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)

Documents
Document Sharing Hub

© ISO 2016

Full document details: ISO PAS 19451-1-2016 (2017)

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

Documents
Document Sharing Hub

Full document details: ISO PAS 19451-1-2016 (2017)

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

AVA Documents
Document Sharing Hub

© ISO 2016 – All rights reserved

Full document details: ISO PAS 19451-1-2016 (2017)

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

Documents
Document Sharing Hub

© ISO 2016 – All rights reserved

Full document details: ISO PAS 19451-1-2016 (2017)

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

Documents
Document Sharing Hub
Full document details: ISO PAS 19451-1-2016 (2017)

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
Documents
Document Sharing Hub
Full document details: ISO PAS 19451-1-2016 (2017)

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

Documents
Document Sharing Hub
Full document details: ISO PAS 19451-1-2016 (2017)

Documents
Document Sharing Hub

Full document details: ISO PAS 19451-1-2016 (2017)

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

Documents
Document Sharing Hub
Full document details: ISO PAS 19451-1-2016 (2017)

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
Documents
Document Sharing Hub
Full document details: ISO PAS 19451-1-2016 (2017)

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

© ISO 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO PAS 19451-1-2016 (2017)

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.

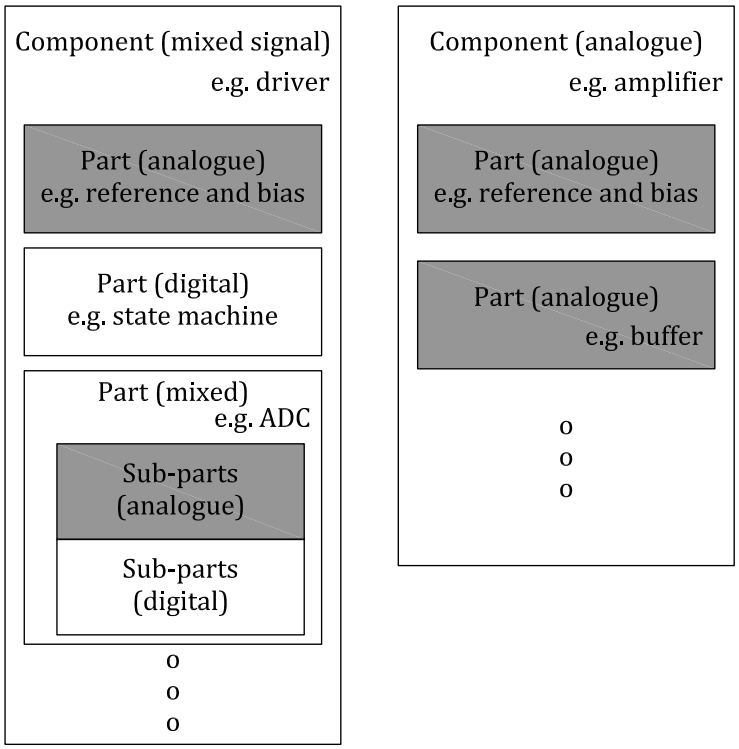

Figure 1 — Generic hierarchy of analogue and mixed signal components

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;

© ISO 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO PAS 19451-1-2016 (2017)

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.

© ISO 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO PAS 19451-1-2016 (2017)

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.

© ISO 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO PAS 19451-1-2016 (2017)

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

© ISO 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO PAS 19451-1-2016 (2017)

Table 1 *(continued)*

Part/sub-part	Short description	Failure modes
Half-bridge driver or full-bridge (H-bridge) driver	HW part/sub-part that can apply voltage across a load in either direction. A half-bridge driver is built with two drivers (one HS and one LS driver). An H-bridge (or full-bridge) driver is built with four drivers (two HS and two LS drivers)	HS/LS driver is stuck in ON or OFF state HS/LS driver is floating (i.e. open circuit, tri-stated) HS/LS driver ON resistance too high when turned on HS/LS driver OFF 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 'Dead time' is too short (i.e. when turning off high-side driver and turning on low-side driver, or when turning off low-side driver and turning on high-side driver) 'Dead time' is too long
High-side/Low-side pre-driver	HW part/sub-part driving a gate of an external FET that is used as a HS or LS driver.	HS/LS pre-driver is stuck in ON or OFF states HS/LS pre-driver output voltage/current too high or too low HS/LS pre-driver is floating (i.e. open circuit, tri-stated) HS/LS pre-driver slew rate too slow or too fast
Analogue to digital and digital to analogue converters[d]		
N bits analogue to digital converters (N-bit ADC)[d]	HW part/sub-part converting a continuous-time and continuous-amplitude analogue signal (i.e. a voltage value) to a discrete-time and discrete-amplitude digital signal coded on "N bits."	One or more outputs are stuck (i.e. high or low) One or more outputs are floating (i.e. open circuit) Accuracy error (i.e. Error exceeds the LSBs) Offset error not including stuck or floating conditions on the outputs, low resolution No monotonic conversion characteristic (i.e. given two input analogue voltage V1 > V2, the correspondent digital values are D1 < D2) Full-scale error not including stuck or floating conditions on the outputs, low resolution Linearity error with monotonic conversion curve not including stuck or floating conditions on the outputs, low resolution Incorrect settling time (i.e. outside the expected range)

© ISO 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO PAS 19451-1-2016 (2017)

Table 1 *(continued)*

Part/sub-part	Short description	Failure modes
N bits digital to analogue converters (DAC)[d]	HW part/sub-part converting digital data coded on "N bits" into an analogue signal (voltage or current).	Output is stuck (i.e. high or low) Output is floating (i.e. open circuit) Offset error (not including stuck or floating conditions on the outputs, low resolution) Linearity error with monotonic conversion curve not including stuck or floating conditions on the outputs, low resolution Full-scale gain-error not including stuck or floating conditions on the outputs, low resolution No monotonic conversion curve Incorrect settling time (i.e. outside the expected range) Oscillation[a] of the output signal including drift[c]
Oscillators and clock generators		
Oscillator	HW part/sub-part generating a periodic, oscillating signal. It can be used as clock in a digital circuit.	Output is stuck (i.e. high or low) Output is floating (i.e. open circuit) Incorrect output signal swing (i.e. outside the expected range) Incorrect frequency of the output signal (i.e. outside the expected range, including harmonics when applicable, for instance EMC emissions) Incorrect duty cycle of the output signal (i.e. outside the expected range) Drift[c] of the output frequency Jitter too high in the output signal
Phase locked loop (PLL)	HW part/sub-part controlling an oscillator in order to generate a square wave signal that maintains a constant phase angle (i.e. lock) on the frequency of an input, or reference signal. It can be used as clock in a digital circuit.	Output is stuck (i.e. high or low) Output is floating (i.e. open circuit) Incorrect frequency of the output signal (i.e. outside the expected range, including harmonics when applicable, e.g. EMC emissions) Incorrect duty cycle of the output signal (i.e. outside the expected range) Drift[c] of the output frequency Jitter too high in the output signal Loss of lock condition (i.e. phase error, output clock not in sync with input clock not leading to incorrect frequency and incorrect duty cycle Missing pulse in the output signal Extra pulse in the output signal
Generic		

