PUBLICLY AVAILABLE SPECIFICATION

ISO/PAS 19451-1

First edition
2016-07-15

Corrected version
2017-05

Application of ISO 26262:2011-2012 to semiconductors —

Part 1: Application of concepts

Application de l'ISO 26262:2011-2012 aux semi-conducteurs —

Partie 1: Application des concepts

Reference number
ISO/PAS 19451-1:2016(E)

© ISO 2016



COPYRIGHT PROTECTED DOCUMENT

© ISO 2016, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

 © ISO 2016 – All rights reserved

Contents

Page

Foreword ... **vi**
Introduction ... **vii**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Symbols and abbreviated terms ... **2**
5 Analogue/mixed signal components and ISO 26262 ... **4**
5.1 About analogue and mixed signal components ... 4
5.2 Analogue and mixed signal components and failure modes ... 5
5.2.1 About failure modes ... 5
5.2.2 About safe faults ... 13
5.2.3 About transient faults ... 14
5.3 Notes about safety analysis ... 14
5.3.1 General ... 14
5.3.2 Level of granularity of analysis ... 14
5.3.3 Examples of usage of failure mode distributions ... 15
5.3.4 Example of failure rates estimation for an analogue part ... 16
5.3.5 Example of safety metrics computation ... 17
5.3.6 Dependent failures analysis ... 31
5.3.7 Verification of architectural metrics computation ... 31
5.4 Examples of safety mechanisms ... 32
5.4.1 Resistive pull up/down ... 33
5.4.2 Over and under voltage monitoring ... 33
5.4.3 Voltage clamp (limiter) ... 34
5.4.4 Over-current monitoring ... 34
5.4.5 Current limiter ... 34
5.4.6 Power on reset ... 34
5.4.7 Analogue watchdog ... 34
5.4.8 Filter ... 35
5.4.9 Thermal monitor ... 35
5.4.10 Analogue Built-in Self-Test (Analogue BIST) ... 35
5.4.11 ADC monitoring ... 35
5.4.12 ADC attenuation detection ... 35
5.4.13 Stuck on ADC channel detection ... 35
5.5 About avoidance of systematic faults during the development phase ... 36
5.6 About safety documentation ... 39
6 Intellectual property and ISO 26262 ... **39**
6.1 About intellectual property ... 39
6.1.1 Understanding intellectual property ... 39
6.1.2 Types of intellectual property ... 40
6.2 Safety requirements for intellectual property ... 41
6.3 Intellectual property lifecycle ... 43
6.3.1 ISO 26262 and the intellectual property lifecycle ... 43
6.3.2 Intellectual property as safety element out of context (SEooC) ... 44
6.3.3 Intellectual property designed in context ... 45
6.3.4 Intellectual property use through hardware component qualification ... 45
6.3.5 Intellectual property use through proven in use argument ... 45
6.4 Work products for intellectual property ... 45
6.4.1 ISO 26262 and work products for intellectual property ... 45
6.4.2 Safety plan ... 45
6.4.3 Safety requirements and verification review of the IP design ... 46
6.4.4 Safety analysis report ... 46

© ISO 2016 – All rights reserved

6.4.5 Analysis of dependent failures ... 46
6.4.6 Confirmation measure reports ... 46
6.4.7 Development interface agreement ... 47
6.4.8 Integration documentation set ... 47
6.5 Integration of black-box intellectual property ... 48

7 Multi-core components and ISO 26262 ... 49
7.1 Types of MC components ... 49
7.2 Implications of ISO 26262 on MC components ... 49
7.2.1 Introduction ... 49
7.2.2 ASIL decomposition in MC components ... 50
7.2.3 Coexistence of elements with different ASILs in MC components ... 52
7.2.4 Freedom from interference (FFI) in MC components ... 53
7.2.5 Software partitioning in MC components ... 53
7.2.6 Dependent failures in MC component ... 54
7.2.7 Timing requirements in MC component ... 54

8 Programmable logic devices and ISO 26262 ... 55
8.1 About programmable logic devices ... 55
8.1.1 General ... 55
8.1.2 About PLD types ... 56
8.1.3 ISO 26262 Lifecycle mapping to PLD ... 57
8.2 Fault models and failure modes of PLD ... 60
8.3 Notes about safety analyses for PLDs ... 61
8.3.1 Quantitative analysis for a PLD ... 61
8.3.2 Dependent failure analysis for a PLD ... 65
8.4 Examples of safety mechanisms for PLD ... 67
8.5 Avoidance of systematic faults for PLD ... 68
8.5.1 Avoiding systematic faults in the implementation of PLD ... 68
8.5.2 About PLD supporting tools ... 68
8.5.3 Avoiding systematic faults for PLD users ... 68
8.6 Safety documentation for a PLD ... 70
8.7 Example of safety analysis for PLD ... 71
8.7.1 Architecture of the example ... 71
8.7.2 PLD external measures ... 72
8.7.3 PLD internal measures ... 73

