models of memories | 61 |
| 5.1.4 Failure modes of digital components | 62 |
| 5.1.5 Example of failure mode definitions for common digital blocks | 62 |
| 5.1.6 Qualitative and quantitative analysis of digital component | 66 |
| 5.1.7 Notes on quantitative analysis of digital components | 67 |

| | | |
|---|---|------------|
| 5.1.8 | Example of quantitative analysis | 69 |
| 5.1.9 | Example of techniques or measures to detect or avoid systematic failures during design of a digital component | 70 |
| 5.1.10 | Verification using fault injection simulation | 74 |
| 5.1.11 | Example of safety documentation for a digital component | 75 |
| 5.1.12 | Examples of safety mechanisms for digital components and memories | 76 |
| 5.1.13 | Overview of techniques for digital components and memories | 77 |
| 5.2 | Analogue/mixed signal components | 80 |
| 5.2.1 | About analogue and mixed signal components | 80 |
| 5.2.2 | Analogue and mixed signal components and failure modes | 82 |
| 5.2.3 | Notes about safety analysis | 91 |
| 5.2.4 | Examples of safety mechanisms | 94 |
| 5.2.5 | Avoidance of systematic faults during the development phase | 97 |
| 5.2.6 | Example of safety documentation for an analogue/mixed-signal component | 100 |
| 5.3 | Programmable logic devices | 101 |
| 5.3.1 | About programmable logic devices | 101 |
| 5.3.2 | Failure modes of PLD | 105 |
| 5.3.3 | Notes on safety analyses for PLDs | 106 |
| 5.3.4 | Examples of safety mechanisms for PLD | 112 |
| 5.3.5 | Avoidance of systematic faults for PLD | 113 |
| 5.3.6 | Example of safety documentation for a PLD | 116 |
| 5.3.7 | Example of safety analysis for PLD | 116 |
| 5.4 | Multi-core components | 116 |
| 5.4.1 | Types of multi-core components | 116 |
| 5.4.2 | Implications of ISO 26262 series of standards for multi-core components | 117 |
| 5.5 | Sensors and transducers | 119 |
| 5.5.1 | Terminology of sensors and transducers | 119 |
| 5.5.2 | Sensors and transducers failure modes | 120 |
| 5.5.3 | Safety analysis for sensors and transducers | 125 |
| 5.5.4 | Examples of safety measures for sensors and transducers | 126 |
| 5.5.5 | About avoidance of systematic faults for sensors and transducers | 130 |
| 5.5.6 | Example of safety documentation for sensors and transducers | 131 |
| Annex A (informative) Example on how to use digital failure modes for diagnostic coverage evaluation | | 132 |
| Annex B (informative) Examples of dependent failure analysis | | 136 |
| Annex C (informative) Examples of quantitative analysis for a digital component | | 150 |
| Annex D (informative) Examples of quantitative analysis for analogue component | | 155 |
| Annex E (informative) Examples of quantitative analysis for PLD component | | 169 |
| Bibliography | | 175 |

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.

