BS ISO 26262-11:2018

BSI Standards Publication

Road vehicles — Functional safety

Part 11: Guidelines on application of ISO 26262 to semiconductors

Documents
Document Sharing Hub

Full document details: BS ISO 26262-11:2018

National foreword

This British Standard is the UK implementation of ISO 26262-11:2018.

The UK participation in its preparation was entrusted to Technical Committee AUE/32, Electrical and electronic components and general system aspects (Road vehicles).

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 580 93000 3

ICS 43.040.10

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 December 2018.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO 26262-11:2018

INTERNATIONAL STANDARD

ISO 26262-11

First edition
2018-12

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

Reference number
ISO 26262-11:2018(E)

Documents
Document Sharing Hub
© ISO 2018

Full document details: BS 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

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO 26262-11:2018

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

AVA Documents
Document Sharing Hub

© ISO 2018 – All rights reserved

Full document details: BS ISO 26262-11:2018

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**

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

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.

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

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.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

EXAMPLE "2-6" represents ISO 26262-2:2018, Clause 6.

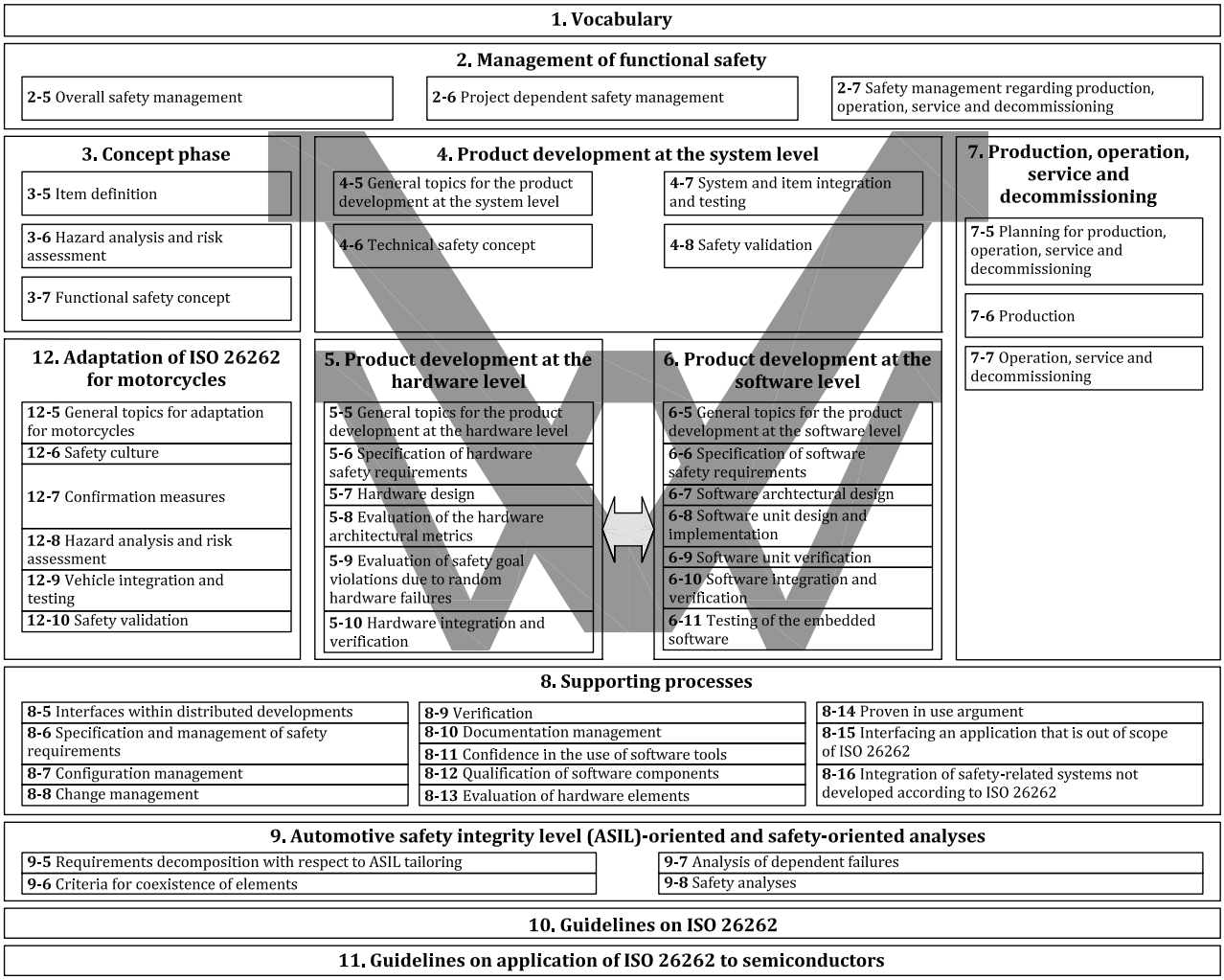

Figure 1 — Overview of the ISO 26262 series of standards

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

Documents
Document Sharing Hub

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.

Documents
Document Sharing Hub

© ISO 2018 – All rights reserved

Full document details: BS ISO 26262-11:2018

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).

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

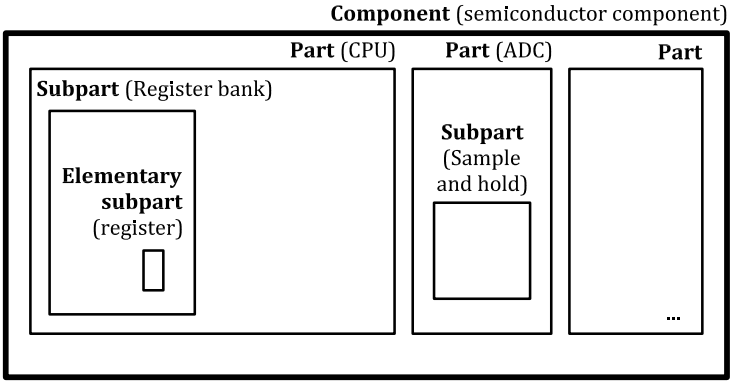

Figure 2 — A semiconductor, its parts and subparts

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.

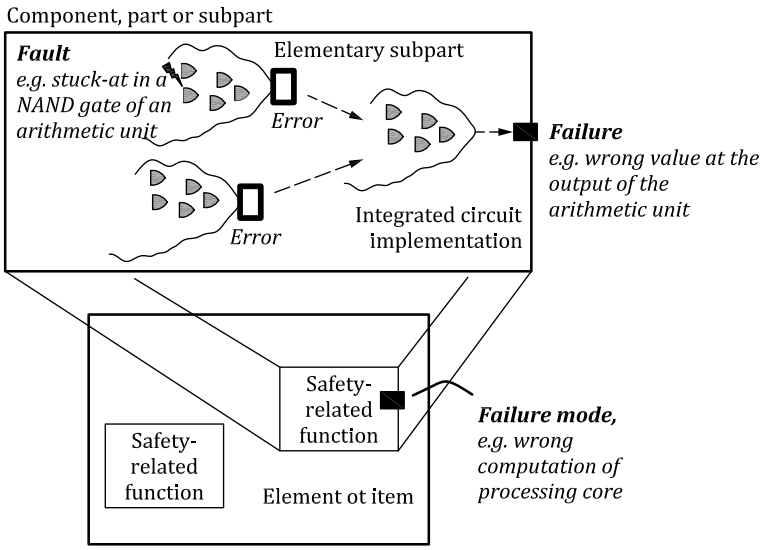

Figure 3 — Relationship between hardware faults and failure modes

4.3.1 Fault models

Fault models are an abstract representation of physical faults.

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

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* % × *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.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

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;

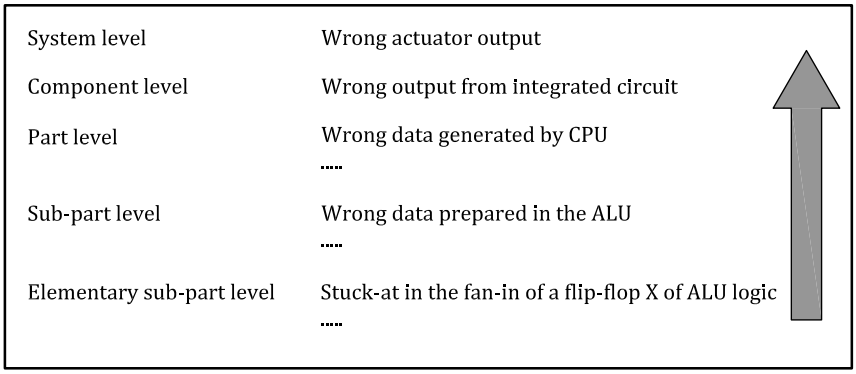

Figure 4 — Example of bottom-up approach to derive system level failure modes

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.

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

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.

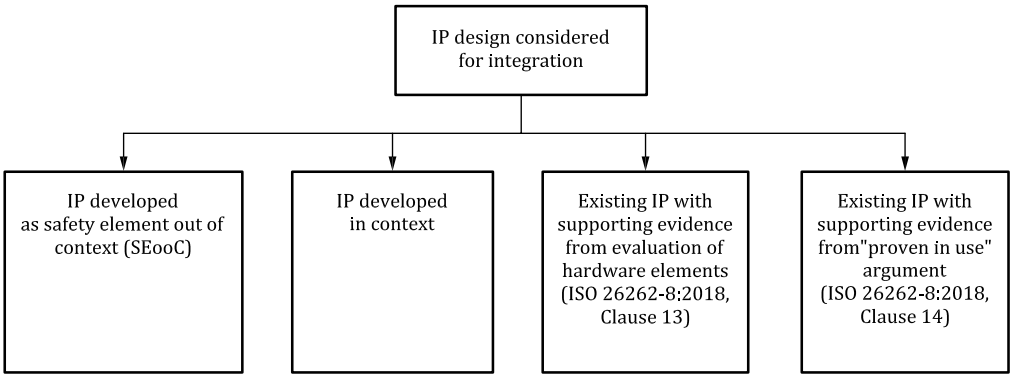

Figure 5 — Possible approaches for using IP in safety-related designs

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.

© ISO 2018 – All rights reserved
Documents Document Sharing Hub
Full document details: BS ISO 26262-11:2018

Table 1 — Types of IP

IP type	Description
Physical representation	A complete chip layout description, containing instantiations of standard cells for a specific cell library or analogue cells for a target manufacturing process. EXAMPLE ADC macro, PLL macro.
Model representation	A description of a design in terms of a hardware description language (HDL) such as Verilog or VHDL, or analogue transistor level circuit schematic. A logic design in model representation is synthesized into a list of gates consisting of basic cells, followed by placement and routing to achieve a semiconductor design. Analogue circuit schematic components, such as transistors, diodes, resistors, and capacitors, are mapped into target technology library components, followed by placement and routing to achieve a semiconductor design. EXAMPLE Processor or memory controller design exchanged without mapping to a particular technology, operational amplifier transistor level schematic.
NOTE 1 Physical representation IPs are also known as “hard IPs”. NOTE 2 Model representation IPs are also known as “soft IPs”. NOTE 3 This classification is applicable to generic IP design including digital, analogue, mixed signal, PLD, Sensors and Transducers.	

NOTE 1 IP in the form of logic design can also be configurable. In this case, the configuration options are specified by the IP integrator.

EXAMPLE 1 Configuration options to define interface bus width, memory size, and presence of fault detection mechanisms.

NOTE 2 IP can also be generated with dedicated tools (memory compilers, C to HDL compilers, network-on-chip generators). In this case:

— confidence in software tools can be demonstrated using the methods described in ISO 26262-8:2018, Clause 11, tailored based on the amount of verification performed on the generated IP;

— the necessary verification activities to guarantee the correctness of the generated IP are performed by the IP integrator or IP supplier as applicable (e.g. agreement in DIA);

— the necessary work products, as listed in following clauses, are made available; and

— the IP integrator verifies the correct integration of the IP in its context.

4.5.2 Category and safety requirements for IP

In general, two categories of IP can be determined based on the allocation of safety requirements: IP with no allocated safety requirements, and IP with one or more allocated safety requirements. When the IP has no allocated safety requirements, no additional considerations are required for ISO 26262 series of standards unless identified during the safety analysis. In the case of coexistence of non-safety-related IPs with safety-related elements, dependent failure(s) analysis is used to evaluate freedom from interference. For dependent failure analysis guidance, see ISO 26262-9:2018, Clause 7 together with the additional guidance in 4.7 of this document.

If one or more safety requirements are allocated to the IP, the requirements of ISO 26262 series of standards are applicable. In particular requirements of ISO 26262-2, ISO 26262-4 [65], ISO 26262-5, ISO 26262-8, and ISO 26262-9 are often tailored to apply to IP designs. The following text gives guidance for IP with allocated safety requirements, and how to consider these requirements for IP with and without integrated safety mechanisms.

Safety-related IPs can be further classified based on the integration of safety mechanisms. Two possible cases are illustrated in Figure 6, with subfigure (a) illustrating IP which has integrated safety mechanisms, and subfigure (b) illustrating IP which has no integrated safety mechanisms.

© ISO 2018 – All rights reserved

AVA Documents Document Sharing Hub
Full document details: BS ISO 26262-11:2018

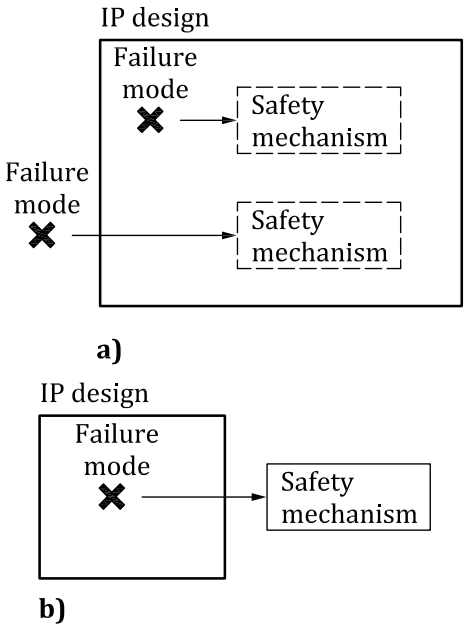

Figure 6 — Types of IP with allocated safety requirements

NOTE 1 IP safety mechanisms can be included for detection of failure modes of the IP, as well as failure modes external to the IP.

