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 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

Contents

Page

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.

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.

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

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

FMEA	Failure Modes and Effects Analysis
FPGA	Field Programmable Gate Array
FTA	Fault Tree Analysis
GPU	Graphics Processing Unit
HV	High Voltage
HW	Hardware
HS	High Side
ISA	Instruction Set Architecture
LDO	Low Drop Output Regulator
LS	Low Side
LSB	Least Significant Bit
MMU	Memory Management Unit
MPU	Memory Protection Unit
OP AMP	Operational Amplifier
OS	Operating System
OV	Over Voltage
PAL	Programmable Array Logic
PLD	Programmable Logic Device
PLL	Phase Locked Loop
RF	Radio Frequency
SEB	Single Event Burnout
SEE	Single Event Effect
SEGR	Single Event Gate Rupture
SEL	Single Event Latch-up
SET	Single Event Transient
SEU	Single Event Upset
SMPS	Switched Mode Power Supply
SoC	System on Chip
SW	Software
UV	Under Voltage
VMM	Virtual Machine Monitor

5 Analogue/mixed signal components and ISO 26262

5.1 About analogue and mixed signal components

As described in ISO 26262-10:2012, Annex A, an integrated component is structured in parts and sub-parts. If the signals that are handled in an element (component, part or sub-part) are not limited to digital states this element is seen as analogue element. This is the case for all measurement interfaces to the physical world, including sensors, actuator outputs, and power supplies.

For analogue components, all elements are analogue and no digital element is included. Mixed signal components consist of at least one analogue element and one digital element. Since analogue and digital elements require different methodologies and tooling for design, layout, verification and testing, it is recommended to clearly partition the analogue and digital blocks. The partitioning can result in a variety of configurations ranging from analogue dominated components with digital support blocks (e.g. digitally configurable voltage regulators or auto zeroing amplifiers) to microcontrollers with a few mixed signal peripherals (e.g. analogue to digital converters and phase locked loops).

A hierarchy of a typical mixed signal component including exemplary parts and sub-parts is shown in Figure 1.

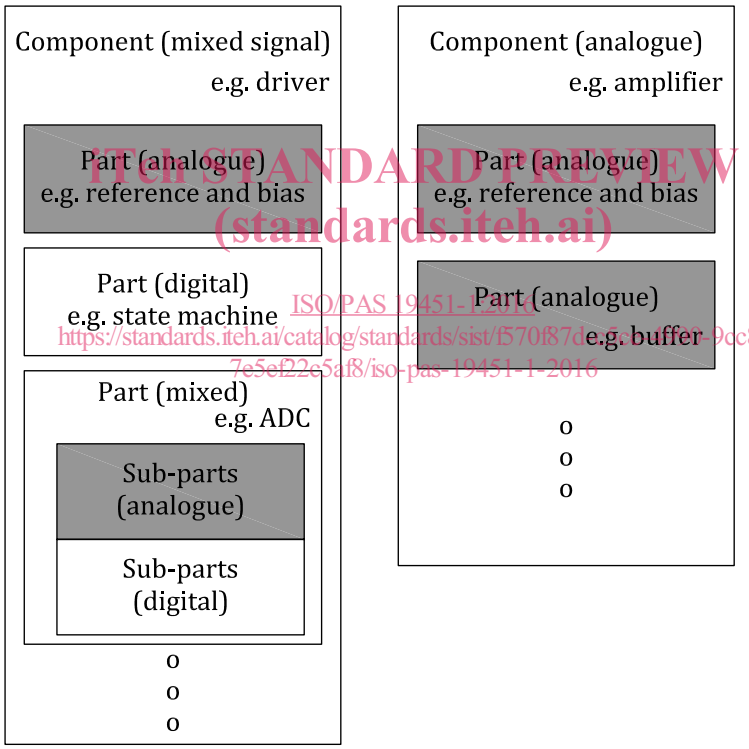

Figure 1 — Generic hierarchy of analogue and mixed signal components

It can be helpful to choose the partitioning of a mixed signal component in a way that simplifies the safety analysis. For an easy definition of fault models and failure modes, the analogue part boundaries can be defined by their function. Additionally, all elements that have freedom of interference or independence requirements (e.g. redundant paths or functions and corresponding diagnostic functions) are separated by part or sub-part boundaries. There are several additional criteria to further divide a mixed signal element (component or part) into sub elements (part or sub-part):

— Signal flow;

EXAMPLE 1 Mixed signal control loops can consist of feedback ADC, digital regulator and output driver.

— Connectivity;

EXAMPLE 2 Reference and bias circuits can serve multiple analogue blocks and oscillators can serve multiple digital or mixed signal blocks.

— Different technologies;

EXAMPLE 3 HV switch is a DMOS transistor while the gate driver can use conventional MOS devices.

NOTE One benefit for a separation of these parts is that they can have failure rates with different orders of magnitude or different fault models.