© ISO 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO PAS 19451-1-2016 (2017)

Table 1 *(continued)*

Part/sub-part	Short description	Failure modes
Voltage/Current comparator	HW part/sub-part comparing an input analogue signal with a predefined threshold (i.e. voltage or current constant value) and producing a binary signal at the output; the output depends on which is higher between the input signal and the threshold and it remains constant as the difference between them stays with the same polarity.	Voltage/Current comparator not triggering when expected Voltage/Current comparator falsely triggering Output is stuck (i.e. high or low) Output is floating (i.e. open) Oscillation[a] of the output
Operational amplifier and buffer	HW part/sub-part integrating a DC-coupled high-gain voltage amplifier with a differential input and, usually, a single-ended output.	Output is stuck (i.e. high or low) Output is floating (i.e. open circuit) Incorrect gain on the output voltage (i.e. outside the expected range) Incorrect offset on the output voltage (i.e. outside the expected range) Incorrect output dynamic range (i.e. outside the expected range) Incorrect input dynamic range (i.e. outside the expected range) Output voltage accuracy too low, including drift[c] Output voltage affected by spikes[b] Output voltage oscillation[a] Settling time of the output voltage too low
Sample and hold	HW part/sub-part sampling the voltage of a continuously varying analogue input signal and holding its value at a constant level for a specified minimum period of time.	Output is stuck (i.e. high or low) Output is floating (i.e. open circuit) Incorrect sampling leading to gain/offset error on output voltage dependent on input signal Incorrect gain on the output voltage (i.e. outside the expected range) Incorrect offset on the output voltage (i.e. outside the expected range) Incorrect output dynamic range (i.e. outside the expected range) Incorrect input dynamic range (i.e. outside the expected range) Output voltage accuracy too low during hold phase, including drift[c] Output voltage during hold phase affected by spikes[b] Output voltage oscillation[a] during hold phase Output does not settle sufficiently accurate during hold time

© ISO 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO PAS 19451-1-2016 (2017)

Table 1 *(continued)*

Part/sub-part	Short description	Failure modes
Analogue multiplexer	HW part/sub-part consisting of multiple analogue input signals, multiple control inputs and one output signal.	Output is stuck (i.e. high or low) Output is floating (i.e. open circuit) Incorrect channel selection Offset affecting the output signal too high Resistive or capacitive coupling among input channels and output signal including crosstalk Resistive or capacitive coupling among selectors and output signal including crosstalk Incorrect output dynamic range (i.e. outside the expected range) Attenuation of the output signal Drift[c] affecting the output signal Spikes[b] affecting the output signal (i.e. during switching)
Analogue switch	HW part/sub-part capable of switching or routing analogue signals based on the level of a digital control signal. Commonly implemented using a "transmission gate".	Output is stuck (i.e. high or low) Output is floating (i.e. open circuit or tri-stated) Offset too high affecting the output signal Resistive or capacitive coupling between control signal and output signal including crosstalk Attenuation of the output signal Drift[c] affecting the output signal Spikes[b] affecting the output signal, e.g. during switching
Passive network	HW part/sub-part consisting of a network of passive devices (resistor and capacitor) providing a specific low pass transfer function	Output is stuck (i.e. high or low) Output is floating (i.e. open circuit) Incorrect output dynamic range (i.e. outside the expected range) Incorrect attenuation of the output signal (i.e. outside the expected range) Incorrect settling time (i.e. outside the expected range) Drift[c] affecting the output signal Oscillation[a] affecting the output signal (i.e. due to crosstalk, coupling or parasitic effects) Spikes[b] affecting the output (i.e. due to crosstalk, coupling or parasitic effects)

© ISO 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO PAS 19451-1-2016 (2017)

Table 1 *(continued)*

Part/sub-part	Short description	Failure modes
Voltage references	HW part/sub-part producing a constant DC (direct-current) output voltage regardless of variations in external conditions such as temperature, barometric pressure, humidity, current demand, or the passage of time.	Output is stuck (i.e. high or low) Output is floating (i.e. open circuit) Incorrect output voltage value (i.e. outside the expected range) Output voltage accuracy too low, including drift[c] Output voltage affected by spikes[b] Output voltage oscillation[a] within the expected range Incorrect start-up time (i.e. outside the expected range)
Current source (including bias current generator)	HW part/sub-part delivering or absorbing a current (i.e. reference current) which is independent of the voltage across it. It typically includes multiple branches which are routed to other circuits requiring a reference or bias current.	One or more outputs are stuck (i.e. high or low) One or more outputs are floating (i.e. open circuit) Incorrect reference current (i.e. outside the expected range) Reference current accuracy too low, including drift[c] Reference current affected by spikes[b] Reference current oscillation[a] within the expected range One or more branch currents outside the expected range while reference current is correct One or more branch currents accuracy too low, including drift[c] One or more branch currents affected by spikes[b] One or more branch currents oscillation[a] within the expected range

© ISO 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO PAS 19451-1-2016 (2017)

Table 1 *(continued)*

Part/sub-part	Short description	Failure modes
[a] An oscillation is an instability of the part/sub-part caused by internal failure, e.g. regulation loop failures, lower or negative hysteresis for a comparator, etc.. Oscillation includes any repetitive voltage and current variation (i.e. periodic pulse) [b] A spike is a non-repetitive variation on the output voltage or current, i.e. pulse due to load jumps, etc. [c] Drift is a slow and continuous variation of a parameter (i.e. current, voltage, threshold, etc.) outside the expected range reported into the circuit specification. Slow variation means slower as compared to the fault tolerant time interval (FTTI). For example drift covers floating or stuck at open failure modes. [d] Several of the failure modes reported for the ADC or DAC can be grouped into two main sets: static error and absolute accuracy (total) error Static errors are errors that affect the accuracy of a converter when it is converting static (DC) signals and can be completely described by four terms: — offset error; — gain error; — integral non-linearity; — differential non-linearity. Each term can be expressed in LSB units or sometimes as a percentage of the full scale range (FSR). For example, an error of 1/2 LSB for an 8-bit converter corresponds to 0,2 % FSR. The absolute accuracy (total) error is the maximum value of the difference between an analogue value and the ideal mid-step value. It includes offset, gain, and integral linearity errors, and also the quantization error in the case of an ADC.		