NOTE 2 Safety mechanisms implemented in the IP can provide full or partial diagnostic coverage of a defined set of failure modes. It is also possible that only failure mode detection is performed by the IP, with failure mode control being provided by components external to the IP.

The IP provider is responsible for providing the usage assumptions made during IP development in order to allow the IP integrator to check consistency with safety requirements.

The hardware features of the IP can be initially developed targeting its integration into a safety-related hardware environment, by providing safety mechanisms based on assumed safety requirements that aim at controlling given failure modes. In this case the requirements of ISO 26262-2, ISO 26262-4, ISO 26262-5, ISO 26262-6 (in the case of software based safety mechanisms to cover hardware failures), ISO 26262-8, and ISO 26262-9, whenever applicable, can be used for the design of the safety mechanisms during the development of the IP.

EXAMPLE 1 Bus “fabric” with built-in bus supervisors including fault detection and notification logic (e.g. interrupt signals).

EXAMPLE 2 Voltage regulator with monitoring (under-voltage and over-voltage detection), protection (current limit or thermal protection) and self-diagnostics (monitoring and protection circuit built-in self-tests).

Alternatively the IP can be developed with no assumed safety requirements or specific safety mechanisms to detect and control faults.

EXAMPLE 3 Bus “fabric” without built-in bus supervisors or error reporting logic.

EXAMPLE 4 Voltage regulator without monitoring, protection or built-in monitoring or protection circuit diagnostics.

Safety analyses defined in ISO 26262-9:2018, Clause 8 can be applied to the IP. A qualitative safety analysis, and in some cases a quantitative analysis, can be provided to the IP integrator to justify the capabilities of the safety mechanisms to control given failure modes or to provide information on failure

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

modes and related failure mode distribution. Similarly a dependent failure analysis can be provided to demonstrate required independence or freedom from interference.

NOTE 3 The IP supplier includes example information concerning failure mode distribution in the safety analysis results, based on specific implementation assumptions. Documentation related to safety mechanisms can be provided with other safety-related documentation for the IP. This information can also be combined into a single safety manual or safety application note as described in 5.1.11 (for digital components), 5.2.6 (for analogue or mixed signal components), 5.3.6 (for PLD) and 5.5.6 (for sensors/transducers).

NOTE 4 The base failure rate depends on the actual implementation, including the technology, of the IP into the integrated circuit and the use condition of the integrated circuit, as described in 4.6. So the base failure rate can only be provided as a reference to the IP integrator who is responsible for recalculating the failure rate according to the actual use case.

NOTE 5 This information can be included within existing documentation (e.g. integration guidelines, technical reference documents, application notes).

The IP integrator can request additional information from the IP supplier in implementing safety requirements. The IP supplier can support the request by providing information concerning measures used to avoid systematic faults, as well as safety analysis results. Safety analysis results can be used to support the evaluation of hardware metrics for the integrated IP, as well as to demonstrate freedom from interference and independence.

Since the IP will be integrated into a safety-related design, consideration of coexistence is important to ensure that the integrated IP cannot have an adverse impact on other safety-related functions. In order to claim freedom from interference, dependent failure analysis as described in ISO 26262-9:2018, Clause 6 and ISO 26262-9:2018, Clause 7 can be used, together with the additional guidance in 4.7 of this document.

If the IP integrator determines that the fulfilment of safety requirements is not possible with the supplied IP, a change request to the supplier can be raised as described in ISO 26262-8:2018, 5.4.4 and, in cases where the IP is an SEooC, ISO 26262-10 [61]. Alternatively, other measures by the IP integrator to comply with safety requirements can be applied, such as additional safety mechanisms at integration level. Safety mechanisms can be implemented in hardware, software, or a combination of both. If evidence of a compliant development is missing, ISO 26262-8:2018, Clause 13 and ISO 26262-8:2018, Clause 14, can provide alternative means to argue compliance.

The IP integrator is responsible for each integration and associated verification and testing activities related to the allocated safety requirements and safety mechanisms, as applicable.

NOTE 6 The IP supplier is responsible for ensuring that the delivery complies with the specified properties and for avoidance of systematic faults in the generated IP. Moreover the IP supplier provides supporting information to allow the IP integrator to conduct integration activities.

4.5.3 IP lifecycle

4.5.3.1 Introduction

Avoidance and detection of systematic faults during the IP lifecycle are required to ensure that the resulting design is suitable for use in applications with one or more allocated safety requirements. Requirements for avoidance and detection of systematic faults are provided in ISO 26262-5:2018, Clause 7, in the context of hardware design. In this document, 5.1.9 (for digital components), 5.2.5 (for analogue or mixed-signal components), 5.3.5.3 (for PLD) and 5.5.5 (for Sensors and Transducers) provide further guidance. This guidance can be used to determine the general methods that can be used during IP development to avoid and detect systematic faults.

For IP which exhibits programmable behaviour, ISO 26262-4:2018, 6.4.6.5 can be considered as well as the guidelines described in 5.3.

The IP integrator is responsible for integrating the supplied IP. For the integration activities the assumptions of use and integration guidelines described for the IP are considered. The impact of

© ISO 2018 – All rights reserved

AVA Documents Document Sharing Hub
Full document details: BS ISO 26262-11:2018

assumptions of use which cannot be fulfilled by, or which are invalid for, the design into which the IP is being integrated is analysed and considered with change management conducted as described in ISO 26262-8:2018, Clause 8. Figure 7 provides an example lifecycle based on SEooC development, as already provided in ISO 26262-10 [61].

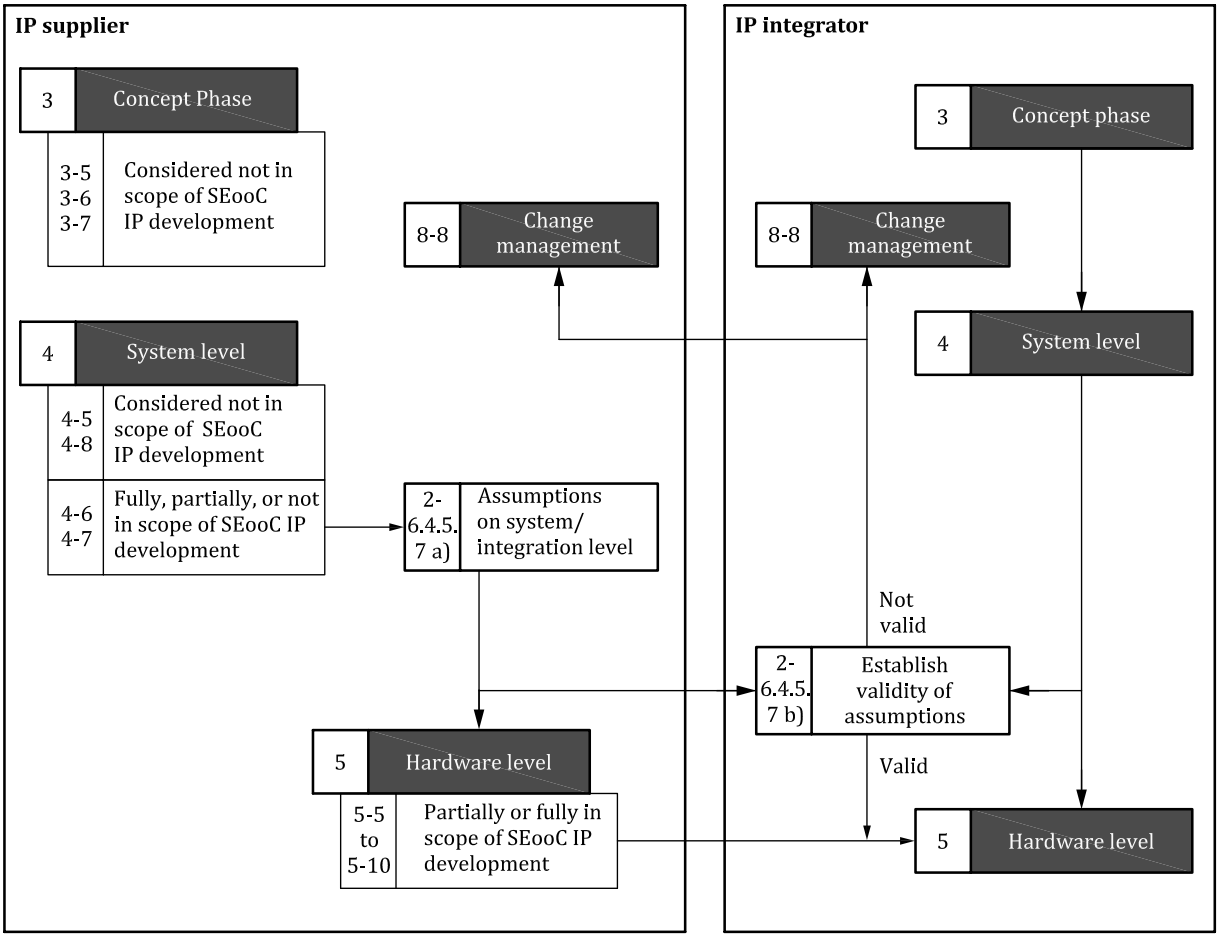

Figure 7 — IP lifecycle when IP is treated as SEooC

NOTE 1 The references shown in Figure 7 are related to the ISO 26262 series of standards.

NOTE 2 In Figure 7, ISO 26262-5:2018, Clause 10 is only partially the responsibility of the IP supplier because a number of the related requirements are not applicable to IP suppliers, such as ESD tests.

The DIA can define work products (as listed in 4.5.4) to be provided by the IP supplier to support the IP integrator in IP integration activities.

4.5.3.2 IP as SEooC

When developing an SEooC IP, applicable safety activities are tailored as described in ISO 26262-2:2018, 6.4.5.7. Such tailoring for the SEooC development does not imply that any step of the safety lifecycle can be omitted. In cases where certain steps are deferred during the SEooC development, they can be completed during the item development.

In cases where a mismatch exists between the SEooC ASIL capability (see ISO 26262-1:2018, 3.2) and the ASIL requirements specified by the IP integrator, the IP integrator can implement additional safety mechanisms external to the IP. Additional safety measures for systematic failure avoidance are also considered. It is possible to use ASIL decomposition as defined in ISO 26262-9:2018, Clause 5, provided that it can be shown that there are redundant and independent requirements, and the methods for systematic failure avoidance and control for the integrated IP are taken into account.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

An SEooC is developed based on assumptions of the intended functionality and use context which includes external interfaces. These assumptions are set up in a way that addresses a superset of components into which the SEooC can be integrated, so that the SEooC can be used later in multiple different designs. The validity of these assumptions is established in the context of the actual component integrating the SEooC. In that context, IP developed as an SEooC can often be configured to target a number of different designs. Configuration can be done before synthesis, after synthesis, or by fuse, laser cut, flash, or any other programming. In that case, the IP supplier provides information on the IP configurations which have been covered by testing and verification activities.

EXAMPLE Configuration options to determine bus width for interconnects, internal cache memory sizes, number of interrupts, memory maps.

NOTE 1 IP configuration differs from configuration data for software: therefore ISO 26262-6:2018, Annex C is not directly applicable to IPs.

NOTE 2 The IP integrator performs the necessary verification activities to guarantee the correctness of the generated IP; the necessary work products, as listed in following clauses, are made available; and the IP integrator verifies the correct integration of the IP in its context.

4.5.3.3 IP designed in context

When developing IP in context, the IP supplier tailors the safety activities as described in ISO 26262-2:2018, 6.4.5.1. For in context designs, the IP supplier can develop the IP with knowledge of the safety requirements.

EXAMPLE An analogue component designed in context of a specific safety requirement at the system level.

4.5.3.4 IP use through evaluation of hardware element

In cases where no SEooC or in-context information is available for the IP, evaluation of hardware elements as described in ISO 26262-8:2018, Clause 13 can be used to increase confidence in the IP. Activities foreseen for the evaluation of hardware elements can be applied to IP without pre-existing supporting information available (as described in 4.5.5).

4.5.3.5 IP use through the “proven in use” argument

If the evidence for systematic faults avoidance is not available, the “proven in use” argument as described in ISO 26262-8:2018, Clause 14 can provide a means for the IP integrator to demonstrate compliance with ISO 26262.

The conditions surrounding the validity of the “proven in use” argument can be restricting. Ensuring that an effective field monitoring program described in ISO 26262-8:2018, 14.4.5.3 is in place can be challenging due to the typically limited field feedback from designs incorporating IP or due to differences in IP configuration.

4.5.4 Work products for IP

4.5.4.1 List of work products for IP

Example work products are described in 5.1.11 (for digital components), 5.2.6 (for analogue or mixed signal components), 5.3.6 (for PLD) and 5.5.6 (for Sensors and Transducers). The following gives guidance on contents of work products which can be provided for IP designs in general.

NOTE The DIA (see ISO 26262-8:2018, Clause 5) can be used to specify which documents are made available to the IP integrator and what level of detail is included.

4.5.4.2 Safety plan

For IP with one or more allocated safety requirements, the safety plan is developed based on the requirements in ISO 26262-2:2018, 6.4.6. A single plan or multiple related plans can be used. Detailed

© ISO 2018 – All rights reserved

AVA Documents Document Sharing Hub
Full document details: BS ISO 26262-11:2018

plans are included for applicable supporting processes as described in ISO 26262-8, covering configuration management, change management, impact analysis and change requests, verification, documentation management and software tool qualification.

4.5.4.3 Safety requirements allocated to the IP design

The hardware safety requirements can be allocated to the IP design as defined in ISO 26262-5:2018, Clause 6.

EXAMPLE The requirement for a safety mechanism in the IP is described, allowing the requirement to be verified at an appropriate level of integration. The integration and test specifications can be linked to requirements defined in the technical safety concept.

4.5.4.4 Hardware design verification and verification review of the IP design

Defining criteria for design verification, in particular for environmental conditions (vibration, EMI, etc.), for an IP design which is provided in the form of logic design is not typically possible since the physical characteristics are highly dependent on the physical implementation of the design by the IP integrator.

NOTE For IP provided as a digital logical design, hardware design verification can be done using the techniques listed in 5.1.9.