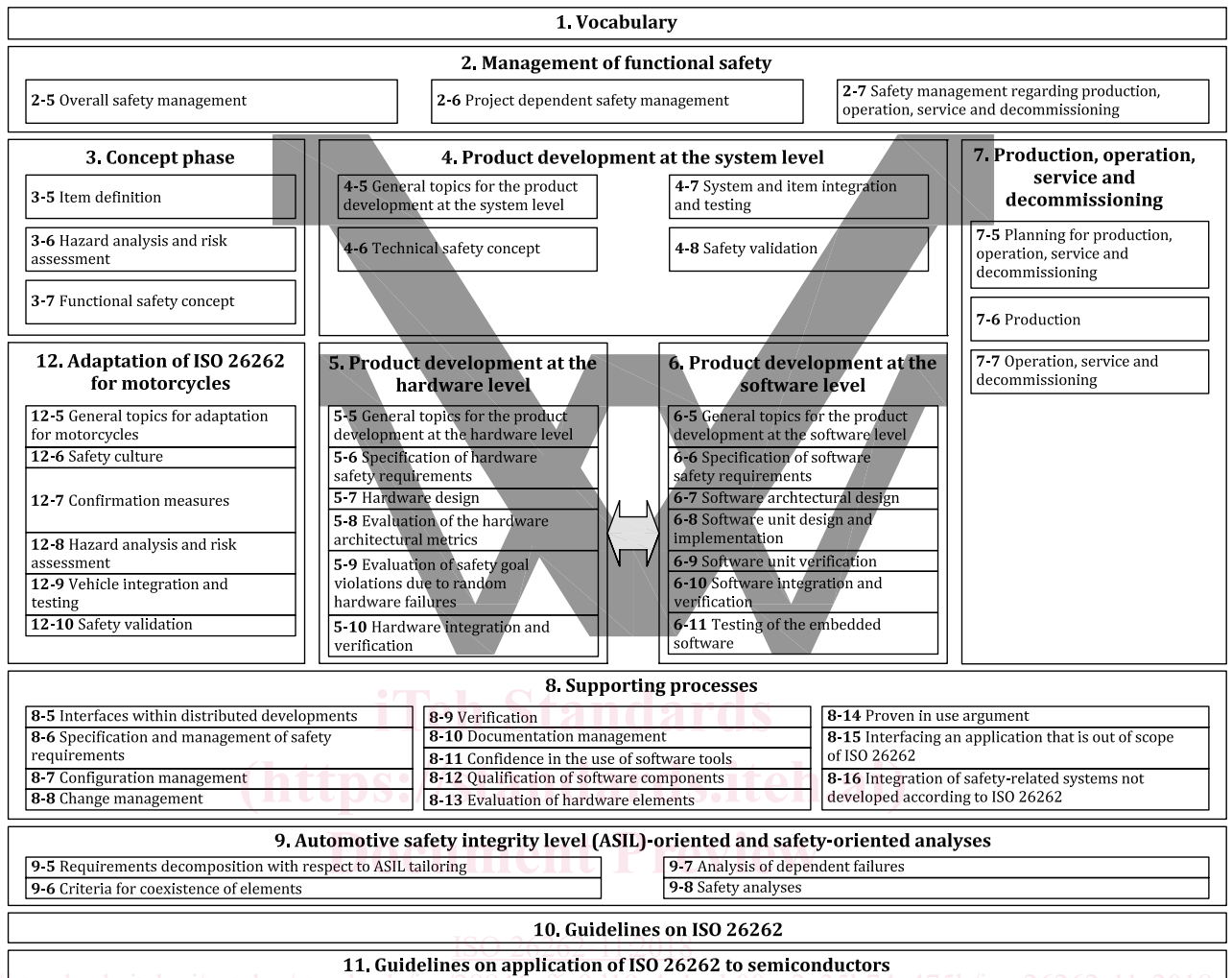


Figure 1 — Overview of the ISO 26262 series of standards

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*

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <https://www.iso.org/obp>

4 A semiconductor component and its partitioning

4.1 How to consider semiconductor components

4.1.1 Semiconductor component development

If a semiconductor component is developed as a part of an item development compliant with the ISO 26262 series of standards, it is developed based on hardware safety requirements derived from the top-level safety goals of the item, through the technical safety concept. Targets for diagnostic coverages for relevant failure modes to meet hardware architectural metrics and Probabilistic Metric for random Hardware Failures (PMHF) or Evaluation of Each Cause of safety goal violation (EEC) are allocated to the item: in this case, the semiconductor component is just one of the elements. As mentioned in the EXAMPLE of ISO 26262-5:2018 [66], 8.2, to facilitate distributed developments, target values can be assigned to the semiconductor component itself, by either deriving target values for the SPFM, LFM and PMHF at the item level or applying EEC to the HW part level. The safety analysis of a semiconductor component is performed based on the requirements and recommendations defined in ISO 26262-5:2018, 7.4.3 and in ISO 26262-9:2018 [70], Clause 8.

NOTE If an element has not been developed in compliance with the ISO 26262 series of standards, the requirements in ISO 26262-8:2018 [69], Clause 13 can be considered.

The semiconductor component can be developed as a SEooC, as described in ISO 26262-10 [61]. In this case, the development is done based on assumptions on the conditions of the semiconductor component usage (Assumptions of Use or AoU, see 4.4), and then the assumptions are verified at the next higher level of integration considering the semiconductor component requirements derived from the safety goals of the item in which the semiconductor component is to be used.