Given the variety of implementations and the lack of data available from the field and from theory, Table 1 does not give any indication about the quantitative impact of the listed failure modes, i.e. the failure mode distribution. It is the responsibility of the safety analyst to identify such quantitative data. An example is given in 5.3.3.

NOTE 1 Even though it is known that a single physical root cause can lead to more than one failure mode, it is a common simplification that the sum of the distribution of all failure modes is 100 %.

NOTE 2 Transient failure modes are considered if they are relevant, for example if for the technology in use the risk of single-event effects (SEE) is not negligible, see 5.2.3.

5.2.2 About safe faults

ISO 26262-10:2012, 8.1.7 states that safe faults can be faults of one of two categories:

— all n point faults with $n > 2$, unless the safety concept shows them to be a relevant contributor to a safety requirement, or

— faults that will not contribute to the violation of a safety requirement.

Analogue components are characterized by continuous (output) signal (function) regions and as such, tolerances shall be taken into consideration when used in systems. The tolerances on analogue functions as specified as part of the safety requirements allocated to that analogue component can be less constrained than the actual tolerance of the analogue component itself. For this reason, the fraction of the failure mode that leads to parametric failure or drift, but which remains within these tolerance ranges is safe. An analogue component has therefore an inherent capability to tolerate a fault. These faults are safe faults.

EXAMPLE 1 A resistor is used to limit the current flowing through a specific branch. A failure in the accuracy of the resistor increasing its value (e.g. of 50 %) but not preventing the current limiting function would be a safe fault.

© ISO 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO PAS 19451-1-2016 (2017)

A specific fault in an element can have a different classification depending on the specific safety requirement considered. For more details see ISO 26262-5.

Depending on the system configuration and the system safety requirements some failure modes are not relevant, i.e. they cannot violate the requirements. In this case, these failure modes can be classified as safe: They contribute to the safety metrics increasing the failure rate of safe faults

EXAMPLE 2 An output driver can have an output slope control to limit the rise and fall times of the output value for EMI purposes. If the slew rate is irrelevant for the violation of the safety goal, failures in this slope control would be safe faults.

EXAMPLE 3 If a voltage regulator is used to supply digital circuits only, failure modes affecting the stability and the accuracy of the output voltage within the OV/UV thresholds can be classified as safe.

5.2.3 About transient faults

As defined in ISO 26262-1:2011, definition 1.135, a transient fault is a fault that occurs once and subsequently disappears. Soft errors such as Single Event Upset (SEU) and Single Event Transient (SET) are defined as transient faults. ISO 26262-5:2011, 8.4.7 states that transient faults are considered when shown to be relevant due, for instance, to the technology used and can be addressed either by a quantitative approach, specifying and verifying a dedicated target “single-point fault metric” value to them or by a qualitative rationale based on the verification of the effectiveness of the internal safety mechanisms implemented to cover these transient faults.

In terrestrial analogue circuits, transient faults are caused by alpha-particle or neutron hits or by electromagnetic interference such as power transients and crosstalk. They can cause SEU or even SET also called Analogue Single Event Transients (ASETs), such as transient pulses in operational amplifiers, comparators or reference voltage circuits.

Due to the intrinsic nature of analogue technology (in which transient or noise effects are considered by design), the susceptibility to transient faults is lower than in digital circuits by orders of magnitude. Therefore, the analysis of those effects can be limited in a first approximation to their digital part (e.g. the digital decimation filter of a sigma-delta ADC).

However in some cases, like in the early part of the conversion cycle of an ADC (see reference[37]) or in PLL (see reference[28]) or differential switched-capacitor circuits (see reference[17]), the vulnerability to soft-error can be high. In those cases, more detailed analyses are done and appropriate countermeasures are identified (see reference[8]).

For mixed signal components, the impact of soft errors in the digital part is considered as described in ISO 26262-5. ISO 26262-10 can also be referred as a guideline.

NOTE If more detailed analyses are needed in the analogue part, since SER evaluation by irradiation tests in analogue circuits is not a simple task, in those cases measurement is done mainly by analytical.

5.3 Notes about safety analysis

5.3.1 General

The examples and guidelines given in ISO 26262-10:2012, Annex A are also valid for an analogue or mixed signal component. The following paragraphs describe some of the topics that can require additional clarification for an analogue or mixed signal component.

5.3.2 Level of granularity of analysis

One of the key aspects for the safety analysis of analogue elements is the proper identification of the level of hierarchy on which to base the analysis. On one hand, a lower level of granularity is beneficial as it allows for a better understanding of the failure modes and failure mode distributions. On the other, a higher level of granularity allows for a clear allocation of safety mechanisms. Analogue elements are

© ISO 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO PAS 19451-1-2016 (2017)

often used to interface with physical objects making it useful to also consider mechanical characteristics and differentiate the failure modes accordingly.

As seen in ISO 26262-9:2011, 8.2, qualitative and quantitative safety analyses are performed at the appropriate level of abstraction during the concept and product development phases. The level of abstraction can be consequently adjusted depending on the target of the analysis. Qualitative analysis is more suited to identify failure modes while quantitative analysis to quantify their failure rate and distribution.