A verification report includes results of the activities used to verify the IP design. Verification can be done as described in ISO 26262-8:2018, Clause 9, including planning, execution and evaluation of verification activities.

4.5.4.5 Safety analysis report

The requirements for safety analysis in ISO 26262-9:2018, Clause 8 are applicable for IP designs. The selection of appropriate safety analysis methods is based on ISO 26262-5:2018, Table 2.

For qualitative analysis, the supplier provides the identified failure modes of the IP in order to support its integration.

For quantitative analysis, the data included supports the evaluation of hardware architectural metrics and evaluation of safety goal violations due to random hardware faults, as specified in ISO 26262-9:2018, 8.4.10.

EXAMPLE Data includes estimated failure rate and failure mode distribution information.

NOTE 1 For IP provided as logical design, such as Register Transfer Level (RTL), quantitative analysis relies on assumptions about failure rates and failure mode distributions, and can therefore not be representative of actual physical designs. The IP integrator verifies the assumptions and quantitative safety analysis results for the specific implementation.

NOTE 2 In estimating the metrics, safety mechanisms embedded in the IP and their expected failure mode coverage (at a level that is applicable to the given IP) can be considered.

In the case of configurable IP, the safety analyses can include information about the impact of configuration options on the failure modes distribution.

NOTE 3 An analysis of the impact of configuration options on the implementation and diagnostic coverage of safety mechanisms is performed.

Additional safety mechanisms realized by a combination of features internal and external to the IP, as well as safety mechanisms implemented outside the IP can be defined. These additional safety mechanisms can rely on assumptions of use for the SEooC design, which can be validated at the appropriate level as described in ISO 26262-2:2018, 6.4.5.7.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

4.5.4.6 Analysis of dependent failures

Dependent failure analysis for IP can be performed as described in ISO 26262-9:2018, Clause 7. Additional guidance on how to apply dependent failure analysis for semiconductor devices is included in 4.7 of this document.

4.5.4.7 Confirmation measures

Results from conducted confirmation measures include evidence and arguments related to the IP development process and about avoidance of systematic faults. Confirmation measures are described in ISO 26262-2:2018, Table 1. For semiconductor IP typical confirmation measure reports include:

— confirmation review of the safety plan;

— confirmation review of the safety analyses;

— confirmation review of the completeness of the safety case; and

— functional safety audit and assessment reports.

Examples of techniques applicable to IP development activities for systematic fault avoidance are included in 5.1.9 (for digital components), 5.2.5 (for analogue or mixed-signal components), 5.3.5.3 (for PLD) and 5.5.5 (for Sensors and Transducers).

4.5.4.8 Development interface agreement

The requirements for distributed development in ISO 26262-8:2018, Clause 5 are applicable to IP designs. The DIA defines the exchanged work products for IP designs, and the roles and responsibilities for safety between the IP supplier and the IP integrator.

4.5.4.9 Integration documentation set

An integration documentation set can include a safety manual or safety application note for IP developed as an SEooC. The integration documentation set can also include the following information:

— description of the tailoring of the lifecycle for the IP development;

— assumptions of use for the IP, including for example:

  — assumed safe states of the IP;

  — assumptions on maximum fault handling time interval and Multiple Point Fault Detection Interval (MPFDI), as applicable;

  — assumptions on the integration environment for the IP, including interfaces; and

  — recommended IP configurations.

— description of the safety architecture, including:

  — fault detection and control mechanisms;

  — fault reporting capabilities;

  — self-test capabilities and additional requirements for self-testing for potential latent faults, if applicable;

  — fault recovery mechanisms, if applicable; and

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

  - impact of configuration parameters on the above items if applicable.

- hardware-software interfaces required to support the IP safety mechanisms, and to control failures after detection;

- specification of software-based test routines to detect faults of the IP component, if applicable. This could also be provided as source code or binary library;

- description of safety analysis results for the IP; and

- description of confirmation measures used for the IP.

It is possible for the IP integrator to formally identify each hardware feature related to the safety mechanisms so that a mapping with hardware safety requirements at the level of the IP integrator can be done, and the integration verification and validation activities that are the responsibility of the IP integrator can be identified.

NOTE 1 The IP safety mechanism requirements are specified in a way which allows them to be traceable to IP integrator's requirements.

NOTE 2 For IP with no specific features for fault detection, providing the assumptions of use can be sufficient to comply with the IP integrator's requirements.

For IP developed in-context, similar documentation is typically provided.

NOTE 3 For in-context IP, assumptions of use are not required, as the IP is designed with full context information in place.

4.5.4.10 Applicability of work products to IP categories

The applicability of the work products described in 4.5.4.1 to 4.5.4.9 depends on the classification of the IP as described in 4.5.2. For intellectual properties without integrated safety mechanisms:

- the safety analysis report is limited to the failure modes distribution of the IP. There is no estimation of the hardware metrics because there are no integrated safety mechanisms. The failure mode distribution is needed to enable the IP integrator to perform safety analyses at the integration level;

- the integration documentation set (not a specific work product but rather a collection of information as described in 4.5.4.9) is limited to the description of the assumptions on the integration environment for the IP, including interfaces;

- it does not typically include the analysis of dependent failures.

4.5.5 Integration of black-box IP

In some developments the IP integrator can encounter a situation where it is necessary to integrate an IP of which the contents are not fully disclosed. The IP to be integrated is a "black box" from the perspective of the IP integrator.

EXAMPLE 1 IP integrator's customer requires use of their proprietary logic, such as a specific communications interface, timer peripheral, or similar logic.

EXAMPLE 2 IP integrator is asked to integrate logic from a competitor, in order to facilitate a multi-source supply agreement.

Black box IP can be integrated in many forms, including but not limited to:

- pre-hardened, or handed off as a gate level layout or transistor level;

- as encrypted netlist, which cannot be meaningfully parsed except by trusted tools; and

- as obfuscated RTL source (where meaningful variable names are replaced with randomized character strings and any explanatory comments are removed).

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

NOTE 1 A black box integration approach can also be applied to cases in which no information is available from the IP supplier.

When black box IP is integrated, the division of responsibility between IP supplier, IP integrator and the IP integrator's customer can be defined through a development interface agreement as described in ISO 26262-8:2018, Clause 5.

EXAMPLE 3 In cases where the IP integrator is required to use black box IP, for example because of a requirement from their customer, the DIA can specify that it is the customer responsibility to evaluate and accept the suitability for the use of the black box IP in a safety-related context.

The development interface agreement can also include details about the tailoring of the safety activities as described in ISO 26262-2:2018, 6.4.5.7 and the exchange of documentation across the supply chain.

EXAMPLE 4 A development interface agreement can specify that integration details are provided by the IP supplier in the form of an integration guide which also contains a set of validation tests. These tests can be used to confirm proper integration.

Unless the IP has been developed specifically targeting the automotive market, it is possible that specific evidence is not available. In this case the responsibility for the acceptance of available evidence can be defined in the development interface agreement.

EXAMPLE 5 IP developed according to other functional safety standards such as IEC 61508:2010 [14].

NOTE 2 In this case information on the development lifecycle and associated processes used to develop the IP can be used to perform a gap analysis to evaluate the suitability of the IP for use in the context of ISO 26262 series of standards.

The IP integrator does not always have enough data to evaluate the base failure rate of a black box IP. Since this can affect the results of quantitative analysis, the development interface agreement can specify the responsibilities between the IP supplier, IP integrator and the IP integrator's customer for the estimation of the base failure rate. The responsibilities for safety analysis of the black box IP can be defined in a similar way.

NOTE 3 The integration of black box IP into a hardware development has parallels in software development, such as the case in which a developer integrates unit software from a third-party supplier as compiled object code. As such, the integrator of black box IP into a hardware development can find methods and techniques in 5.1.9.1 including the link with applicable tables of ISO 26262-6.

In cases where the black box IP requires safety mechanisms, the IP integrator could not have enough information to implement the safety mechanism outside of the IP. The development interface agreement specifies requirements for such safety mechanism in these cases.

4.6 Base failure rate for semiconductors

4.6.1 General notes on base failure rate estimation

4.6.1.1 Introduction

The scope of this sub-clause is to give clarifications, guidelines and examples on how to calculate and use the base (or raw) failure rate. Base failure rate is a primary input for calculation of the quantitative safety analyses and metrics according to ISO 26262-5.

NOTE Quantitative safety analysis in ISO 26262-5 focuses on random hardware failures and excludes systematic failures. Therefore the base failure rate used in the context of ISO 26262 series of standards focuses on random hardware failures only. See also 4.6.1.3.

Each technique available for base failure rate estimation makes assumptions about the failure mechanisms to be considered. Differences in results obtained from different base failure rate estimation techniques are often due to a lack of consideration for the same set of failure mechanisms. Results from

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

the use of different techniques applied to the same component are unlikely to be comparable without harmonization on a common set of failure mechanisms.

EXAMPLE 1 Harmonization can be done, for instance, by considering the same failure mechanisms and the same source of stresses.

Failure mechanisms for semiconductors are dependent on circuitry type, implementation technology, and environmental factors. As semiconductor technology is rapidly evolving, it is difficult for published recognized industry sources for failure rates to keep pace with the state of the art, particularly for deep submicron process technologies. Because of this, it is helpful to consider the publications of industry groups such as JEDEC (Joint Electron Device Engineering Council), International Roadmap for Devices and Systems (IRDS), and the SEMATECH/ISMI Reliability Council to get a broad view of semiconductor state of the art.

EXAMPLE 2 JEDEC publishes several documents which can be helpful in providing references to understand specific failure mechanisms and estimate failure rates:

— Reference [16] summarises many different well understood and industry accepted failure mechanisms for silicon and packaging; it can also be used to provide a physics of failure mode for estimation of failure rates for the identified failure mechanisms;

— Reference [53] provides guidance on developing a reliability evaluation methodology based on an application-specific use model (mission profile); and

— Reference [17] summarises a number of transient fault mechanisms related to exposure to naturally occurring radiation sources and provides guidance on how to experimentally derive failure rates for susceptibility to soft error.

4.6.1.2 Quantitative target values and reliability prediction

Quantitative target values for the maximum probability of the violation of each safety goal at item level due to random hardware failures (PMHF) are sometimes misunderstood as inputs for reliability prediction. As stated in ISO 26262-5:2018, 9.4.2.2, NOTE 1, these quantitative target values do not have an absolute significance but are useful for comparing a new design with existing ones. They are intended to make available design guidance and to make available evidence that the design complies with the safety goals. Therefore those values cannot be used “as is” in reliability prediction.

4.6.1.3 Difference between systematic and random failures

ISO 26262 series of standards makes a distinction between systematic and random failures. Most available techniques for base failure rate estimation are intended to provide reliability estimates and make no such distinction. The result of such techniques can be excessively conservative due to inclusion of factors which estimate systematic failures. For example, estimation techniques based on observations of field failures do not, in general, have appropriate sample size or observation quality to differentiate between systematic and random failures. Similarly, models which include systematic capability as part of the base failure rate calculation can be challenging to use in the context of ISO 26262 series of standards (e.g. π_{pm} and $\pi_{process}$ factors defined in Reference [9]).

4.6.1.4 Effect of failure recovery mechanisms

A concern is the handling of diagnostics which can be used to enhance availability. This can lead to a mix of base failure rate with diagnostics while the ISO 26262-5 requires separating them for the metrics computation.

EXAMPLE Consider a common SEC-DED (Single Error Correct-Dual Error Detect) ECC used in many state of the art automotive functional safety electronics. A reported MTTF (mean time to failure) for an SRAM with SEC-DED ECC cannot consider a fault which results in a correctable error — thus mixing effects of base failure rate and diagnostics, which is separated for calculation of ISO 26262-5 metrics.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

4.6.1.5 Considerations about non-constant failure rates

Many standardised models make use of a “bathtub curve” simplification, which assumes that “early life” (infant mortality) defects have been effectively screened by the supplier and that “wear out” (end-of-life) failure mechanisms, such as electro-migration, time-dependent dielectric breakdown, hot carriers, or negative bias temperature instability will effectively occur at negligible rates during useful mission lifetime.

In some cases, the failure rate distribution from reliability models does not fit the constant failure rate of the "bathtub curve" simplification. Using a non-constant failure rate is not compatible with the computation of hardware architectural metrics as described in ISO 26262-5.

One possibility is to simplify non-constant failure rate distributions by using approximations of constant failure rate.

EXAMPLE 1 A constant failure rate is conservatively assumed at the maximum failure rate of the reliability model failure rate distribution.

EXAMPLE 2 Depending on the distribution, it can be possible to limit the operating lifespan of the product such that a constant failure rate approximation is more appropriate. This case often applies when an end-of-life mechanism becomes dominant in the overall failure rate distribution.

NOTE 1 If an exponential model is used, reaching the end of the bathtub within the product lifetime is a systematic issue when failure rate targets are exceeded. If this is acceptable or not is not evaluated within the hardware metrics of ISO 26262-5:2018 Clause 8 and Clause 9. This is evaluated separately, for example based on the results of the qualification of an integrated circuit according to AEC-Q100 [62].

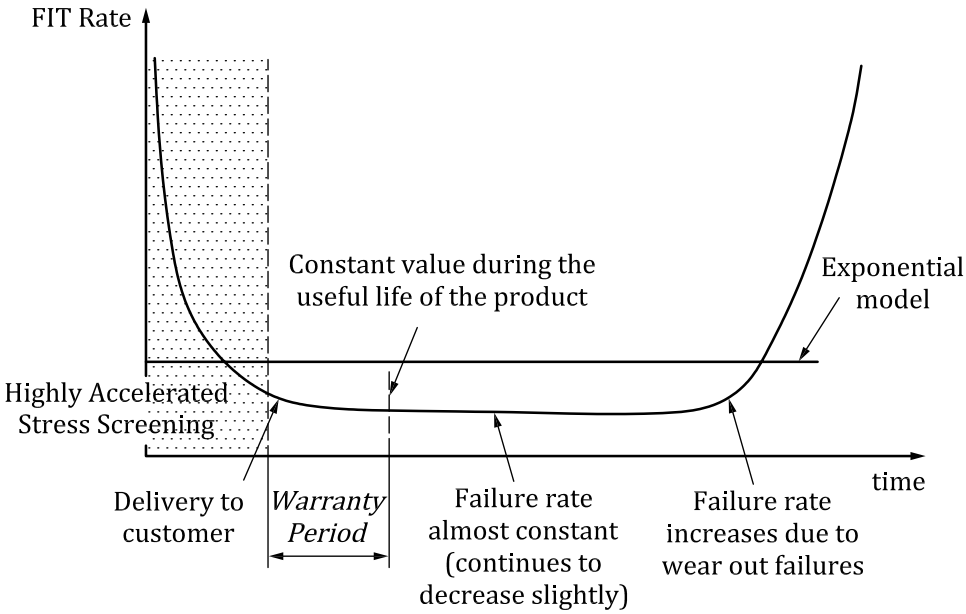

Figure 8 — Bathtub curve — Evolution of failure rate over time

NOTE 2 In Figure 8, the real bath tub curve can be approximated by the ‘Constant value during the useful life of the product’ or calculated by the exponential model with the confidence level of 70 %.