— Different supply domains;

EXAMPLE 4 Feedback DAC can be supplied with different supplies than the other mixed signal block output driver.

— Other criteria for partitioning.

EXAMPLE 5 High versus low frequency sub-parts.

The level of detail of the analysis and partitioning is determined by the relevant safety requirements, safety mechanisms and the need to show independence of safety mechanisms. A higher granularity does not necessarily result in a significant benefit for the safety analysis.

5.2 Analogue and mixed signal components and failure modes

5.2.1 About failure modes

The failure modes affecting a HW element depend on its function. The failure mode distribution depends on the HW element implementation.

NOTE The implementation includes both the actual circuit and the technology process used.

The classification of a failure mode depends on the functional and safety requirements of the system integrating the element. Based on the integration, a specific failure mode can or cannot lead to a violation of a safety requirement. Table 1 identifies possible failure modes that can be of concern for an analogue and mixed signal part or sub-part. The table can be used to extend the list of failure modes reported in ISO 26262-5:2011, Annex D.

The failure modes identified in Table 1, as well as the mentioned parts and sub-parts, are a general reference and can be adjusted on a case by case basis. The actual failure mode list used in a specific project can be adjusted (adding or removing failure modes) based on the specific implementation details or on the level of granularity deemed necessary for the analysis.

It is noted that the relevance of the failure modes, including but not limited to the ones listed in Table 1 are dependent on the context of the function to be analysed.

EXAMPLE 1 The obvious failure modes of a voltage regulator are over-voltage and under-voltage. These failure modes can be detected by an over voltage and under voltage (OV/UV) monitor as described in 5.4.2.

Besides the obvious failure modes reported in the above example, it is important to identify all relevant failure modes in order to perform a complete and thorough analysis.

EXAMPLE 2 If a voltage regulator used as a sensor supply or as an ADC reference supply, then the failure modes affecting the stability and the accuracy of the output voltage, even within the OV/UV thresholds, can be critical. Output voltage with insufficient accuracy and output voltage oscillation within the OV/UV thresholds can be mitigated by using appropriate measures. An independent ADC (internal or external) can be used to periodically measure the regulator output voltage with the required accuracy to detect those failure modes.

EXAMPLE 3 If a voltage regulator is used as a supply for a radio frequency (RF) module which has tight supply voltage ripple requirements, the prevention of fluctuation on the regulated output voltage caused by input voltage variations (i.e. the PSRR, power supply rejection ratio) is an important feature. Failure modes like output voltage oscillation within the OV/UV (i.e. ripple) limits and spikes affecting the regulated voltage can be relevant. A low pass filter as described in 5.4.8 can be used to mitigate these failures.

EXAMPLE 4 If a voltage regulator is used as an MCU core supply is sensitive to output voltage drops during start-up (power-up) due to in-rush current exceeding regulator load current and/or current limit, a too fast start-up time can be critical. A proper regulator soft-start function can be used to mitigate such failure.

If failure modes are classified as not safety related, an argument is provided in the safety analysis to support the classification.

Table 1 — Possible failure modes of analogue and mixed signal parts and sub-parts

Part/sub-part	Short description	Failure modes
Regulators and Power stages		
Voltage regulators (linear, SMPS, etc.)	HW part/sub-part that maintains the voltage of a power source within a prescribed range that can be tolerated by elements using that voltage.	Output voltage higher than a high threshold of the prescribed range (i.e. over voltage – OV) Output voltage lower than a low threshold of the prescribed range (i.e. under voltage – UV) Output voltage affected by spikes[b] Incorrect start-up time (i.e. outside the expected range) Output voltage accuracy too low, including drift[c] Output voltage oscillation[a] within the prescribed range Output voltage affected by a fast oscillation[a] outside the prescribed range but with average value within the prescribed range Quiescent current (i.e. current drawn by the regulator in order to control its internal circuitry for proper operation) exceeding the maximum value
Charge pump, regulator boost	HW part/sub-part that converts, and optionally regulates, voltages using switching technology and capacitive-energy storage elements, and maintains a constant output voltage with a varying voltage input.	Output voltage higher than a high threshold of the prescribed range (i.e. over voltage – OV) Output voltage lower than a low threshold of the prescribed range (i.e. under voltage – UV) Output voltage affected by spikes[b] Incorrect start-up time (i.e. outside the expected range) Quiescent current (i.e. current drawn by the regulator in order to control its internal circuitry for proper operation) exceeding the maximum value
High-side/Low-side (HS/LS) driver	HW part/sub-part that applies voltage to a load in a single direction: high side driver to connect the load to high rail, low side driver to connect the load to low rail.	HS/LS driver is stuck in ON or OFF state HS/LS driver is floating (i.e. open circuit, tri-stated) HS/LS driver resistance too high when turned on HS/LS driver resistance too low when turned off HS/LS driver turn-on time too fast or too slow HS/LS driver turn-off time too fast or too slow