Consider an example in which, a linear voltage regulator is monitored using a windowed voltage monitor. The voltage monitor is at the output of the regulator and is able to detect over-voltage conditions. If the output value, allowed in the working condition to fluctuate in a range around a nominal value, e.g. 1,2 V ± 0,12 V, moves outside that range it is to be considered faulty. If the analysis focuses on the output of the regulator it can be relatively easy to discriminate between types of failures (e.g. safe because within allowed range, over or under voltage) and quantify the protection offered by the voltage monitor. However it is difficult to quantify the likelihood of each type of failure as required for metric computation. If the analysis goes inside the regulator and focuses, for instance, on faults of the bandgap it is easier to analyse propagation and likelihood of each failure of the regulator but not simple to quantify the protection that the external voltage monitor offers on the bandgap itself.

For the safety analysis, the type of safety mechanisms can drive the selection of the level of abstraction. If the safety mechanisms addressing analogue features are located at system level, going down in the block structure can lead to an overly complex analysis. The quantification of the failure mode distribution can require an investigation on lower levels of abstraction. For instance, applying an equal distribution to the failure modes of the linear voltage regulator can give less accurate results than applying an equal distribution to the blocks composing the linear voltage regulator as, for instance, the bandgap, the buffer, the driver, etc. With respect to terminology, in line with the classification done for microcontroller in ISO 26262-10:2012, Annex A and according to ISO 26262-10:2012, Table D.1, the linear voltage regulator is to be considered a part and the bandgap, the buffer, the driver, etc. sub-parts.

5.3.3 Examples of usage of failure mode distributions

The failure distribution model is dependent on the circuit implementation and targeted process. Each supplier provides details on the failure mode distribution model used in the analysis.

EXAMPLE 1 A simple and pessimistic model can be used for the initial analysis, like considering only failure modes capable of violating a safety requirement (i.e. not a safe failure mode) and using a linear distribution for the defined failure modes; for instance if five failure modes are defined, each failure mode is allocated 20 % distribution.

NOTE 1 In the EXAMPLE 1 above, this analysis considers all the applicable failure modes except those not capable of violating the safety requirement. Safe failure modes are not included in the computation.

If the analysis using such failure mode distribution model does not fulfil the required Single Point Fault and/or Latent Fault metrics for the targeted ASIL level, the definition of the failure modes and related distribution is further refined.

EXAMPLE 2 Failure modes not capable of violating the safety requirement, i.e. safe failure modes, that are applicable to the circuit under analysis, are added in the computation with F_{safe} = 100 %

NOTE 2 The uniform failure mode distribution and the list of safe and not safe failure modes are considered in the FMEA example in 5.3.5.

EXAMPLE 3 A more detailed distribution for all failure modes can be considered based on area; if the area of the circuit or circuits identified as the root cause for the defined failure mode is 5 %, then the allocated failure mode distribution is 5 %.

Applicable failure modes and detailed failure mode distributions are justified according to the circuit implementation and its physical area and documented in the product safety case.

© ISO 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO PAS 19451-1-2016 (2017)

5.3.4 Example of failure rates estimation for an analogue part

Calculation methods to derive the base failure rate for analogue and mixed signal components are described in Clause 9.

The base failure rate is allocated to the different elements composing the hardware component. Different allocation methods can be applied depending on the type of elements considered.

The base failure rate can be considered proportional to the area of the circuit.

EXAMPLE 1 The base failure rate divided by the overall area of the component in order to obtain FIT/mm^2 for each relevant fault model as reported in Table 2.

Table 2 — Base failure rate allocation based on area

Fault model	Failure rate value	Unit
Permanent faults	2,00E-02	FIT/mm^2
Transient faults	2,00E-05	FIT/mm^2

The failure rate of each sub-part of the analogue and mixed signal component shown in Figure 2 is computed by using the FIT/mm^2 reported in Table 2.

The results of the computation, considering the block diagrams of Figure 2, Figure 3, and Figure 4 are reported in Table 3.

Table 3 — Failure rate for each part/sub-part

Part	Sub-part	Block Area mm^2	Failure rate Permanent faults FIT	Failure rate Transient faults FIT
Low Drop Regulator	**Regulator Core**	0,52	0,0104	0,0000104
	BANDGAP 1	0,15	0,0030	0,0000 030
	Bias Current Generator	0,01	0,0002	0,0000002
	Current Limiter	0,075	0,0015	0,0000015
	TOTAL	**0,755**	**0,0151**	**0,000 0151**
Voltage Monitor	**CMP1**	0,03	0,0006	0,0000006
	CMP2	0,03	0,0006	0,0000006
	Passive Network	0,08	0,0016	0,0000016
	BANDGAP 2	0,15	0,0030	0,0000030
	TOTAL	**0,29**	**0,0058**	**0,0000058**
ADC	**ADC**	0,85	0,0170	0,0000170
Analogue BIST	**Analogue BIST**	0,35	0,0070	0,0000070
	TOTAL	**2,535**	**0,0507**	**0,0000507**

NOTE 1 The numbers reported in Table 2 and Table 3 are only examples.

NOTE 2 Block area reported in Figure 3 includes internal routing. Routing at top level, if relevant, is included in a separate block.

In alternative to the area-based approach, as seen in ISO 26262-10:2012, A.3.3.1, the failure rate and failure mode distribution can be estimated based on the number of equivalent transistors for each sub-part or elementary part. In the case of mixed signal or analogue components, distinction between active devices, passive devices and routing can be taken into account in the estimation of the number of equivalent transistors. The selection of the method used can be based on the layout (or planned

© ISO 2016 – All rights reserved
Documents Document Sharing Hub
Full document details: ISO PAS 19451-1-2016 (2017)

layout) of the circuit under analysis or on the analysis of how failure modes are shared between the HW elements.

NOTE 3 For a transient fault model, the base failure rate proportional to area is a simplified example because, in reality, not all the elements in a mixed signal circuit have the probability of failure.

EXAMPLE 2 In switched-capacitor architectures, the capacitors holding the signal are more sensitive with respect to transient faults than other portions of the circuit because they are used as memory elements.

5.3.5 Example of safety metrics computation

The following is an example of a quantitative analysis using the method described in ISO 26262-10:2012, A.3.3 in order to calculate the single-point fault metric and the latent-fault metric for a given safety requirement allocated to the mixed signal HW element depicted in Figure 2.

The example consists of a mixed signal HW element composed of:

— a low drop voltage regulator (low drop voltage regulator in Figure 3) providing an output voltage within a prescribed range;

— a voltage monitor (voltage monitor in Figure 4) capable of detecting overvoltage (VA > OV_th) and under-voltage (VA < UV_th) on the LDO output by monitoring the regulated voltage VA and comparing it with two predefined thresholds; the predefined thresholds are generated from a reference voltage provided by an independent bandgap (bandgap2 in Figure 4) in order to ensure independence with respect to the voltage regulator;

— an analogue BIST controlled through the digital system (the digital controller is not depicted in the block diagram in Figure 2);

— an ADC channel.