If the overall failure rate distribution is a result of integrating multiple fault models, separation of failure modes can result in the ability to simplify safety analysis by evaluating the impact of each failure mode separately using different (but constant) failure rate approximations, as recommended in 5.1.7.2 for consideration of transient faults.

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

4.6.1.6 Techniques and sources for base failure rate estimation

There are many different techniques which can be utilised for base failure rate estimation. In general these techniques can be summarised as follows:

— failure rates derived from experimental testing, such as:

  — temperature, bias and operating life test (TBOL), also known as High Temp Operational Life (HTOL) testing or extended life test (ELT) for intrinsic product operating reliability,

  — reliability test chip and/or on-chip test structures to assess intrinsic reliability of the silicon technology,

  — soft error testing based on exposure to radiation sources, or

    NOTE 1 JEDEC standards such as JESD89 [17] give guidance for soft error testing.

  — convergence characteristic of acceleration test for screening.

— failure rates derived from observation of field incidents, such as analysis of material returned as field failures;

  NOTE 2 For permanent faults: data provided by semiconductor industries can be based on the number of (random) failures divided by equivalent device hours. These are obtained from field data or from accelerated life testing (as defined in standards such as JEDEC and AEC) scaled to a mission profile (e.g. temperature, on/off periods) with the assumption of a constant failure rate (random failures, exponential distribution). The numbers can be used as inputs for the estimation of the failure rate, provided as a maximum failure rate based on a sampling statistics confidence level.

— failure rates estimated by application of industry reliability data books or derived from them and combined with expert judgment;

  EXAMPLE 1 IEC 61709 [15], SN 29500 [38] or FIDES Guide [9].

  EXAMPLE 2 Model for reliability prediction of electronics components (former IEC TR 62380) as described in 4.6.2.1.1.

  NOTE 3 The actual failure rate achieved is expected to be lower than the failure rate derived from those methods.

  EXAMPLE 3 Reliability estimations via physics of failure methods as in ISO 26262-5:2018, 8.4.3, Notes 6 and 7.

— The documents maintained by the International Roadmap for Devices and Systems (IRDS) such as the International Technology Roadmap for Semiconductor (ITRS [41]) provide projected values for the soft error rate for each generation so that this information is useful for a first estimation and refined when technology data is available.

4.6.1.7 Documentation on the assumptions for base failure rate calculation

When calculating the base failure rate the supplier provides documentation describing the assumptions made and supporting rationale.

EXAMPLE Assumptions can be:

— the selected method to calculate the failure rate (e.g. industry source or field data),

— the assumed mission profile,

— the confidence level of the used failure rate data (e.g. in case of field data or testing based data),

— any scaling or de-rating applied to the failure rate data,

— how the non-operating time and solder joint were taken into account, or

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

— the model used for failure rate derived from field data (Weibull or exponential models).

This information can be used by the integrator at element or item level to evaluate, understand, judge, compare and possibly harmonize failure rates from different suppliers and components.

4.6.1.8 Transient fault quantification

As described in 5.1.2, soft errors are a typical example of transient faults.

Transient faults caused by soft errors initiated by internal or external α, β, neutron, or γ radiation sources are random hardware failures that can be quantified with a probabilistic method supported by measured data.

Transient faults caused by EMI or cross-talk are not quantified. Even if they can lead to the same effects as other transient faults, they are mostly related to systematic causes. These can be avoided with proper techniques and methods during the design phase (e.g. cross-talk analysis during component development back-end).

ISO 26262-5:2018, 8.4.7, NOTE 2 specifies that transient faults are considered when shown to be relevant due, for instance, to the technology used. Therefore, depending on the impact of the faults and when applicable, they can be considered in the safety analysis. The analysis for transient faults and permanent faults is done separately. This holds for qualitative or quantitative analysis.

Each elementary subpart type (e.g. flip flops, latches, memory elements, analogue devices) is investigated if it is susceptible to soft errors, specifically with respect to direct or induced alpha particles and neutrons. The susceptibility to those phenomena depends on the semiconductor front end technology and the materials on top of the die's surface including the package, e.g. the mould compound and the solder material (flip chip) can influence the soft error rate.

EXAMPLE 1 Base failure rate for alpha particles can be influenced by the type of package, e.g. low alpha (LA) or ultra-low alpha (ULA) emitting semiconductor assembly materials.

Depending on factors such as the technology and on the operating frequency, transient fault models like single event upset (SEU), multiple-bit upset (MBU) and single event transient (SET) are considered as in References [2] and [22].

NOTE 1 Destructive single event effects like Single Event Latch-up (SEL), Single Event Burnout (SEB), and Single Event Gate Rupture (SEGR) are not considered as transient faults because these faults lead to permanent effects.

NOTE 2 See 5.1.2 for more details on digital fault models.

JESD89 [17] is considered as the main reference related to measurement and reporting of alpha particle and terrestrial cosmic ray-induced soft errors in semiconductors. In that context, the base failure rate for soft errors is provided together with the conditions in which it has been computed or measured.

NOTE 3 Conditions such as neutron particle flux, altitude, temperature, and supply voltage are relevant to transient failure rate estimation of soft errors. JESD89 [17] is used to understand those conditions.

ISO 26262-5:2018, 8.4.3, NOTE 2 states that in applying a selected industry source the following considerations are appropriate to avoid artificial reduction of the calculated base failure rate: mission profile, the applicability of the failure modes with respect to the operating conditions, or the failure rate unit (per operating hour or per calendar hour).

EXAMPLE 2 In case of soft errors, reducing the base failure rate by only considering the operating time of the vehicle leads to an excessive and therefore artificial reduction of the average probability per hour.

NOTE 4 If the semiconductor provider delivers a de-rated soft error rate, information about the de-rating factor is made available for example in the Safety Manual as defined in 5.1.11 (for digital components), 5.2.6 (for analogue or mixed signal components), 5.3.6 (for PLD) and 5.5.6 (for Sensors and Transducers).

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

Moreover, the base failure rate for soft errors is provided without de-rating it with respect to "architectural vulnerability factors" or the effect of safety mechanisms such as ECC.

NOTE 5 Architectural vulnerability factor (AVF) is the probability that a fault in a design structure will result in a visible error in the final output of the function as, for example, described for processor designs in Reference[25].

NOTE 6 Vulnerability factors are taken into account when considering the number of safe faults, as described in 5.1.7.2.

4.6.1.9 Notes on component package failure rate

In the estimation of a hardware component failure rate, the semiconductor providers consider the failures relating to the silicon die, to the enclosure/encapsulation (e.g. case) and to the connection points (e.g. pins). The connections between the connection points to the board (e.g. solder joints) are considered as board failures and are typically considered by the system integrator during the safety analysis at the system or element level.

NOTE 1 According to Reference [59], the package failure rate $\lambda_{package}$ as calculated in the model described in Figure 9 corresponds to the fault models inside of the package itself (including e.g. the connection between the die and the lead frame) but it also includes the failure rate related to the connection between the package connection points and the board (solder joints).

NOTE 2 The failure rate of the hardware component calculated in SN 29500-2 includes the fault models related to the die and to the package however unlike the model described in 4.6.2.1.1 it does not include the failure rate of the connection between the package connection points and the board which is treated separately in SN 29500-5.

NOTE 3 FIDES Guide provides separate failure rates for package (cases) and solder joints due to thermal cycling.

NOTE 4 In reality, the failure rate of the connection between the package connection points and the board is dependent on many factors involving the specific design of the circuit board and how the board is packaged inside of a protective housing. These factors are constantly changing as both electronic components and circuit board material technologies rapidly evolve.

4.6.1.10 Consideration of power-up time and power-down time

According to ISO 26262-5:2018, 8.4.3, NOTE 2, in applying a selected industry source the following considerations are appropriate to avoid artificial reduction of the calculated base failure rate:

— mission profile;

— the applicability of the failure modes with respect to the operating conditions; and

— the failure rate unit (per operating hour or per calendar hour).

The base failure rate is provided along with the mission profile used. If the power-up and power-down times are defined in the mission profile then they can be considered for the computation of stress factors as described by the method described in 4.6.2.1.1 (τ_{on} and τ_{off}) and in SN 29500 (π_w).

4.6.2 Permanent base failure rate calculation methods

4.6.2.1 Permanent base failure rate calculation using or based on industry sources

4.6.2.1.1 Model for reliability prediction of electronics components (former IEC TR 62380)

The former IEC TR 62380 [40] is used in this document as the basis for a model for reliability prediction of electronics components.

The mathematical model used in this sub-clause is described in Figure 9.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

$$\lambda = \left(\underbrace{\left\{ \lambda_1 \times N \times {}^{-0,35\times a} + \lambda_2 \right\} \times \left\{ \frac{\sum_{i=1}^{y} (\pi_t)_i \times \tau_i}{\tau_{on} + \tau_{off}} \right\}}_{\lambda_{die}} + \underbrace{\left\{ 2{,}75\times 10^{-3} \times \pi_\alpha \times \left(\sum_{i=1}^{z} (\pi_n)_i \times (\Delta T_i)^{0,68} \right) \times \lambda_3 \right\}}_{\lambda_{package}} + \underbrace{\left\{ \pi_I \times \lambda_{EOS} \right\}}_{\lambda_{overstress}} \right) \times 10^{-9} / h$$

Figure 9 — Mathematical model for reliability prediction

In the model described in Figure 9, several parameters are used to determine the failure rate:

— a parameter per transistor per type of technology used (λ_1). A λ_1 value is provided for different types of integrated circuit families as shown in Figure 10;

— a parameter related to the mastering of the technology and valid for the whole component regardless the number of integrated elements (λ_2), as shown in Figure 10;

— a parameter related to the number of transistors of the hardware component (N);

— a parameter related to the difference between the year of manufacturing or technology release/update and the reference year (1998) (α);

— a parameter related to the operating and non-operating phases seen by the hardware component (τ_i, τ_{on} and τ_{off});

— a parameter related to a temperature stress factor [$(\pi_t)_i$] applicable to the die part of the component;

— parameters related to the possible exposure of the integrated circuit to electrical overstress (π_I and λ_{EOS}) as shown in Figure 11;

— a parameter related to the number and the amplitude of the temperature cycling seen by the hardware component (n_i and ΔT_i) as shown in Figure 11;

— a parameter related to the mismatch between the thermal coefficients of the board and the package material (α_S and α_C), as shown in Figure 11 and Figure 12; and

— a parameter related to the package (λ_3), either as a function of type of the package and its pin number S (as shown in Figure 14) or as a function of the package diagonal D for surface mounted integrated circuits packages (as shown in Figure 15).

Selection of parameters can be done based on the process technology and type of circuitry utilised by the design.

NOTE 1 In Figure 10, the "actual number" corresponds to the real number of transistors regardless the sizes of those transistors.

NOTE 2 To calculate the digital component die failure rate for the whole device, the number of equivalent gates is used. The number of effective equivalent transistors is computed by multiplying the equivalent gate count by the representative number of transistors per gate. When calculating the microcontroller die failure rate due to Complementary Metal Oxide Semiconductor (CMOS) digital logic, the contribution of each digital logic of the modules (e.g. CPU, CAN, Timer, FlexRay, Serial Peripheral Interface or "SPI") is included in N.

NOTE 3 The process maturity de-rating factor was introduced considering Moore's law and the fact that device failure rates are more or less constant. If the failure rate per transistor would have stayed the same, the failure rate would have increased according to Moore's law. This was not observed. Therefore, the transistor failure cannot stay constant when changing process nodes. One option is to use the manufacturing date. Another option, to reflect process technology changes, the year of first introduction of this particular technology node can be used instead of its year of manufacturing. To achieve independence from the silicon vendor, the year from the ITRS[41] can be used.

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

NOTE 4 For analogue parts or for the digital component built primarily on analogue process technologies, the "Linear Circuits" entry of Figure 10 can be used, unless more precise data are provided by the semiconductor vendor.

NOTE 5 If supported by adequate justification, data specific to the technology under consideration can be used in replacement of the parameters described above to achieve a more accurate estimation of base failure rate.