The descriptions and methods in this part are provided assuming the semiconductor component is a SEooC, but the described methods (e.g. the method for failure rate computation of a semiconductor component) are still valid if the semiconductor component is not considered as an SEooC. When those methods are conducted considering the stand-alone semiconductor component, appropriate assumptions are made. Sub-clause 4.4 describes how to adapt and verify those methods and assumptions at the system or element level. At the stand-alone semiconductor component level, the requirements of ISO 26262-2 [63], ISO 26262-5, ISO 26262-6[67], ISO 26262-7[68], ISO 26262-8 and ISO 26262-9 (e.g. related to safety analyses, dependent failure analysis, verification, etc.) can be applied.

4.2 Dividing a semiconductor component in parts

As shown in Figure 2 and according to the definitions in ISO 26262-1:2018, 3.21, a semiconductor component can be divided into parts: the whole semiconductor hierarchy can be seen as a component, the second level of hierarchy (e.g. a CPU) as a part, the following levels of hierarchy (e.g. the CPU register bank) as subparts, till the elementary subparts (its internal registers and the related logic).

NOTE The level of detail (e.g. whether to stop at part level or go down to subpart or elementary subpart level) as also the definition of the elementary subpart (e.g. flip-flop, analogue transistor) can depend on the safety concept, the stage of the analysis and on the safety mechanisms used (inside the semiconductor component or at the system or element level).

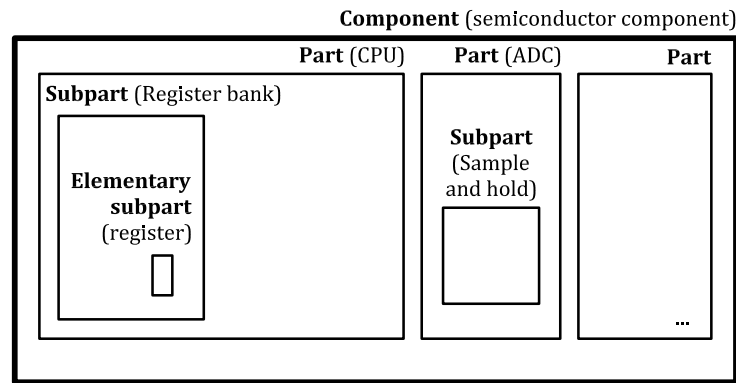


Figure 2 — A semiconductor, its parts and subparts

4.3 About hardware faults, errors and failure modes

Random hardware faults and failure modes of an integrated circuit are linked together as shown in Figure 3 below.

NOTE 1 The failure mode can be abstract or tailored to a specific implementation, e.g. related to a pin of a component, part or subpart.

In general, failure modes are described in this document as functional failure modes. Further characterisation of failure modes are possible.

EXAMPLE An example of failure modes for digital circuits is given in Annex A.

Faults and errors described in this document are related to the physical implementation of a given semiconductor component.

NOTE 2 The terms fault, error, and failure are used according to the ISO 26262-1 definitions, i.e. faults create errors which can lead to a failure. In many reliability modelling standards the terms fault and failure are used interchangeably.

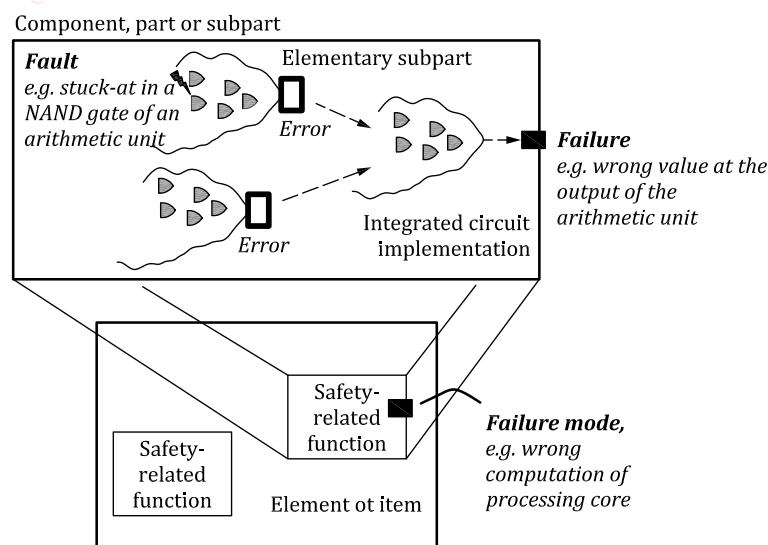


Figure 3 — Relationship between hardware faults and failure modes

4.3.1 Fault models

Fault models are an abstract representation of physical faults.

The failure mode distribution is correlated with the fault models illustrated in [Figure 3](#).