The ASIL B safety requirement is: “The regulated voltage output does not go out of regulation, i.e. the regulated voltage VA is not outside the VA_UV-VA_OV range for more than 1ms.”

The component can be considered in a safe state when an out of regulation condition is detected and signalled to an external element of the system/item. The external system is responsible for fault reaction including transitioning the system to a safe state.

As shown in Figure 4, the voltage monitor is composed of two voltage comparators, a passive network and a bandgap; the low drop regulator includes a bandgap, a current limiter, the bias generator and the regulator core as shown in Figure 3.

The ADC is included in the mixed signal HW element but it is not used for any function related to the safety requirement and so its potential failure cannot contribute to the violation of such requirement; therefore the ADC is assumed not safety related.

NOTE 1 The example shows that parts which could be easily isolated and disabled in a way that they can be considered not safety-related without risk, can coexist with parts that are safety related.

© ISO 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO PAS 19451-1-2016 (2017)

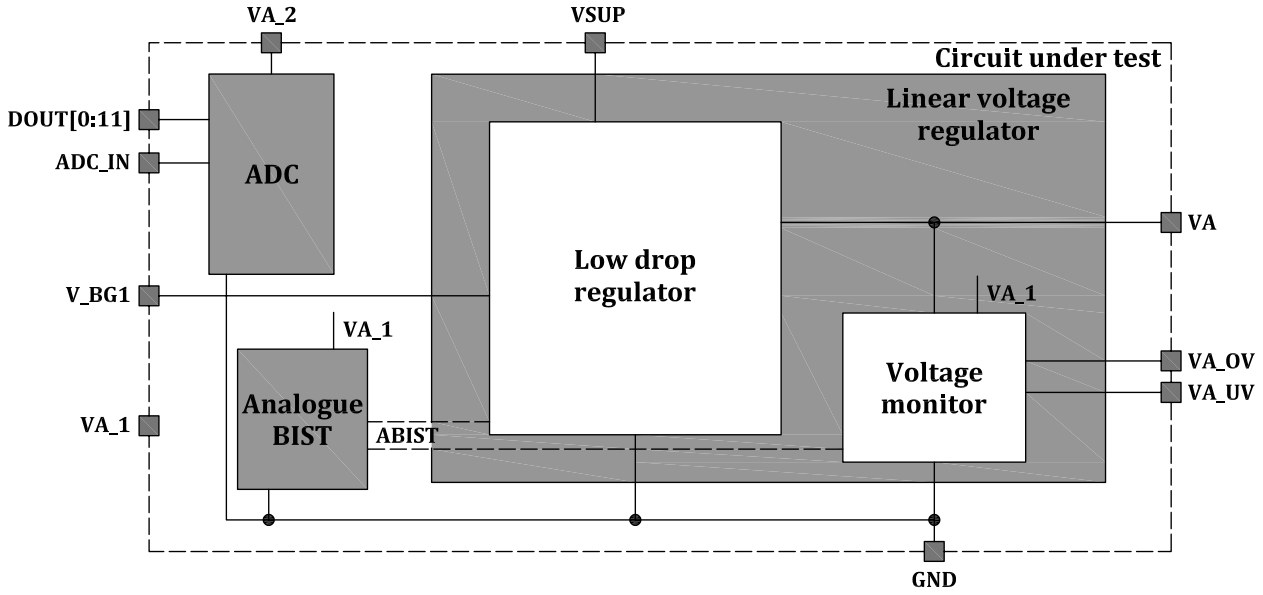

Figure 2 — Example of analogue and mixed signal HW element (circuit under analysis)

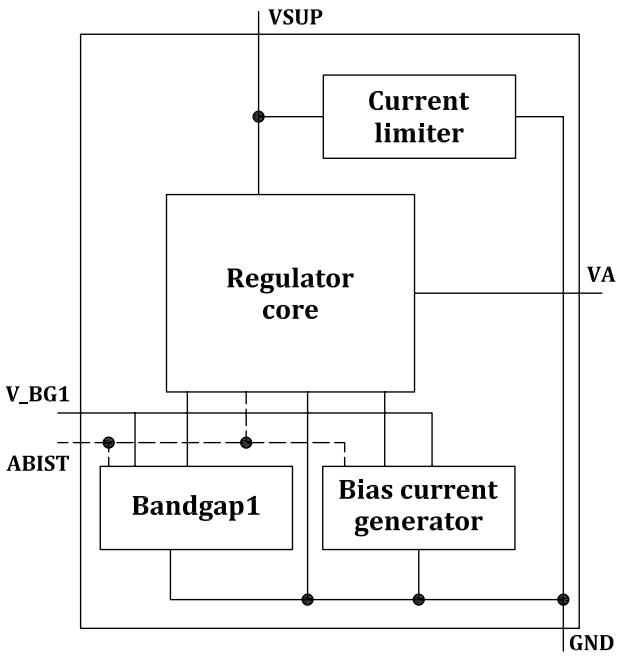

Figure 3 — Detailed block diagram of the low drop regulator part

© ISO 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO PAS 19451-1-2016 (2017)

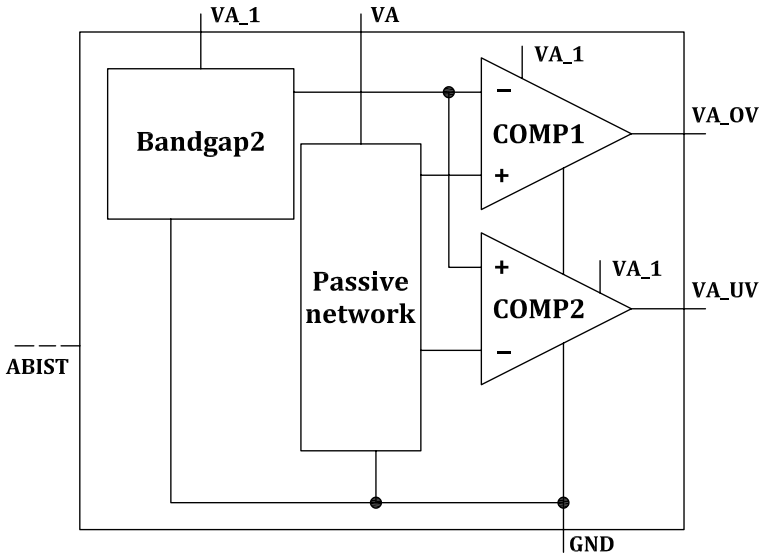

Figure 4 — Detailed block diagram of the voltage monitor part

The following safety mechanisms are considered:

— The voltage monitor detecting overvoltage (safety mechanism SM2) and under-voltage (safety mechanism SM1) failures with a diagnostic coverage of 99,9 %. The safety mechanism is described in 5.4.2.