ABBREVIATIONS	TYPES	N Is the representative number of transistors	λ_1 in FIT	λ_2 in FIT
Silicon: **MOS : Standard circuits (3)**				
	Digital circuits, Micros, DSP	4 per gate	$3{,}4\ 10^{-6}$	1,7
	Linear circuits	Actual number	$1{,}0\ 10^{-2}$	4,2
	Digital / linear circuits (Telecom, CAN, CNA, RAMDAC, ...)	Actual number	$2{,}7\ 10^{-4}$	20
	MEMORIES:			
ROM	Read only memory	1 per bit	$1{,}7\ 10^{-7}$	8,8
DRAM/VideoRAM/AudioRAM	Dynamic, Read Access Memory	1 per bit	$1{,}0\ 10^{-7}$	5,6
High speed SRAM, FIFO	Static Read Access Memory - First in First out register; ("mixed MOS ")	4 per bit	$1{,}7\ 10^{-7}$	8,8
Low consumption SRAM	Static Read Access Memory - Low consumption; (CMOS)	6 per bit	$1{,}7\ 10^{-7}$	8,8
Double access SRAM	Double Access Static RAM	8 per bit	$1{,}7\ 10^{-7}$	8,8
EPROM,UVPROM,REPROM	Electrically programmable, UV erasable - Read only memory			
OTP	One time programmable EPROM	1 /programmable point	$2{,}6\ 10^{-7}$	34
FLASH	Electrically programmable and erasable (block) (1)			
EEPROM, flash EEPROM	Electrically programmable and erasable (word) (2)	2 /programmable point	$6{,}5\ 10^{-7}$	16
(1) Whole memory array or blocks of words erasable (2) Blocks of words or word erasable (3) MOS include CMOS, HCMOS, NMOS, ... technologies				
Silicon: **MOS : Asic circuits**				
	Standard Cell, Full Custom	4 per gate	$1{,}2\ 10^{-5}$	10
	Gate Arrays	4 per gate	$2{,}0\ 10^{-5}$	10
	USER PROGRAMMABLE LOGIC DEVICE:			
LCA (RAM based)	Logic Cell Array electrically configured by external memory	40 per gate (1)	$4{,}0\ 10^{-5}$	8,8
PLD (GAL, PAL) (2)	Electrically Programmable and erasable (AND/OR array)	3 par grid point	$1{,}2\ 10^{-3}$	16
CPLD (EPLD,MAX,FLEX, FPGA, etc)	Electrically Programmable (interconnected macrocells array) (2)	100 per macrocell	$2{,}0\ 10^{-5}$	34
(1) or 4 000 per macrocell; (2) EEPROM, EPROM, or Antifuse technologies.				
Silicon: **Bipolar circuits (1)**				
	Digital circuits	3 per gate	$6{,}0\ 10^{-4}$	1,7
	Linear circuits (FET, others)	Actual number	$2{,}2\ 10^{-2}$	3,3
	MMIC	Actual number	1,0	3,3
	Linear / Digital circuits, low voltage (< 30V)	Actual number	$2{,}7\ 10^{-3}$	20
	Linear / Digital circuits, high voltage(= 30V)	Actual number	$2{,}7\ 10^{-2}$	20
	MEMORIES – PROGRAMMABLE ARRAYS- GATE ARRAYS:			
SRAM	Static read access memories	2,5 per bit	$3{,}0\ 10^{-4}$	1,7
PROM,	Programmable read only memory	1,2 /, programmable point	$1{,}5\ 10^{-4}$	32
PLD (PAL)	One time electrically programmable logic array (AND / OR arrays)	1,6 per grid point	$1{,}5\ 10^{-4}$	32
	Gate arrays	3 per gate	$1{,}0\ 10^{-3}$	10
Bipolar include : TTL, MTTL, LSTTL, FET, JFET, ECL, etc... technologies.				
Silicon: **Bipolar and MOS circuits (BICMOS)**				
	Digital circuits	4 per gate	$1{,}0\ 10^{-6}$	1,7
	Linear / digital circuits low voltage (< 6V)	Actual number	$2{,}7\ 10^{-4}$	20
	Linear / digital circuits, high voltage (= 6V) and Smart Power	Actual number	$2{,}7\ 10^{-3}$	20
SRAM	Static Read Access Memory	4 per bit	$6{,}8\ 10^{-7}$	8,8
	Gate arrays	4 per gate	$6{,}4\ 10^{-5}$	10
Gallium arsenide				
Digital	with only normally on transistors.	5 per gate	2,5	25
Digital	with normally off and normally on transistors.	3 per gate	$4{,}5\ 10^{-4}$	16
MMIC	Low noise or low power (< 100mW) microwave circuits.	Actual number	2,0	20
MMIC	Power (> 100mW) microwave circuits.	Actual number	4,0	40

Figure 10 — Values of λ_1 and λ_2 for integrated circuits families

© ISO 2018 – All rights reserved
Documents Document Sharing Hub
Full document details: BS ISO 26262-11:2018

Technological structure	Temperature factor π_t
MOS **BiCMOS** (low voltage)	$e^{\left[A\left(\frac{1}{328}-\frac{1}{273+t_j}\right)\right]}$ A=3 480 ; (Ea=0,3 eV)
Bipolar **BiCMOS** (high voltage)	$e^{\left[A\left(\frac{1}{328}-\frac{1}{273+t_j}\right)\right]}$ A=4 640 ; (Ea=0,4 eV)
AsGa Numerical	$e^{\left[A\left(\frac{1}{373}-\frac{1}{273+t_j}\right)\right]}$ A=3 480 ; (Ea=0,3 eV)
AsGa MMIC	$e^{\left[A\left(\frac{1}{373}-\frac{1}{273+t_j}\right)\right]}$ A=4 640 ; (Ea=0,4 eV)
t_j = Junction temperature in °C.	

Interface circuits Typical calculated values			λ_{EOS} FIT	π_I
Function	**Electrical environment**			
Interfaces	Computer		10	1
	Telecoms	switching	15	1
		transmitting, access, subscriber cards	40	1
		subscriber equipment	70	1
	Railways, payphone		100	1
	Civilian avionics (on board calculators)		20	1
	Voltage supply, Converters		40	1
Non Interfaces	All electrical environment		-	0

Mathematical expression of the Influence factor $(\pi_n)_i$	$n_i \leq 8\,760$ Cycles/year	$(\pi_n)_i = n_i^{0,76}$
	$n_i > 8\,760$ Cycles/year	$(\pi_n)_i = 1,7 \times n_i^{0,60}$
n_i : Annual number of cycles with the amplitude ΔT_i		
For an on/off phase	$\Delta T_i = \left[\frac{\Delta T_j}{3} + (t_{ae})_i\right] - (t_{ae})_i$	
For a permanent working phase, storage or dormant	ΔT_i =average per cycle of the (t_{ae}) variation, during the ith phase of the mission profile.	

Mathematical expression of the influence factor Π_α	$\pi_\alpha = 0,06 \times (\lvert\alpha_S - \alpha_C\rvert)^{1,68}$
Mismatch between substrate and package for the thermal expansion coefficient	$\lvert\alpha_S - \alpha_C\rvert$
α_S	See Figure 12
α_C	

Figure 11 — Temperature and overstress factors

Linear thermal expansion coefficients	Material type	Values in ppm/°C
α_S (Substrate)	Epoxy Glass (FR4, G-10)	16
	PTFE Glass (polytetrafluoroethylene)	20
	Flexible substrate (Polyimide Aramid)	6,5
	Cu/Invar/Cu (20/60/20)	5,4
α_C (Component)	Epoxy (Plastic package)	21,5
	Alumina (ceramic package)	6,5
	Kovar (Metallic package)	5

Figure 12 — Thermal expansion coefficients α_S and α_C

Climate type	t_{ae} night	t_{ae} day-light	t_{ae} mean day-light/night	ΔT_i day-light/night
World-wide	5 °C	15 °C	14 °C	10 °C
France	6 °C	14 °C	11 °C	8 °C

Figure 13 — Climates

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

Abbreviation	Material type	Description		Pin number: S	λ_3 in FIT
SO, SOP:1,27 mm pitch	Epoxy	Plastic Small Outline, L lead; Widths: 3,8 – 7,5 mm		4 to 40	$=0{,}012\times S^{1{,}65}$
Power SO	Epoxy	idem SO with heat sink			idem SO
SOJ: 1,27 mm pitch	Epoxy	Plastic Small Outline, J Lead; Width: 10,16 mm		28 to 44	$=0{,}023\times S^{1{,}5}$
VSOP: 0,76 mm pitch	Epoxy	Very Small Outline, L Lead; Width: 10,16 mm		40 to 56	$=0{,}011\times S^{1{,}47}$
SSOP: 0,65 mm pitch	Epoxy	Shrink Small Outline, L Lead; Width: 10,16 mm		8 to 56	$=0{,}013\times S^{1{,}35}$
TSSOP: 0,65 mm pitch	Epoxy	Thin Shrink Small Outline, L Lead; Widths: 4,1 – 6,1 mm		8 to 38	$=0{,}011\times S^{1{,}4}$
TSOP I: 0,55 mm pitch	Epoxy	Thin Small Outline, L Lead on small edge; Length: 11,8 mm		18 to 32	$=0{,}54\times S^{0{,}4}$
TSOP I: 0,5 mm pitch	Epoxy	Thin Small Outline, L Lead on small edge; Length: 18,4 mm		18 to 32	$=1{,}0\times S^{0{,}36}$
TSOP II: 0,8 mm pitch	Epoxy	Thin Small Outline, L Lead on long edge; Width: 10,16mm.		28 to 54	$=0{,}04\times S^{1{,}2}$
TSOP II: 0,65 mm pitch	Epoxy	Thin Small Outline, L Lead on long edge; Width: 10,16mm.		34 to 60	$=0{,}042\times S^{1{,}1}$
TSOP II: 0,5 mm pitch	Epoxy	Thin Small Outline, L Lead on long edge; Width: 10,16mm		34 to 60	$=0{,}075\times S^{0{,}9}$
TSOP II: 0,4 mm pitch	Epoxy	Thin Small Outline, L Lead on long edge; Width: 10,16mm		34 to 60	$=0{,}13\times S^{0{,}7}$
PLCC: 1,27 mm pitch	Epoxy	Plastic Leaded Chip Carrier, J Lead, all bodies		20 to 84	$=0{,}021\times S^{1{,}57}$
CLCC: 1,27 mm pitch	Alumina	Ceramic Leadless (and Leaded) Chip Carrier, all bodies			idem PLCC
MQUAD: 1,27 mm pitch	Kovar	Metallic Quad Flat Package (PLCC footprint); all bodies			idem PLCC
PQFP, TQFP	Epoxy	Plastic (Thin) Quad Flatpack, L Lead, Bodies defined in following column	5x5 mm²	32 to 40	1,3
			10x10 mm²	40 to 60	4,1
			14x14 mm²	60 to 68	7,2
			14x20 mm²	68 to 110	10,2
			28x28 mm²	110 to 225	23
			32x32 mm²	225 to 280	29
			40x40 mm²	280 to 304	42
ED QUAD, Power QUAD	Epoxy	idem PQFP with heat sink (exposed slug)			idem PQFP
CQFP, CERQUAD	Alumina	Ceramic Quad Flat pack			idem PQFP
MQFP, MQUAD	Kovar	Metallic Quad Flat pack			idem PQFP
PBGA	Epoxy	Plastic Ball Grid Array- pas >1mm. Bodies defined in following column	13,5x15 mm²	64 to 80	11,4
			17,4x19 mm²	80 to 160	16,6
			23x23 mm²	160 to 280	26,6
			35x35 mm²	280 to 400	51,3
SBGA	Epoxy	Shrink BGA-pas 1mm-Corps 42,5x42,5 mm²		580	71
SBGA	Epoxy	Shrink BGA-pas 1mm-Corps 27x27 mm²		672	33
CBGA	Alumina	Ceramic			idem PBGA
PDIL	Epoxy	Palstic Dual In Line		8 to 64	$=9+0{,}09\times S$
CDIL, CERDIP	Alumina	Ceramic Dual In Line		8 to 64	$=9+0{,}09\times S$
PPGA	Epoxy	Plastic Pin Grid Array		40 to 160	$=9+0{,}09\times S$
CPGA	Alumina	Ceramic Pin Grid Array		40 to 160	$=9+0{,}09\times S$

Figure 14 — λ_3 values for integrated circuits as a function of S

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

Packages types	Examples	λ_3 in FIT
Two rows connections packages	SO; SOP; SOJ; VSOP; SSOP; TSSOP; TSOP I; TSOP II; etc…	$= 0{,}024 \times D^{1{,}68}$ (1)
Peripheral connections packages	PLCC; CLCC; MQUAD; PQFP; TQFP; CQFP; MQFP; etc…	$= 0{,}048 \times D^{1{,}68}$ (2)
Matrix connections packages	PBGA; CBGA; SBGA; µBGA; CSP; etc…	$= 0{,}073 \times D^{1{,}68}$ (3)
Bare die with epoxy drop	COB (chip on board)	$= 0{,}048 \times D^{1{,}68}$ (4)

Note (1) : $D = \left[\left(\left(\frac{S}{2} - 1\right) \times (pitch)\right)^2 + (Width)^2\right]^{\frac{1}{2}}$

Note (2) : $D = \left[\left(\left(\frac{S}{4} - 1\right) \times (pitch)\right)^2 + (Width)^2\right]^{\frac{1}{2}}$

Note (3) : $D = \left[(Length)^2 + (Width)^2\right]^{\frac{1}{2}}$

Note (4) : D report area diagonal

Figure 15 — λ_3 values for surface mounted integrated circuits packages

Once the base FIT rate of the component die has been generated, a de-rating factor is applied based on thermal effects and operating time. The de-rating factor is determined based on:

— junction temperature of the component die, which is calculated based on:

  — power consumption of the component die; and

  — package thermal resistance, based on package type, number of package pins and airflow;

— an application profile which defines 1 to Y usage phases, each of which is composed of an application "on-time" as a percentage of total device lifetime, and an ambient temperature; and

EXAMPLE Two examples for possible automotive profiles: "motor control" and "passenger compartment" as shown in Figure 16.

Mission profile phases	Temp. 1		Temp. 2		Temp. 3		Ratios on/off		2 night starts		4 day light starts		Non used vehicle	
Application types	$(t_{ac})_1$ °C	τ_1	$(t_{ac})_2$ °C	τ_2	$(t_{ac})_3$ °C	τ_3	τ_{on}	τ_{off}	n_1 cycles/ year	ΔT_1 °C/cycle	n_2 cycles/ year	ΔT_2 °C/cycle	n_3 cycles/ year	ΔT_3 °C/cycle
Motor control	32	0,020	60	0,015	85	0,023	0,058	0,942	670	$\frac{\Delta Tj}{3}$ +55	1 340	$\frac{\Delta Tj}{3}$ +45	30	10
Passenger compartment	27	0,006	30	0,046	85	0,006	0,058	0,942	670	$\frac{\Delta Tj}{3}$ +30	1 340	$\frac{\Delta Tj}{3}$ +20	30	10

Figure 16 — Examples of mission profiles for automotive

— activation energy and frequency per technology type to complete the Arrhenius equation.

NOTE 6 Data specific to the product under consideration, such as package thermal characteristics, manufacturing process, Arrhenius equation, etc., could be used in replacement of the general factors described above to achieve a more accurate estimation of base failure rate.

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

4.6.2.1.1.1 How to combine λ_1 and λ_2

With respect to the method described in Figure 9, multiple options exist about how to combine λ_1 and λ_2 in the case of circuit elements with different technologies (CPU, memories, etc.) implemented in the same device.