9 Base failure rate estimation and ISO 26262 (all parts) ... 77
9.1 About base failure rate estimation ... 77
9.1.1 Impact of failure mechanisms on base failure rate estimation ... 77
9.1.2 Considerations in base failure rate estimation for functional safety ... 77
9.1.3 Techniques for base failure rate estimation ... 78
9.1.4 Documentation on the assumptions for base failure rate calculation ... 78
9.2 (General) clarifications on terms ... 79
9.2.1 Clarification of transient fault quantification ... 79
9.2.2 Clarification on component package failure rate ... 80
9.2.3 Clarification on power-up and power-down times ... 80
9.3 Permanent base failure rate calculation methods ... 80
9.3.1 Permanent base failure rate calculation using industry sources ... 80
9.3.2 Permanent base failure rate calculation using field data statistics ... 88
9.3.3 Calculation example of hardware component failure rate ... 91
9.3.4 Base failure rate calculation using accelerated life tests ... 94
9.3.5 Failure rate distribution methods ... 95

10 Semiconductor dependent failure analysis and ISO 26262 ... 96
10.1 Introduction to DFA for semiconductors ... 96
10.2 Relationship between DFA and safety analysis ... 97
10.3 Dependent failure scenarios ... 98
10.4 Distinction between cascading failures and common cause failures ... 100
10.5 Dependent failure initiators ... 100

 © ISO 2016 – All rights reserved

10.5.1 Dependent failure initiator list 100
10.5.2 Verification of mitigation measures 106
10.6 DFA workflow 107
10.6.1 DFA decision and identification of HW and SW elements (B1) 109
10.6.2 Identification of DFI (B2) 109
10.6.3 Sufficiency of insight provided by the available information on the effect of identified DFI (B3 and B4) 109
10.6.4 Consolidation of list of relevant DFI (B5) 110
10.6.5 Identification of necessary safety measures to control or mitigate DFI (B6) 110
10.6.6 Sufficiency of insight provided by the available information on the defined mitigation measures (B7 and B8) 110
10.6.7 Consolidate list of safety measures (B9) 110
10.6.8 Evaluation of the effectiveness to control or to avoid the dependent failure (B10) 110
10.6.9 Assessment of risk reduction sufficiency and if required improve defined measures (B11 and B12) 111
10.7 Examples of dependent failure analysis 111
10.7.1 Microcontroller example 111
10.7.2 Analog example 117

Bibliography 127

© ISO 2016 – All rights reserved

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. 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. 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 meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT), see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 22, *Road vehicles*, Subcommittee SC 32, *Electrical and electronic components and general system aspects*.

ISO/PAS 19451 consists of the following parts, under the general title *Application of ISO 26262:2011-2012 to semiconductors*:

— *Part 1: Application of concepts*

— *Part 2: Application of hardware qualification*

This corrected version of ISO/PAS 19451-1:2016 incorporates the following corrections plus other minor editorial modifications:

— Blurry figures have been replaced with clear ones.

© ISO 2016 – All rights reserved

Introduction

This document is an informative guideline which provides users of the ISO 26262 series of standards recommendations and best practices which can be utilized when applying ISO 26262 to semiconductor components and parts. This document was created by a group of industry experts including semiconductor developers, system developers, and vehicle manufacturers in order to clarify concerns seen after the initial release of the ISO 26262 series of standards and when possible to align on common interpretations of the standard.

This document serves to augment the existing normative and informative guidance in the ISO 26262 series of standards. The approach is similar to that taken in writing ISO 26262-10:2012, Annex A, “ISO 26262 and microcontrollers,” with extension to additional types of semiconductor technologies and relevant topics.

© ISO 2016 – All rights reserved

Application of ISO 26262:2011-2012 to semiconductors —

Part 1:
Application of concepts

1 Scope

This document is applicable to developers who are evaluating the use of semiconductor components or parts in hardware components, systems, or items developed according to ISO 26262.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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*

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

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

3 Terms and definitions

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

3.1
base failure rate
BFR
failure rate of a hardware element in a given application use case used as an input to functional safety analysis according to ISO 26262-5:2011, 8.4.3

3.2
guest machine
virtual instance of a *processing element* (3.7)

3.3
host machine
processing element (3.7) which implements a *hypervisor* (3.4) and one or more *guest machines* (3.2)

3.4
hypervisor
software or hardware that instantiates and manages one or more virtual design elements

Note 1 to entry: A hypervisor is sometimes referred to as a virtual machine monitor.

3.5
microkernel
μ-kernel
software which provides the minimal mechanisms needed to implement an operating system

© ISO 2016 – All rights reserved

3.6
multi-core
MC
hardware element which includes two or more hardware processing elements

3.7
processing element
PE
element providing a set of functions for data processing, normally consisting of a register set, an execution unit, and a control unit

EXAMPLE A hardware component consisting of four cores can be described as having four processing elements.

3.8
programmable logic device
PLD
device which provides user programmable logic and signal routing functions which generate application specific logic functions

3.9
virtualization
creation of a virtual (rather than physical) version of an element, including but not limited to a computer hardware platform, operating system (OS), storage device, or computer network resource

4 Symbols and abbreviated terms

ADC	Analogue to Digital Converter
ASET	Analogue Single Event Transient
BIST	Built-In Self-Test
CPU	Central Processing Unit
DAC	Digital to Analogue Converter
DFA	Dependent Failure Analysis
DFI	Dependent Failure Initiator
DMA	Direct Memory Access
DMOS	Double Diffused Metal Oxide Semiconductor (HV MOS)
DSP	Digital Signal Processor
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESD	Electrostatic Discharge
EVR	Embedded Voltage Regulator
FET	Field Effect Transistor
FFI	Freedom from Interference
FIT	Failures in Time

© ISO 2016 – All rights reserved