— the analogue BIST detecting failures affecting the voltage monitor with a diagnostic coverage of 60 % (safety mechanism SM6). The safety mechanism is described in 5.4.10.

The coverage levels claimed by the safety mechanisms are reported in the following Table 4. They are assumed to be proven with simulations, testing to characterize and confirm the behaviour of the silicon and the related evidences are documented in the product safety case. It is out of the scope of this example to provide those evidences.

Each safety mechanism signals the detection of a fault to an element of the system/item which is then responsible to transition the system to a safe state.

Under this assumption, the failure mode coverage with respect to latent failures related to the low drop regulator is claimed to be 100 % based on the example in ISO 26262-5:2011, Annex E.

Table 4 — Safety mechanisms considered in the example and related coverage for HW element

ID	Safety mechanism	Claimed failure mode coverage
SM1	Under-voltage (UV) Monitor	99,9 %
SM2	Over-voltage (OV) Monitor	99,9 %
SM6	Analogue BIST diagnostics	60 %

NOTE 2 The effectiveness of safety mechanisms could be affected by dependent failures. Adequate measures are considered as described in 5.3.6.

Based on the guidelines provided in ISO 26262-10:2012, A.3.3.1, the failure rates and the metrics can be computed in the following way for analogue and mixed signal HW elements:

— First, the HW element is divided into parts or sub-parts;

NOTE 3 The validity of assumptions on the independence of identified parts is established during the dependent failure analysis.

© ISO 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO PAS 19451-1-2016 (2017)

NOTE 4 The necessary level of detail (e.g. if analysis at part level or sub-part level) can depend on the stage of the analysis and on the safety mechanisms.

— Second, the failure rates of each part or sub-part can be computed using one of the methods described in 5.3.4;

NOTE 5 In this example the failure rate distribution is assumed to be proportional to the area both for permanent and transient faults using the values reported in Table 2.

— For each part/sub-part the relevant failure modes are listed and a failure mode distribution is assigned to each of them;

The failure mode distribution in the examples of Table 5 and Table 6 is considered equally distributed over the failure modes belonging to each part/sub-part. This assumption is to be understood as reference only, valid for the specific examples.

— The evaluation is completed by classifying the faults into safe faults, residual faults, detected dual-point faults and latent dual-point faults;

— Finally, the failure mode coverage with respect to residual and latent faults of that part or sub-part is determined.

NOTE 6 Numbers used in this example (e.g. failure rates, amount of safe faults and failure mode coverage) can vary from architecture to architecture.

The example of quantitative analysis, limited to permanent faults, is reported in Table 5 and Table 6 using the same format of ISO 26262-10:2012, Table A.5. The quantitative analysis gives the view of failure modes at sub-part level.

NOTE 7 In this example a separate analysis with respect to transient faults is not reported but it can be added when relevant.

Depending on the system functions and safety requirements, different operating phases can be relevant and so additional failure modes can be considered.

EXAMPLE For systems that need to fulfil start-stop requirements, the regulator start phase can be safety relevant and the failure mode “Incorrect start-up time (i.e. outside the expected range) - Voltage ramp too fast” can be added.

© ISO 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO PAS 19451-1-2016 (2017)

Table 5 — Example of quantitative analysis – mission parts

Part	Sub-part	Safety Related Component or No Safety Related Component	Potential Effect of Failure Mode in Absence of Safety Mechanism (SM) on IC level[a]	Fault Model[b]	Failure distribution	Failure rate (FIT)	Amount of Safe Faults	Safety mechanism(s) preventing the violation of the safety requirement	Failure mode coverage with respect to violation of safety requirement	Residual or Single Point Fault failure rate/FIT	Safety mechanism(s) to prevent latent faults	Failure mode coverage with respect to Latent failures	Latent Multiple Point Fault failure rate/FIT
Low Drop Regulator	Low Drop Regulator	SR	Regulated voltage higher than VA_OV	P	14 %	2,16E-03	0 %	SM2	99,9 %	2,16E-06	SM2	100 %	0,0E+00
		SR	Regulated voltage lower than VA_UV	P	14 %	2,16E-03	0 %	SM1	99,9 %	2,16E-06	SM1	100 %	0,0E+00
		SR	Regulated voltage out of the expected range (VA_UV-VA_OV)	P	14 %	2,16E-03	0 %	SM1 SM2	99,9 %	2,16E-06	SM1 SM2	100 %	0,0E+00
		SR	No effect-Regulated voltage within the expected range but with low accuracy	P	14 %	2,16E-03	100 %			0,0E+00			0,0E+00
		SR	Regulated voltage out of the expected range (VA_UV-VA_OV)	P	14 %	2,16E-03	0 %	SM1 SM2	99,9 %	2,16E-06	SM1 SM2	100 %	0,0E+00
		SR	No effect-Regulated voltage within the expected range but with low accuracy	P	14 %	2,16E-03	100 %			0,0E+00			0,0E+00
		SR	no effect - assuming during the voltage regulator start up the item is in safe state	P	0 %	0,00E+00	100 %			0,00E+00			0,0E+00

© ISO 2016 – All rights reserved

Full document details: ISO PAS 19451-1:2016 (2017)
AVA Documents Document Sharing Hub