In one option, each circuit element inherits the λ_1 and λ_2 of the respective technologies, so basically the λ_1 and λ_2 are summed — as shown in Table 2.

NOTE The λ_2 values are weighted, for example with the transistor counts of the individual circuit elements as shown in the Equation (1).

$$\lambda_{\text{die}} = \sum_{\text{elements}} \left(\lambda_{1,\text{element}} \times N_{\text{element}} \times e^{-0,35\times a} + \frac{N_{\text{element}}}{N_{\text{total}}} \times \lambda_{2,element} \right) \times \frac{\sum_{i=1}^{y} \left(\pi_{t,\text{element}}\right)_i \times \tau_i}{\tau_{\text{on}} + \tau_{\text{off}}} \quad (1)$$

In this example, we assume a CMOS technology based Micro Controller Unit (MCU) which consumes 0,5 W power. The digital component die is packaged in a 144 pin quad flat package and cooled by natural convection. The MCU is exposed to the "motor control" temperature profile. The resulting increase of the junction temperature ΔT_j is 26,27 °C. An activation energy of 0,3 eV is assumed for the Arrhenius equation. Using the model in Figure 9, this results in a de-rating factor (i.e. the second factor of λ_{die}) of 0,17.

Table 2 — Digital component example with summed λ_2

Circuit Element	λ_1 (FIT)	N (transistors)	α	λ_2 (FIT)	Base failure rate (FIT)	De-rating for temp	Effective failure rate (FIT)
50 k gate CPU	$3,4 \times 10^{-6}$	200 000 (4 transistors/gate)	10	1,7	1,73	0,17	0,06
16 kB SRAM	$1,7 \times 10^{-7}$	786 432 (6 transistors/ bit for a low-power consumption SRAM)	10	8,8	8,80	0,17	1,18
						Die failure rate (FIT)	1,25

As an alternative approach, it is possible (see Table 3) to use the Equation (2) with a single (conservative) maximum λ_2 as representative value:

$$\lambda_{\text{die}} = \sum_{\text{elements}} \left(\lambda_{1,\text{element}} \times N_{\text{element}} \times e^{-0,35\times a} \times \frac{\sum_{i=1}^{y} \left(\pi_{t,\text{element}}\right)_i \times \tau_i}{\tau_{\text{on}} + \tau_{\text{off}}} \right) + Max\left(\lambda_{2,\text{element}}\right) \times \frac{\sum_{i=1}^{y} Max\left(\pi_{t,\text{element}}\right)_i \times \tau_i}{\tau_{\text{on}} + \tau_{\text{off}}}$$

(2)

Table 3 — Mixed signal example with max of λ_2

Circuit Element	λ_1 (FIT)	N (transistors)	α	Base failure rate without λ_2 (FIT)	λ_2 (FIT)	De-rating for temp	Effective failure rate (FIT)
Digital circuits	$1,0 \times 10^{-6}$	28 000	10	$8,5 \times 10^{-4}$	1,7		
Linear/digital circuits low voltage (<6 V)	$2,7 \times 10^{-4}$	30 000	10	0,25	20		
Die failure rate (FIT)				0,25	Max(20,1,7) = 20	0,17	3,44

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

In the following example the integrated circuit consists of three elements. Its composition and the corresponding λ_1 and λ_2 values from Figure 10 are shown in Table 4.

Table 4 — Composition of the example IC in BiCMOS technology

element 1	Digital circuits	λ_1 [FIT]	$1{,}00 \times 10^{-6}$	N	100 000
		λ_2 [FIT]	1,70		
element 2	Linear circuits LV	λ_1 [FIT]	$2{,}70 \times 10^{-4}$	N	5 000
		λ_2 [FIT]	20		
element 3	Linear circuits HV	λ_1 [FIT]	$2{,}70 \times 10^{-3}$	N	2 000
		λ_2 [FIT]	20		

Using the motor control profile (from Figure 16) as mission profile and 2018 as the manufacturing year, the λ_1 related term of the die failure rate is computed as in the Equations (3) to (8).

$$\lambda_{1,\text{element1}} \times N_{\text{element1}} \times e^{-0,35\times a} = \left(1,0\times 10^{-6} \times 100\ 000\right) \times e^{-0,35\times(2018-1998)} = 9,12\times 10^{-5}\ \text{FIT} \quad (3)$$

$$\left(\pi_{\text{t,element1}}\right)_1 \times \tau_1 = e^{\left[3\ 480\left(\frac{1}{328}-\frac{1}{273+32}\right)\right]} \times 0,020 = 8,99\times 10^{-3} \quad (4)$$

$$\left(\pi_{\text{t,element1}}\right)_2 \times \tau_2 = e^{\left[3\ 480\left(\frac{1}{328}-\frac{1}{273+60}\right)\right]} \times 0,015 = 1,76\times 10^{-2} \quad (5)$$

$$\left(\pi_{\text{t,element1}}\right)_3 \times \tau_3 = e^{\left[3\ 480\left(\frac{1}{328}-\frac{1}{273+85}\right)\right]} \times 0,023 = 5,60\times 10^{-2} \quad (6)$$

$$\sum_{i=1}^{3}\left(\pi_{\text{t,element1}}\right)_i \times \tau_i = 8,25\times 10^{-2} \quad (7)$$

$$\lambda_{1,\text{element1}} \times N_{\text{element1}} \times e^{-0,35\times a} \times \sum_{i=1}^{3}\left(\pi_{t,\text{element1}}\right)_i \times \tau_i = 7,53\times 10^{-6}\ \text{FIT} \quad (8)$$

An analog calculation provides for the other elements following results:

$$\sum_{i=1}^{3}\left(\pi_{\text{t,element2}}\right)_i \times \tau_i = 8,25\times 10^{-2} \quad (9)$$

$$\lambda_{1,\text{element2}} \times N_{\text{element2}} \times e^{-0,35\times a} \times \sum_{i=1}^{3}\left(\pi_{t,\ \text{element2}}\right)_i \times \tau_i = 1,02\times 10^{-4}\ \text{FIT} \quad (10)$$

$$\sum_{i=1}^{3}\left(\pi_{\text{t,element3}}\right)_i \times \tau_i = 1,01\times 10^{-1} \quad (11)$$

$$\lambda_{1,\text{element3}} \times N_{\text{element3}} \times e^{-0,35\times a} \times \sum_{i=1}^{3}\left(\pi_{t,\text{element3}}\right)_i \times \tau_i = 4,96\times 10^{-4}\ \text{FIT} \quad (12)$$

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

$$\sum_{\text{element}=1}^{3}\left[\lambda_{1,\text{element}} \times N_{\text{element}} \times e^{-0,35\times a} \times \sum_{i=1}^{3}\left(\pi_{t,\text{element}}\right)_i \times \tau_i\right] = \left(7,53\times 10^{-6} + 1,02\times 10^{-4} + 4,96\times 10^{-4}\right) \text{ FIT}$$
$$= 6,05 \times 10^{-4}\text{FIT} \quad (13)$$

For the λ_2 related term of the die failure rate we get:

$$Max\left(\lambda_{2,\text{element}}\right) = \left(\lambda_{2,\text{element}2}\right) = \left(\lambda_{2,\text{element}3}\right) = 20 \text{ FIT} \quad (14)$$

$$Max\left[\sum_{i=1}^{y}\left(\pi_{t,\text{element}}\right)_i \times \tau_i\right]_{\text{element}} = \sum_{i=1}^{3}\left(\pi_{t,\text{element}3}\right)_i \times \tau_i = 1,01\times 10^{-1} \quad (15)$$

$$Max\left(\lambda_{2,\text{element}}\right) \times Max\left[\sum_{i=1}^{y}\left(\pi_{t,\text{element}}\right)_i \times \tau_i\right]_{\text{element}} = 20\times 1,01\times 10^{-1} \text{ FIT} = 2,01 \text{ FIT} \quad (16)$$

This results in an overall die failure rate of:

$$\lambda_{\text{die}} = 6,05\times 10^{-4} \text{ FIT} + 2,01 \text{ FIT} = 2,01 \text{ FIT} \quad (17)$$

To simplify calculation, if the user can identify a match between its product and one of the integrated circuit family types listed in Figure 10 then — as shown in Table 5 below — the user can directly apply the failure rate calculation method as described in Figure 9.

Table 5 — Digital component example with matching device type

Circuit Element	λ_1 (FIT)	N (transistors)	α	λ_2 (FIT)	Base failure rate (FIT)	De-rating for temp	Effective failure rate (FIT)
50 k gate CPU	$3,4 \times 10^{-6}$	200 000 (4 transistors/gate)	10	1,7	1,80	0,17	0,31
16 kB SRAM		786 432 (6 transistors/ bit for a low-consumption SRAM)					
						Die failure rate (FIT)	0,31

4.6.2.1.1.2 Temperature de-rating

The model in Figure 9 to calculate the temperature de-rating factor δ_T uses the following parameters:

— $(\pi_t)_i$: ith temperature factor related to the ith junction temperature of the integrated circuit mission profile;

— τ_i: ith working time ratio of the integrated circuit for the ith junction temperature of the mission profile;

— τ_{on}: total working time ratio of the integrated circuit, with $\tau_{on} = \sum_{i=1}^{y}\tau_i$;

— τ_{off}: time ratio for the integrated circuit being in storage (or dormant);

— $\tau_{on} + \tau_{off} = 1$.

© ISO 2018 – All rights reserved
Documents Document Sharing Hub
Full document details: BS ISO 26262-11:2018

For the calculation of a conservative temperature de-rating factor, the off time τ_{off} can be set to zero, resulting in a slightly modified version of δ_T for the temperature de-rating factor $\delta_{T,conservative}$:

$$\delta_{T,conservative} = \frac{\sum_{i=1}^{y} (\pi_t)_i \times \tau_i}{\tau_{on}} \tag{18}$$

In Table 2, Table 3 and Table 4, the de-rating factor is calculated after considering the τ_{on} and τ_{off} time. In the above digital component example of Table 5, setting the τ_{off} to zero gives a de-rating factor of 2,91, therefore the effective failure rate value changes from 0,31 to 5,24 FIT.

4.6.2.1.1.3 Package base failure rate calculation

The package failure rate $\lambda_{package}$ as calculated in Figure 9 corresponds to the failure modes inside of the package itself (including e.g. the connection between the die and the lead frame) but it also includes the failure rate related to the connection between the package connection points and the board (solder joints) which represents approximately 20 % of the overall $\lambda_{package}$ FIT rate as described in Reference [54]. The semiconductor provider could then use 80 % of $\lambda_{package}$ value for the distribution of the hardware component package FIT rate.

As already described in 4.6.2.1.1, the package failure rate calculation takes into account the following parameters:

— π_α: influence factor related to the thermal expansion coefficients difference between the mounting substrate and the package material;

— $(\pi_n)_i$: ith influence factor related to the annual cycles number of thermal variations seen by the package, with the amplitude ΔT_i;

— ΔT_i: ith thermal amplitude variation of the mission profile; and

— λ_3: base failure rate of the integrated circuit package.

Table 6 — Package base failure rate calculation example

Package type	ΔT_j (°C)	S (Number of pins)	D (mm)	π_α	λ_3 (FIT)	De-rating for temperature cycling	Effective failure rate (FIT)
PQFP 144	26,27	144	26,58	1,05	11,87	6 009	206
Package failure rate including solder joints between package and board (FIT)							206
Total package failure rate without solder joints between package and board (FIT)							166

The influencing factor π_α is calculated using the formula shown in Figure 11, with α_s, α_c being the linear thermal expansion coefficients for the substrate and for the component respectively. In this example, we assume FR4 as mounting substrate and a plastic package for which Figure 12 delivers the values α_s = 16 and α_c = 21,5.

For an automotive profile with number of cycles/year ≤ 8 760, the parameter $(\pi_n)_i$ is calculated using the formula in Figure 11, with n_i: Annual number of cycles with the amplitude ΔT_i.

To calculate λ_3 in FIT, the formula for peripheral connections packages is used, using a width of 20 mm and a pitch of 0,5 mm as shown in Figure 15. Using the "motor control" temperature profile shown in Figure 16, this results in a total failure rate for the package without solder joints of:

$\lambda_{package}$ = 166 FIT.

The package failure rate is assumed to be equally distributed among the pins, leading to a pin failure rate of:

© ISO 2018 – All rights reserved

AVA Documents Document Sharing Hub
Full document details: BS ISO 26262-11:2018

λ_{pin} = 1,15 FIT.

NOTE 1 The package in the example is a 144 pin quad flat package and cooled by natural convection. The power consumption is 0,5 W leading to an increase of the junction temperature ΔT_j of 26,27 °C. The value of D and λ_3 are computed using Figure 15 on the basis of the following values: pitch = 0,5 mm and width = 20 mm.

NOTE 2 Not all packages are covered by the tables in Figure 14 or Figure 15. In this case expert judgment can be used to estimate the contribution of the package to the overall failure rate.

EXAMPLE 1 Package failure rate estimation is based on the knowledge of the construction and thermal characteristics of the device package and the system's printed circuit board.

NOTE 3 Equal probability for pins can be used in this example but not for all cases.

EXAMPLE 2 In BGAs, certain locations can have higher distribution than other locations.

4.6.2.1.1.4 Example of failure rate resulting from electrical overstress

The failure rate for the whole device due to electrical overstress can be calculated using the formula shown in Figure 9. If the device has a direct connection to the external environment, i.e. the device is an interface, π_I is equal to one. If the device is not an interface, i.e. it has no direct connection to the external environment, π_I is equal to zero.

Figure 11 shows different λ_{EOS} for various electrical environments. Unfortunately, an automotive electrical environment is not given. Instead the "civilian avionics (on board calculators)" can be chosen:

λ_{EOS} = 20 FIT.

This results in a failure rate due to electrical overstress for the whole device of either

$\lambda_{overstress}$ = 20 FIT, if the device has a direct contact to the external environment, or

$\lambda_{overstress}$ = 0 FIT in every other case.

To forecast the impact of electrical overstress on the device is non-trivial. If no particular impact can be argued, then $\lambda_{overstress}$ can be added to λ_{die} to increase the overall die failure rate of the whole device.

NOTE Electrical over-stress can be considered a systematic failure mode and reduced to zero FIT for calculation of random hardware failure metrics.