EXAMPLE If a failure mode is caused $X\%$ by stuck-at faults and $Y\%$ by shorts, and if a safety mechanism only covers stuck-at faults with a coverage of $Z\%$, then the claimed diagnostic coverage is $X\% \times Z\%$.

In the context of a semiconductor component, relevant fault models are identified based on the technology and circuit implementation.

NOTE 1 See [5.1.2](#) for further details on fault models for digital components and [5.1.3](#) for memories.

NOTE 2 Typically it is not possible to evaluate every possible physical fault individually due to the number of faults and required level of detail.

4.3.2 Failure modes

A failure mode is described at a level of detail commensurate with the safety concept and the related safety mechanism.

EXAMPLE 1 In the case of a CPU with a hardware lock-step safety mechanism, the failure modes can be defined by looking at the CPU function as a whole.

EXAMPLE 2 In the case of a CPU with a structural software-based hardware test as safety mechanism, the failure modes for the CPU function are defined in more detail because the software test will cover different failure modes with different failure mode coverage.

EXAMPLE 3 Examples of different level of detail for digital failure modes are given in [Annex A](#).

To define failure modes, keywords are used if applicable.

EXAMPLE 4 Examples of keywords are: wrong program flow execution, data corruption, accessing unintended locations, deadlock, livelock, incorrect instruction execution.

In special cases, failure modes closer to physical implementation could be more helpful.

EXAMPLE 5 Analogue failure mode ([Table 36](#)).

The association between the identified failure modes and circuit implementation fault models is supported by evidence ensuring any failure mode is allocated to a part/subpart of the component, and any relevant part/subpart has at least one failure mode.

NOTE The goal is to ensure that there are no gaps between circuit implementation and the listed failure modes.

4.3.3 The distribution of base failure rate across failure modes

The base failure rate (see [4.6](#)) is distributed across failure modes. The accuracy of that distribution is aligned with the level of detail of the analysis and the consideration of the relevant safety mechanisms available.

EXAMPLE 1 In the case of a CPU with a hardware lock-step safety mechanism, it is not necessary to have a detailed distribution of CPU failure modes.

EXAMPLE 2 In the case of a CPU with a structural software-based hardware test, the distribution is defined in more detail because in this way it will be possible to estimate with enough accuracy the diagnostic coverage of failure modes.

In case there is no data available to compute the distribution with the required accuracy, the failure rate is distributed uniformly across the failure modes or an expert judgment is provided with related arguments.

NOTE A sensitivity analysis to the distribution is done to evaluate the impact on the diagnostic coverage and quantitative safety analysis results.

4.4 About adapting a semiconductor component safety analysis to system level

The adaptation of the semiconductor component safety analysis to system level is done by:

- transforming the detailed failure modes of a semiconductor component into the high-level failure modes needed during the analysis at system level, as shown in [Figure 4](#);

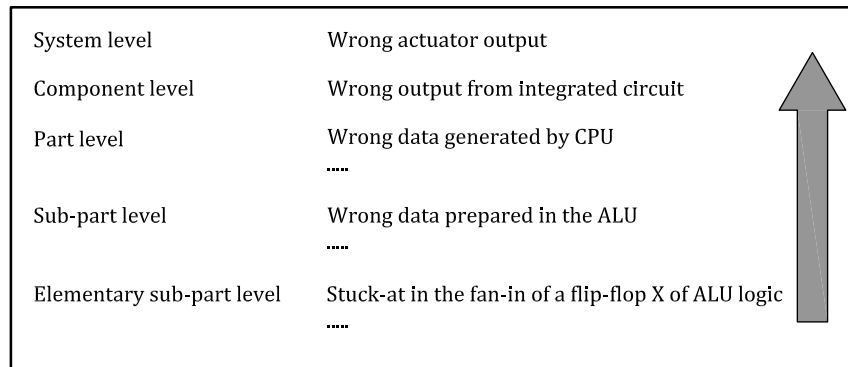


Figure 4 — Example of bottom-up approach to derive system level failure modes

NOTE 1 By combining top-down (e.g. FTA) and bottom-up methods (e.g. FMEA), it can be possible to identify the detailed semiconductor component failure modes and combine them up to the component level.

NOTE 2 Starting from a low level of abstraction allows a quantitative and precise failure distribution for a semiconductor component that otherwise is based on qualitative distribution assumptions.