Table 5 *(continued)*

Part	Sub-part	Safety Related Component or No Safety Related Component	Potential Effect of Failure Mode in Absence of Safety Mechanism (SM) on IC level[a]	Fault Model[b]	Failure distribution	Failure rate (FIT)	Amount of Safe Faults	Safety mechanism(s) preventing the violation of the safety requirement	Failure mode coverage with respect to violation of safety requirement	Residual or Single Point Fault failure rate/FIT	Safety mechanism(s) to prevent latent faults	Failure mode coverage with respect to Latent failures	Latent Multiple Point Fault failure rate/FIT
		SR	no effect - assuming during the voltage regulator start up the item is in safe state	P	0 %	0,00E+00	100 %			0,00E+00			0,0E+00
		SR	Regulated voltage potentially with low accuracy or out of regulation depending on the actual quiescent current	P	14 %	2,16E-03	50 %			1,08E-03	SM1 SM2	100 %	0,0E+00
ADC	ADC	NSR		P	100 %	7,00E-03				0,0E+00			0,0E+00
						Σ					0,00109		
						Total failure rate	0,0221						
						Total Safety Related	0,0151						
						Total Not Safety Related	0,0070						
									Single Point Faults Metric		92,8 %		
											Latent Faults Metric		100 %

a Depending on complexity it can be beneficial to have a dedicated entry in the FMEA giving more details about the potential root causes and the end effect of each failure mode.

b Fault model can be permanent fault (P) or transient fault (T); the example is limited to permanent faults.

© ISO 2016 – All rights reserved

Full document details: ISO PAS 19451-1:2016 (2017)

AVA Documents Document Sharing Hub

Table 6 — Example of quantitative analysis – safety mechanisms

Part	Sub-part	Safety Related Component or No Safety Related Component	Failure Mode	Potential Effect of Failure Mode in Absence of Safety Mechanism (SM) on IC level[a]	Fault Model[b]	Failure distribution	Failure rate (FIT)	Amount of Safe Faults	Safety mechanism(s) preventing the violation of the safety requirement	Failure mode coverage with respect to violation of safety requirement	Residual or Single Point Fault failure rate/FIT	Safety mechanism(s) to prevent latent faults	Failure mode coverage with respect to Latent failures	Latent Multiple Point Fault failure rate/FIT
Voltage Monitor (SM1, SM2)	Voltage Monitor (SM1, SM2)	SR	UV Monitor (SM1) falsely triggering UV event	Nuisance shutdown at nominal regulator loads	P	25 %	1,45E-03	100 %						0,0E+00
		SR	UV Monitor (SM1) not triggering valid UV event	Regulated voltage lower than VA_UV	P	25 %	1,45E-03	0 %				SM6	60 %	5,80E-04
		SR	OV Monitor (SM2) falsely triggering OV event	Nuisance shutdown at nominal regulator loads.	P	25%	1,45E-03	100%						0,0E+00

© ISO 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO PAS 19451-1-2016 (2017)

Table 6 *(continued)*

Part	Sub-part	Safety Related Component or No Safety Related Component	Failure Mode	Potential Effect of Failure Mode in Absence of Safety Mechanism (SM) on IC level[a]	Fault Model[b]	Failure distribution	Failure rate (FIT)	Amount of Safe Faults	Safety mechanism(s) preventing the violation of the safety requirement	Failure mode coverage with respect to violation of safety requirement	Residual or Single Point Fault failure rate/FIT	Safety mechanism(s) to prevent latent faults	Failure mode coverage with respect to Latent failures	Latent Multiple Point Fault failure rate/FIT
		SR	OV Monitor (SM2) not triggering valid OV event	Regulated voltage higher than VA_OV	P	25%	1,45E-03	0%				SM6	60%	5,80E-04
Analog BIST	Analog BIST (SM6)	SR	Analogue BIST (SM6) falsely detects misbehaviour of the linear voltage regulator	No effect[c]	P	50%	3,50E-03	100%						0,0E+00
		SR	Analogue BIST (SM6) does not detect misbehaviour of the linear voltage regulator	No effect[c]	P	50%	3,50E-03	100%						0,0E+00
						Σ					0,00109			1.16E-03
						Total failure rate	0,01280							
						Total Safety Related	0,01280							
						Total Not Safety Related	0,00000							
										Single Point Faults Metric	100%			
												Latent Faults Metric	90.0%	

a Depending on complexity it can be beneficial to have a dedicated entry in the FMEA giving more details about the potential root causes and the end effect of each failure mode.

b Fault model can be permanent fault (P) or transient fault (T); the example is limited to permanent faults.

c It requires more than two faults before it becomes safety relevant: #1 fault: Failure on main safety mechanism (SM1, SM2 or SM3), #2 fault: LDO out of regulation, #3 fault: BIST Diagnostic failure.

© ISO 2016 – All rights reserved

Full document details: ISO PAS 19451-1-2016 (2017)

AVA Documents Document Sharing Hub

Combining together the results of Table 5 and Table 6, the overall values are:

— Single Point Faults Metric = 96,1 %;

— Latent Faults Metric = 95,7 %.

The following example considers the same HW element reported in Figure 2 but a different safety requirement: "The accuracy and the stability of the regulated voltage is such that VA < VA0 + Δ and VA > VA0-Δ where VA0 is within V_{min} – V_{max} and Δ = 5mV."

The component can be considered in a safe state when the low accuracy/stability condition is detected and signalled to an external element of the system/item. The external system is responsible for fault reaction including transitioning the system to a safe state.

The example of quantitative analysis limited to permanent faults is reported in Table 8 using the same format of ISO 26262-10:2012, Table A.5. The safety mechanisms considered in the analysis are:

— The voltage monitor (voltage monitor in Figure 4) detecting overvoltage (safety mechanism SM2) and under-voltage (safety mechanism SM1) failures.

— The independent ADC channel detecting variation of the regulated voltage higher than Δ = 5mV (safety mechanism SM3). The safety mechanism is described in 5.4.11.

— A current limiter detecting failures affecting circuits supplied by the low drop voltage (safety mechanism SM5). The safety mechanism is described in 5.4.5.

— An analogue BIST detecting failures affecting the voltage monitor.

NOTE 8 The independence of the current limiter with respect to the regulator core will be evaluated in the safety analysis.

NOTE 9 The ADC used as safety mechanism SM3 is assumed to be external to the HW element under analysis and so it is not considered in the FMEA. There is an ADC included in the HW element which is not SM3: It is therefore reported in the FMEA as not safety related.

The coverage levels claimed by the safety mechanisms are reported in the following Table 7.