4.6.2.1.2 SN 29500

The SN 29500 follows a table look up approach. Expected values for failure rates under specified reference conditions are given. Values are to be looked up in tables using product type, technology and transistor count as an input. If the integrated circuits are operated under conditions different from the reference conditions a calculation from reference to operating conditions is to be used. The calculation takes into consideration temperature, voltage and drift (for analogue elements). For the temperature part of the calculation to operating conditions a modified Arrhenius equation is used.

4.6.2.1.2.1 Example of computation for a semiconductor component

Parameters required for the calculation of the failure rate with SN 29500:

— N, the number of equivalent transistors;

— λ_{ref}, the basic failure rate for the hardware component, based on the process technology;

— ΔT_j, the junction temperature increase; and

— the mission profile of the hardware component.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

NOTE 1 In cases where the number of equivalent transistors N is not listed in the failure rates families tables 1, 2 or 3 of SN 29500-2:2010 and when possible the user can use an interpolation or extrapolation method to determine the equivalent λ_{ref} and $\theta_{vj,1}$ (virtual junction temperature) values.

EXAMPLE For "microprocessors and peripherals, microcontrollers and signal processors" family as defined in SN 29500-2:2010, Table 2, the following interpolation example is done to determine λ_{ref} and $\theta_{vj,1}$ values.

Assuming a microcontroller with 500 K gates the calculation of the λ_{ref} could be done using the following steps:

— 1st step: translating λ_{ref} values from Table 2 to a same virtual reference temperature $q_{vj,1}$ for example 90 °C by using the temperature dependent factor π_T:

$$\pi_T = \frac{A \times e^{E_{a_1} \times z} + (1 - A) \times e^{E_{a_2} \times z}}{A \times e^{E_{a_1} \times z_{ref}} + (1 - A) \times e^{E_{a_2} \times z_{ref}}} \tag{19}$$

SN 29500–2:2010, Table 2 — CMOS							
(19)	**1k**	**10k**	**100k**	**1M**	**10M**	**100M**	$\theta_{vj,1}$
λ_{ref} (50°C)	25						50 °C
λ_{ref} (60 °C)		30					60 °C
λ_{ref} (80 °C)			50				80 °C
λ_{ref} (90 °C)				80	120	150	90 °C
π_T (90 °C)	5,18	3,47	1,53	1	1	1	—
λ_{ref} (90 °C)	130	105	76	80	120	150	FIT

— 2nd step: linear interpolation of λ_{ref} at 90 °C for desired complexity, i.e. 500 K transistors:

λ_{ref} **(90 °C)**							
Gates	**1k**	**10k**	**100k**	**1M**	**10M**	**100M**	$\theta_{vj,1}$
λ_{ref} (90 °C)	130	105	76	80	120	150	FIT

$$\lambda_{ref(500\ K@90\ ^oC)} = \lambda_{ref(100\ K@90\ ^oC)} + (500\ K + 100\ K) \times \frac{\lambda_{ref(1\ M@90\ ^oC)} - \lambda_{ref(100\ K@90\ ^oC)}}{1\ M - 100\ K} \tag{20}$$

$$= 76 + 400\ K \times \frac{(80 - 75)}{900\ K} = 78,2\ \ \text{FIT}$$

— 3rd step: linear Interpolation of $\theta_{vj,1}$ for the desired complexity i.e. 500 K transistors:

$$\theta_{vj,1(500\ K)} = \theta_{vj,1(100\ K)} + (500\ K - 100\ K) \times \frac{\theta_{vj,1(1\ M)} - \theta_{vj,1(100\ K)}}{1\ M - 100\ K} = 80 + 400\ K \times \frac{(90 - 80)}{900\ K} = 84,4\ ^\circ C$$

(21)

— 4th and final step: translate $\lambda_{ref(500K@90\ °C)}$ to $\theta_{vj,1(500K)}$ using the temperature dependent factor π_T:

$$\pi_{T(90\ °C\ ==>84,4\ °C)} = 0,79 \tag{22}$$

$$\lambda_{ref(500K@84,4°C)} = \lambda_{ref(500K@90°C)} \times \pi_{T(90°C\ ==>\ 84,4\ °C)} = 78,2 \times 0,79 = 62\ \text{FIT} \tag{23}$$

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

SN 29500–2:2010, Table 2 — CMOS							
Gates	**1k**	**10k**	**100k**	**1M**	**10M**	**100M**	$\theta_{vj,1}$
λ_{ref} (50 °C)	25						50 °C
λ_{ref} (60 °C)		30					60 °C
λ_{ref} (80 °C)			50				80 °C
λ_{ref} (90 °C)				80	120	150	90 °C

NOTE 2 The values regarding mission profiles are only examples. The requirements for all semiconductors within an ECU are aligned with the requirements of the respective ECU specifications.

4.6.2.1.2.2 Failure rate calculation for the semiconductor component example without non-operating phase

For the digital component example described in previous clauses, in CMOS technology with 500 k to 5 million transistors we get 80 FIT at 90 °C reference temperature condition. The following parameters are listed in Table 7 and Table 8:

— A, constant;

— E_{a1}, E_{a2}, constant activation energy in eV.

Table 7 — Parameters required for failure rate calculation example with SN 29500

N (transistors)	Technology and family	λ_{ref} (FIT)	ΔT_j (°C)	Temperature dependent reference (Z_{ref}) (1/eV)	A	E_{a1} (eV)	E_{a2} (eV)
986 432 (Digital + SRAM)	CMOS, microprocessor	80	26,27	5,11	0,9	0,3	0,7

Assuming 500 working hours per year and using the motor control mission profile as defined in Figure 16, we have the result of Table 8.

Table 8 — Digital component failure rate calculation example with SN 29500

Ambient temperature θ_U (°C)	Working time (h)	Junction temperature $\theta_{j,2}$ (°C)	Dependence factor Z (1/eV)	Temperature dependence factor $\pi_T(\theta_u)$
32	172,4	58,27	2,04	0,27
60	129,3	86,27	4,77	0,85
85	198,3	111,27	6,87	2,51
Overall Temperature Dependent Factor π_T				1,31
Effective failure rate for the overall hardware component (FIT)				105

4.6.2.1.2.3 Failure rate calculation for the semiconductor component example with non-operating phase

There is a difference between the model described in 4.6.2.1.1 and SN 29500 in the way the non-operating phases are considered. In the model described in 4.6.2.1.1 the non-operating hours are by default included in the mission profile of the product whereas in SN 29500 only the operating hours are by default considered. As described in 4.6.2.1.1.2, an alternative approach for calculating failure rate is setting τ_{off} time to zero.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

In a similar way, operating and non-operating phases can also be taken into account in SN 29500 for the calculation of the failure rate. This is done by applying a stress factor π_{ω} described in SN 29500-2:2010, 4.4. Using the motor control mission profile as defined in Figure 16 and an average temperature of 10,5 °C gives a stress factor value of 0,06. Applying the calculated stress factor to the digital component example failure rate gives the results of Table 9.

Table 9 — SN 29500 failure rate calculation with or without non-operating phases

N (transistors)	Technology and Family	λ_{ref} (FIT)	λ Without non-operating phase (FIT)	Stress Factor	λ With non-operating phase (FIT)
986 432 (Digital + SRAM)	CMOS, microprocessor	80	104,65	0,06	6,3

NOTE The non-operating average temperature is obtained from the average worldwide night and day-light temperatures (respectively 5 °C and 15 °C) as defined in Figure 13 and considering a 50 % ratio between night and day.

4.6.2.1.2.4 Method to split SN 29500 overall failure rate into die and package failure rates

As stated by the maintainer of SN 29500, the base failure rate value calculated with SN 29500 is valid for the whole hardware component only and does not provide a method to split between package failure rate and die failure rate. Therefore, the ratio of die failure rate and package failure rate is estimated based on expert judgement, if required.

EXAMPLE As example of expert judgment, an estimation of the split of package and die failure rates from an SN 29500 base failure rate could be calculated by using the same ratio as determined by method 4.6.2.1.1 or based on other industry sources which provide such data or from field data statistics when available.

4.6.2.1.3 FIDES Guide

The following is an example of the estimation of hardware failure rate as needed to support quantitative analysis using the methods detailed in the FIDES guide [9]. The failure rate model for a semiconductor per FIDES guide considers the failure rate of the device to be a factor of:

— physical contributions ($\lambda_{Physical}$);

— process contributions ($\pi_{Process}$); and

— part manufacturing contributions (π_{PM}).

The first is an additive construction term comprising physical and technological contributing factors to reliability. The second is a multiplicative term including the quality and technical control over the development, manufacturing and the usage process for the product containing the device. The third factor represents for example the quality of the manufacturing site and the experience of the supplier. $\pi_{Process}$ and π_{PM} are set to 1 as these factors are related to systematic issues.

The physical contribution is composed of stress acceleration factors due to usage conditions and an induced (i.e. unexpected overstress) multiplicative term inherent to the application of the product containing the device. However for the sake of simplicity, in the current example this induced multiplicative factor is set to 1. When actually applying it, the value based upon placement, usage controls and sensitivity to over stresses of the component is determined.

The models used in the FIDES guide for integrated circuits include the following physical stress families:

— thermal;

— temperature cycling;

— mechanical; and

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

— humidity.

NOTE For the sake of keeping the examples simple, the following calculations do not include mechanical and humidity related failure modes. These additional failure modes are considered in a real application.

To compute the digital component die and package base failure rates (i.e. before application of de-rating for operating conditions), it is necessary to consider the following elements:

— λ_{0TH}, the basic failure rate associated with the type of device and process technology; and

— physical stress parameters a and b associated with the type of package.

Those factors are combined using FIDES. Parameters selection can be based on the process technology, type of circuitry and package utilised by the design. Values are available related to Microprocessor, Microcontroller, DSP and SRAM, and PQFP package with 144 pins.

Table 10 and Table 11 below show the computation of the failure rates used in the quantitative example of a CMOS technology based MCU which consumes 0,5 W power. The digital component die is packaged in a 144 pin quad flat package and cooled by natural convection and low-conductivity board.

Table 10 — Base failure rate of the die from UTE FIDES

Circuit element	$\lambda 0_{TH}$ (FIT)
50 k gate CPU	0,08
16 kB SRAM	0,06
Sum	0,13

Table 11 — Base failure rate of the package from UTE FIDES

Package	$\lambda 0_{TCy_Case}$			$\lambda 0_{TCy_Solderjoints}$		
	a	b	$\lambda 0_{TCy_Case}$ (FIT)	a	b	$\lambda 0_{TCy_Solder-joints}$ (FIT)
144 pin PQFP	12,41	1,46	0,01	10,80	1,46	0,03

Once the base failure rate for the digital component die and package has been generated, a de-rating factor is applied based on thermal effects and operating time. The de-rating factor takes into account:

— junction temperature of the digital component die, which is calculated based on:

  — power consumption of the digital component die; and

  — package thermal resistance, based on package type, number of package pins and airflow.

— an application profile which defines 1 to Y usage phases, each of which is composed of an application "on-time", "cycle time", "cycle delta temperature", and "cycle max temperature", and "ambient temperature".

NOTE The profile for use in the model considers more/other parameters than those provided in the profile of Reference [40].

At first, the simplified mission profile example shown in Table 12 is considered.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

Table 12 — Simplified mission profile example

			Thermal	Thermal cycling			
PHASE	On/ Off	$T_{annual\text{-}phase}$ (hours)	$T_{ambient}$ (°C)	$\Delta T_{cycling}$ (°C)	θ_{cy} (hours)	$N_{cy\text{-}annual}$ (hours)	$T_{max\text{-}cycling}$ (°C)
Non-operational day	Off	720	15	10	24,0	30	20
Night start	On	168	60	55	0,25	670	60
Day start	On	335	60	45	0,25	1 340	60
Off-operational day	Off	7,538	15	10	22,5	30	20

The die base failure rate with de-rating factors is computed as in Table 13.

Table 13 — Die base failure rate with temperature de-rating factor

Circuit element	λ_{0TH} (FIT)	Derating for temperature	Effective failure rate (FIT)
50 k gate CPU	0,08	5,79	0,43
16 kB SRAM	0,06	5,79	0,32
Sum	0,13		0,75

For evaluating these de-rating factors, the junction temperature, i.e. ΔT_j due to self-heating is calculated as 18 K, using the parameters and formula described in FIDES (see Table 14).

Table 14 — Package base failure rate with temperature cycling de-rating factor

	λ_{TCy_case}			$\lambda_{TCy_solderjoints}$		
Package	$\lambda 0_{TCy_case}$ (FIT)	Derating for cycling	Effective failure rate (FIT)	$\lambda 0_{TCy_solderjoints}$ (FIT)	Derating for cycling	Effective failure rate (FIT)
144 pin PQFP	0,01	130	0,75	0,03	10	0,28

Then, the elaborated mission profile example shown in Table 15 is considered. The de-rating factors are listed in Table 16.

Table 15 — Elaborated mission profile example

			Thermal	Thermal cycling			
PHASE	On/ Off	$t_{annual\text{-}phase}$ (hours)	$T_{ambient}$ (°C)	$\Delta T_{cycling}$ (°C)	$T_{eta\ cy}$ (hours)	$N_{cy\text{-}annual}$ (hours)	$T_{max\text{-}cycling}$ (°C)
Non-operational day	Off	720	14	10	24,0	30	19
Night start	On	117	32	22	0,0	670	32
Day start	On	58	32	18	0,0	1 340	32
Full load operation	On	201	85	53	1,0	335	85
Highway operation	On	131	60	28	4,0	30	60
Off-operational day	Off	7,532	14	10	23,0	30	19

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

Table 16 — Effective failure rate

Circuit element	λ_{0TH} (FIT)	Derating for temperature	Effective failure rate (FIT)
50 k gate CPU	0,08	12,44	0,93
16 kB SRAM	0,06	12,44	0,68
Sum (FIT)	0,13		1,61

For evaluating these de-rating factors, the junction temperature, i.e. ΔT_j, due to self-heating is calculated as 18 K, using the parameters and formula described in FIDES. As shown in Table 17, the component package failure rate is then 0,25 FIT. The solder joints failure rate value in Table 17 is given as information only and is not considered as part of the package failure rate.