NOTE 3 As discussed in [4.2](#), the necessary level of detail can depend on the stage of the analysis and on the safety mechanisms used.

- the diagnostic coverage computed at part or subpart level could be improved by measures at the part, component level or system or item level; or

EXAMPLE 1 A semiconductor component includes an ADC with no safety mechanisms implemented in hardware. At the component stand-alone level, the diagnostic coverage was considered zero. At system level, the ADC is included in a closed-loop, and its faults are detected by a software-based consistency check. In this context, the diagnostic coverage of that subpart is increased due to the safety mechanism implemented at system-level.

- the diagnostic coverage computed at part or subpart level could have been calculated under certain specific assumptions ("Assumptions of Use" or AoU).

NOTE 4 At system level different safety mechanisms or failure masking can be present. This can be taken into consideration in safety analysis when a justification is possible.

EXAMPLE 2 A semiconductor component includes a memory in which each single-error is corrected and signalled by the ECC to the CPU. At the component stand-alone level, it was assumed that a software driver is implemented to handle this event. At system level, for performance reasons, this software driver is not implemented, and therefore the assumption is not fulfilled. The semiconductor component is programmed to send the error correction flag directly to the outside world.

4.5 Intellectual Property (IP)

4.5.1 About IP

4.5.1.1 Understanding IP

In this sub-clause, IP refers to a reusable unit of logical design or physical design intended to be integrated into a design as a part or a component. The term “IP integrator” is used in reference to the organization responsible for integrating IP designs from one or more sources into a design with safety requirements. The term “IP supplier” is used in reference to the organization responsible for designing or developing the IP. The IP integrator and the IP supplier can be separate parties as well as the same company or different organisations in the same company.

Based on the requirements in ISO 26262 series of standards, four possible approaches are identified for IP based designs. These approaches are shown in [Figure 5](#). The IP integrator typically chooses the approach based on consideration of the information provided from the IP supplier as well as the maturity of the IP.

EXAMPLE If no supporting information is available from the IP supplier, possible approaches can be limited to the “proven in use” argument, if applicable. If the proven in use argument is not applicable, then the role of the IP in the safety architecture is treated differently, e.g. using diverse redundancy to reduce risk of systematic and random hardware failures.

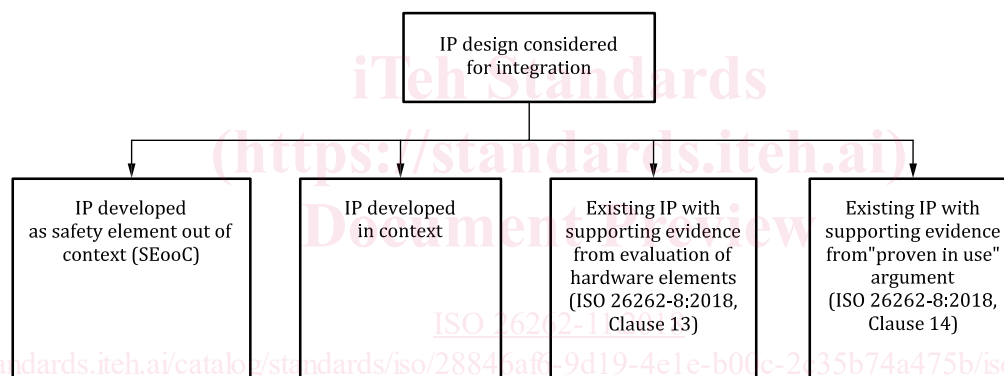


Figure 5 — Possible approaches for using IP in safety-related designs

The IP can be an existing design with a predefined set of features. In this case the IP integrator has the responsibility of identifying the set of features which are required to support the safety concept of the design. IP can also be designed based on an agreed set of safety requirements. In this case the IP integrator identifies the requirements for the IP which are necessary to support the safety concept of the design.

NOTE 1 The guidance in this sub-clause can be applied to newly developed IP, modified IP, and existing unmodified IP.

NOTE 2 A common approach is to assume the possible target usage as defined in ISO 26262-2:2018, 6.4.5.7. This option is described as SEooC in ISO 26262-10 [61]. Development of an SEooC relies on identification of assumed use cases and safety requirements which are verified by the IP integrator.

4.5.1.2 Types of IP

Commonly used IP types are listed in [Table 1](#). This is not an exhaustive list covering the possible IP types. This document considers both the physical and the model representation types of IP as applied to semiconductor designs.