Table 17 — Package and solder joints failure rate

	λ_{TCy_case} (FIT)			$\lambda_{TCy_solderjoints}$ (FIT)		
Package	$\lambda 0_{TCy_case}$ (FIT)	Derating for cycling	Effective failure rate (FIT)	$\lambda 0_{TCy_solderjoints}$ (FIT)	Derating for cycling	Effective failure rate (FIT)
144 pin PQFP	0,01	42	0,25	0,03	4	0,12

4.6.2.2 Permanent base failure rate calculation using field data statistics

It is important to use field data statistics with care, as it is very difficult to get an appropriate estimation. A thorough analysis of the field return process is performed and the result of the analysis is used for the quantitative evaluations. In particular the following topics are evaluated:

— how does the field return process handle known quality issues;

— what kind of information is available about the real mission profile; and

— what is the effectiveness of the field monitoring process.

Because the methodology used to calculate the failure rate from field data has an influence on the confidence level of the resulting failure rate value, the following points are taken into account by the semiconductor suppliers:

— a proper field data collection system as required in ISO 26262-2:2018, 7.4.2.3, NOTE is put in place;

— the goal of the method is not to approximate as close as possible the real failure rate, but to provide a failure rate value for which there is a high confidence that it is above the real failure rate value;

— significant source of systematic faults are only removed from the field statistics if the source of the systematic faults has been mitigated;

EXAMPLE 1 An example of a major source of systematic faults is EOS.

NOTE 1 Evidence of mitigation of the source of the systematic fault is documented.

— because the semiconductor suppliers could not be aware of all failures in the field, a correction factor (CF) can be applied to the total number of returns. That factor can depend on many parameters such as the application and the device population used to estimate the field based failure rate;

NOTE 2 Rationale is provided from those semiconductor suppliers who estimate failure rate based on field returns.

— an acceleration factor (AF) corresponding to the temperature stress or to the thermal cycling stress effects can be respectively calculated using applicable, validated thermal strain or brittle fracture model.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

EXAMPLE 2 Coffin-Manson or Englemaier-Clech methods.

— the total operating time of the products in the field can be estimated using the mission profiles of the products when available. The variability in car usage from the drivers can also be taken into account by estimating the quantity of hours spent in field using for example a mean of 500 hours a year with a standard deviation of 145 hours; and

— the mission profile of the field data is documented and considered appropriately in the quantitative evaluations.

4.6.2.2.1 Exponential model method

The exponential model can be used in general to determine a constant failure rate from field returns. In this model, χ^2 (chi-square) statistical function gives a good approximation of the failure rate. It is proposed to use an interval estimator with a one-sided upper interval estimation at, at least, 70 % confidence level instead of using a point estimator for the failure rate. That means that with 70 % probability, the real value of the failure rate is below that value. The failure rate can be calculated using the formula below:

$$\text{FIT} = \frac{\chi^2_{CL;2n+2} \times 10^9}{2 \times \text{cumulative operational hours} \times \text{AF}} \tag{24}$$

where

n number of failures multiplied by the correction factor;

CL confidence level value (typically 70 %);

AF acceleration factor.

NOTE The acceleration factor is used to adapt failure rate values from one mission profile to another one as described in 4.6.2.2.2.

4.6.2.2.2 Calculation example of hardware component failure rate

In this sub-clause an example of a die failure rate calculation using field data statistics is given using the exponential model method. In this example we assume that the semiconductor supplier is collecting statistics from three products in the field as described in Table 18 below.

Table 18 — Mission profile and equivalent junction temperature $T_{j,eq}$

T_j (°C)	Chip 1 Phase Duration (hours)	T_j (°C)	Chip 2 Phase Duration (hours)	T_j (°C)	Chip 3 Phase Duration (hours)
–20	1 000	–25	100	–20	500
10	2 000	10	500	15	800
30	1 500	35	10 000	45	6 000
45	6 000	55	8 000	80	4 200
70	1 000	90	1 000	100	600
100	1 300	100	200	120	300
130	200	120	200	150	100
$T_{j,eq}$ (°C)	55,1	$T_{j,eq}$	51,4	$T_{j,eq}$	67,4
Total duration	13 000	Total duration	20 000	Total duration	12 500

NOTE 1 The mission profile equivalent temperature $T_{j,eq}$ corresponds to the temperature that would have the same effect as the whole mission profile from a temperature stress perspective. $T_{j,eq}$ can be calculated using the Arrhenius equation. In the above example an activation energy E_a of 0,3 eV was assumed.

Documents
Document Sharing Hub

© ISO 2018 – All rights reserved

Full document details: BS ISO 26262-11:2018

NOTE 2 The device operating hours of the different devices can be summed up together if they are referred to the same reference temperature T_{ref}. In this example T_{ref} is 55 °C and the equivalent devices hours at T_{ref} are calculated using Arrhenius equation associated with an activation energy E_a of 0,3 eV.

NOTE 3 As shown in Table 19, the failure rate per mm² value at the reference temperature T_{ref} is calculated using the χ^2 statistical function from the total number of failures and the total number of die area hours. In this example an upper confidence level of 70 % has been used.

Table 19 — Calculation of failure rate per mm² at reference temperature T_{ref}

Product Name	Die size mm²	Mission profile equivalent temp $T_{j,eq}$ (°C)	Total Device Operating hours (in million device hours)	Arrhenius Acceleration Factor	Equivalent Operating hours at a T_{ref} of 55 °C (in million device hours)	Equivalent die area hours at a T_{ref} of 55 °C (in million mm² hours)	Nb of failures during warranty period	Nb of failures with CF = 5
Chip1	30	55,1	7 000	1,00	7 022,67	210 680	1	5
Chip2	25	51,4	10 200	0,89	9 066,96	226 674	1	5
Chip3	50	67,4	5 000	1,47	7 359,25	367 963	2	10
Total die area hours						805 317	Total nb of failures	20
FIT/mm² at T_{ref} of 55 °C						0,029		

As explained in Figure 17 below, the failure rate per mm² at T_{ref} derived from the field data statistics can then be used to calculate the failure rate of the target product under design (see Table 20).

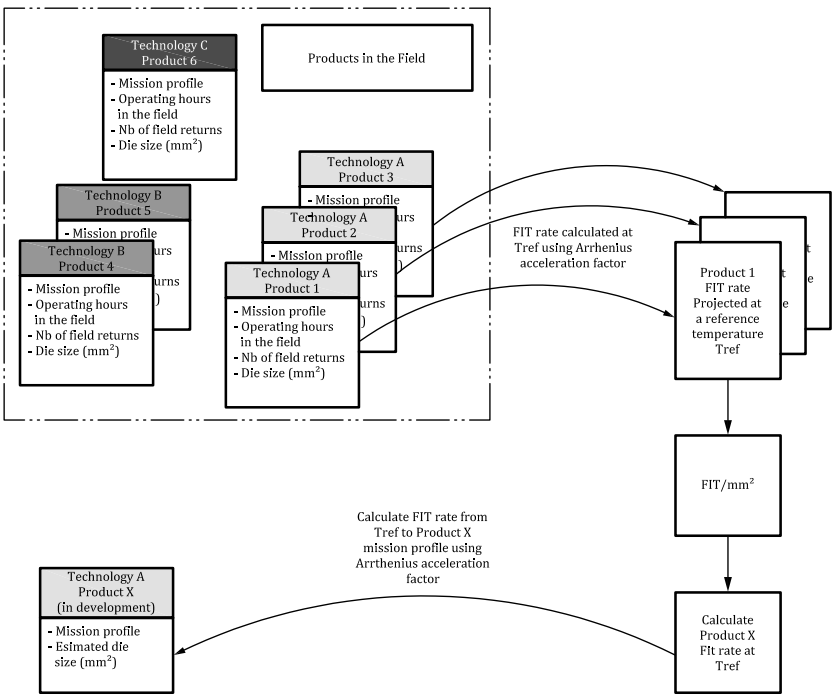

Figure 17 — Die failure rate calculation method using field data statistics

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018

Table 20 — Final chip failure rate calculation

	Mission profile Equiv. Temp $T_{j,eq}$ (°C)	Die size (mm²)	FIT/mm² at T_{ref}	Arrhenius Accelera-tion Factor	FIT/mm² at Equiv. Temp $T_{j,eq}$	Die base failure rate (FIT)
Target Chip under design	75	23	0,03	1,84	0,05	1,22

NOTE 4 Same method is applied to calculate package failure rate but the acceleration factor is calculated using Coffin-Manson or Norris-Landzberg model (as discussed in Reference [15] sub-clause 5.2.7.10 "Failure Modes", Reference [16] sub-clause 5.14 and Reference [9] sub-clause 2.5.1 "Physics of failures and models") instead of Arrhenius model. Figure 18 gives an overview of the methods used to calculate the package failure rate using field data statistics.

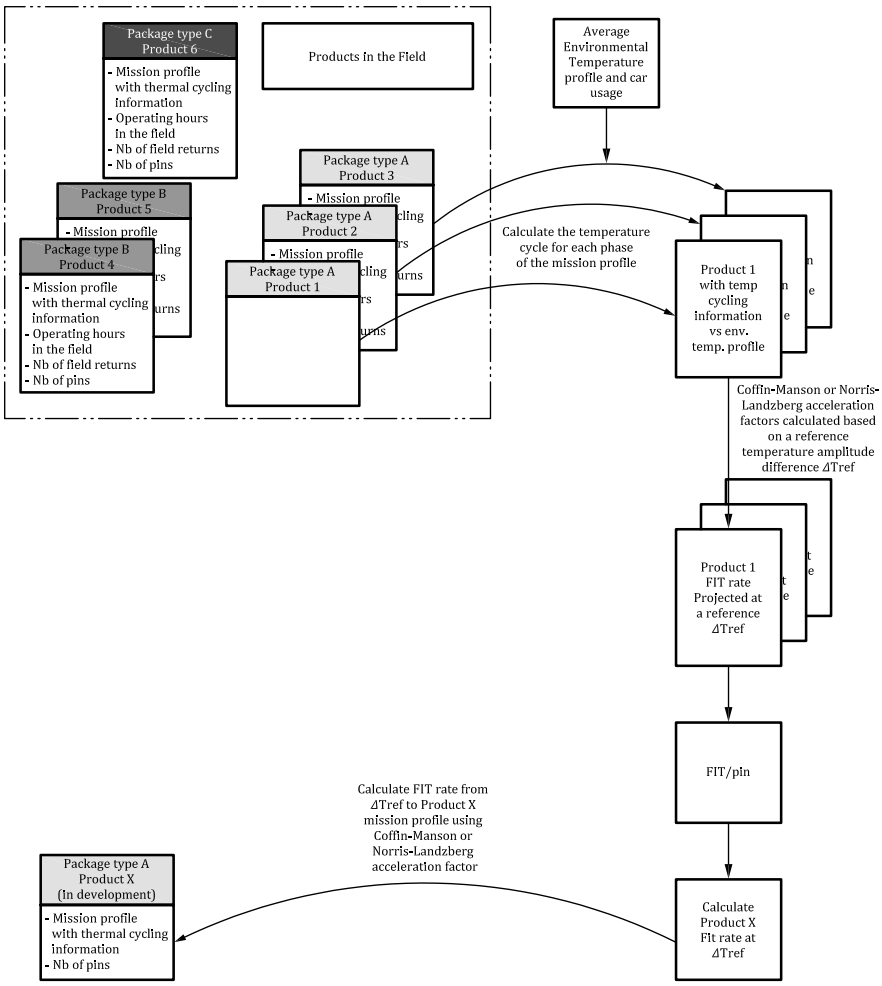

Figure 18 — Package failure rate calculation method using field data statistics

NOTE 5 In case that the field data analysis does not distinguish between die and package (as it is the case for example in SN 29500 [38]) then the Arrhenius law can be used to calculate the hardware component (die and package) failure rate using the mission profile temperatures and reference temperature T_{ref} as in Figure 18.

4.6.2.3 Base failure rate calculation using accelerated life tests

To de-rate from the temperature at which the life test is carried out to the maximum operating temperature an acceleration factor is applied. This calculation uses Arrhenius equation with activation energy of 0,7 eV. It is recommended to estimate and verify activation energy associated with desired failure mechanism.

© ISO 2018 – All rights reserved

AVA Documents Document Sharing Hub
Full document details: BS ISO 26262-11:2018

The number of faults obtained from the sample is used in the χ^2 distribution function with a certain confidence level to obtain the number of faults that would occur over the entire population tested.

Voltage acceleration is also taken into account when determining the life of devices. For CMOS, this is calculated by taking the gate oxide thickness into consideration and de-rating from the stress test voltage to the life operating voltage.

$$AF_v = \exp(\beta) \times [V_t - V_o] \quad (25)$$

where

AF_v voltage acceleration factor;

V_o gate voltage under typical operating conditions (in Volts);

V_t gate voltage under accelerated test conditions (in Volts);

β voltage acceleration coefficient (in 1/Volts).

4.6.2.4 Failure rate distribution methods

The previous sub-clauses detail several methods to determine the base failure rate for the semiconductor component. Depending on the methods, the overall semiconductor component failure rate can be available as a single value or combination of package failure rate and die failure rate. During the safety analysis the semiconductor component failure rate is allocated to the failure modes of elements composing the semiconductor component.

Different distribution methods can be applied:

- failure rate distribution of the die part of the component (i.e. digital blocks, analogue blocks and memories). Two methods can be considered to extract or obtain the distribution:
  - the first method consists of using a failure rate per mm^2 value obtained by dividing the die failure rate or the whole hardware component failure rate (if not separated into package and die contributions) by the die area of the hardware component. The failure rate distribution is done by multiplying the part or subpart area related to the failure mode under analysis by the failure rate per mm^2 value; and
  - the second method is based on base failure rates and elementary subparts. This is done by making an estimation of the number of equivalent gates (or number of transistors) for each part, subpart or basic/elementary subpart related to the failure mode under analysis.
- failure rate distribution of the package. This can be derived only when the failure rate of the package is available. In such a case, for pins that are safety-related, the distribution of the failure rate can be done using a failure rate per pin value which is obtained by dividing the package failure rate by the total number of pins of the package (safety-related or not).

NOTE The selection of the method used can be based on the layout (or planned layout) of the circuit under analysis or on the analysis of how failure modes are shared between the hardware elements.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 26262-11:2018