Table 7 — Safety mechanisms considered in the example with the new safety requirement

ID	Safety mechanism	Claimed failure mode coverage
SM1	Under-voltage (UV) Monitor	99,9 %
SM2	Over-voltage (OV) Monitor	99,9 %
SM3	Independent ADC monitoring	97 %
SM5	Current limiter	98 %
SM6	Analogue BIST diagnostics	90 %

NOTE 10 The effectiveness of safety mechanisms could be affected by dependent failures. Adequate measures are considered as described in 5.3.6.

Moreover, each safety mechanism signals the detection of a fault to an external element of the system/item which is then responsible to transition the system to a safe state.

Under this assumption, the failure mode coverage with respect to latent failures related to the mission circuit is claimed to be 100 % according to ISO 26262-5:2011, Annex E.

Table 8 shows the quantitative analysis for the mission part conducted at a finer level of granularity than the one in Table 5 and Table 6. The examples show that a different safety requirement impacts the level of partitioning and the diagnostic coverage requirement for one or more safety mechanisms.

NOTE 11 In this example the analysis with respect to transient faults is not reported but it can be added when relevant.

© ISO 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO PAS 19451-1-2016 (2017)

Table 8 — Example of quantitative analysis in case of fine granularity – mission parts

Part	Sub-part	Safety Related Component or No Safety Related Component	Failure Mode	Potential Effect of Failure Mode in Absence of Safety Mechanism (SM) on IC level[a]	Fault Model[b]	Failure distribution	Failure rate (FIT)	Amount of Safe Faults	Safety mechanism(s) preventing the violation of the safety requirement	Failure mode coverage with respect to violation of safety requirement	Residual or Single Point Fault failure rate/ FIT	Safety mechanism(s) to prevent latent faults	Failure mode coverage with respect to Latent failures	Latent Multiple Point Fault failure rate/FIT
Linear voltage regulator	Regulator core	SR	Output voltage higher than a predefined high threshold of the prescribed range (i.e. Over voltage – OV)	Regulated voltage higher than VA_OV	P	14 %	1,49E-03	0 %	SM2	99,9 %	1,49E-06	SM2	100 %	0,00E+00
		SR	Output voltage lower than a predefined low threshold of the prescribed range (i.e. Under voltage – UV)	Regulated voltage lower than VA_UV	P	14%	1,49E-03	0%	SM1	99,9%	1,49E-06	SM1	100%	0,00E+00
		SR	Output voltage affected by spikes	Regulated voltage out of the expected range (VA_UV-VA_OV)	P	14%	1,49E-03	0%	SM1 SM2	99,9%	1,49E-06	SM1 SM2	100%	0,00E+00
		SR	Output voltage oscillation within the prescribed range	Regulated voltage within the expected range but with low accuracy	P	14%	1,49E-03	0%	SM3	97,0%	4,46E-05	SM3	100%	0,00E+00
		SR	Output voltage fast oscillation outside the prescribed range but with average value within the prescribed range	Regulated voltage within the expected range but with low accuracy	P	14%	1,49E-03	0%	SM1 SM2	99,9%	1,49E-06	SM1 SM2	100%	0,00E+00

© ISO 2016 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO PAS 19451-1:2016 (2017)

Table 8 *(continued)*

Part	Sub-part	Safety Related Component or No Safety Related Component	Failure Mode	Potential Effect of Failure Mode in Absence of Safety Mechanism (SM) on IC level[a]	Fault Model[b]	Failure distribution	Failure rate (FIT)	Amount of Safe Faults	Safety mechanism(s) preventing the violation of the safety requirement	Failure mode coverage with respect to violation of safety requirement	Residual or Single Point Fault failure rate/FIT	Safety mechanism(s) to prevent latent faults	Failure mode coverage with respect to Latent failures	Latent Multiple Point Fault failure rate/FIT
Linear voltage regulator	Regulator core	SR	Output voltage drift within the prescribed range	Regulated voltage within the expected range but with low accuracy	P	14%	1,49E-03	0%	SM3	97,0%	4,46E-05	SM3	100%	0,00E+00
	Bandgap 1	SR	Quiescent current (i.e. current drawn by the regulator in order to control its internal circuitry for proper operation) exceeding the maximum value	Regulated voltage potentially with low accuracy depending on the actual quiescent current	P	14%	1,49E-03	50%	SM3	97,0%	2,23E-05	SM3	100%	0,00E+00
		SR	Output is stuck (high or low)	Regulated voltage out of the expected range (VA_UV-VA_OV)	P	20%	6,00E-04	0%	SM1 SM2	99,9%	6,00E-07	SM1 SM2	100%	0,00E+00
		SR	Output is floating (e.g. open circuit)	Regulated voltage out of the expected range (VA_UV-VA_OV)	P	20%	6,00E-04	0%	SM1 SM2	99,9%	6,00E-07	SM1 SM2	100%	0,00E+00
		SR	Output voltage oscillation within the expected range	Regulated voltage within the expected range but with low accuracy	P	20%	6,00E-04	0%	SM3	97,0%	1,80E-05	SM3	100%	0,00E+00

© ISO 2016 – All rights reserved

Full document details: ISO PAS 19451-1:2016 (2017)

AVA Documents Document Sharing Hub

Table 8 *(continued)*

Part	Sub-part	Safety Related Component or No Safety Related Component	Failure Mode	Potential Effect of Failure Mode in Absence of Safety Mechanism (SM) on IC level[a]	Fault Model[b]	Failure distribution	Failure rate (FIT)	Amount of Safe Faults	Safety mechanism(s) preventing the violation of the safety requirement	Failure mode coverage with respect to violation of safety requirement	Residual or Single Point Fault failure rate/FIT	Safety mechanism(s) to prevent latent faults	Failure mode coverage with respect to Latent failures	Latent Multiple Point Fault failure rate/FIT
Linear voltage regulator	Bandgap 1	SR	Incorrect output voltage value (i.e. outside the expected range)	Regulated voltage out of the expected range (VA_UV-VA_OV)	P	20%	6,00E-04	0%	SM1 SM2	99,9%	6,00E-07	SM1 SM2	100%	0,00E+00
		SR	Output voltage accuracy too low, including drift	Regulated voltage within the expected range but with low accuracy	P	20%	6,00E-04	50%	SM3	97,0%	9,00E-06	SM3	100%	0,00E+00
		SR	Output voltage affected by spikes	Not applicable due to circuit implementation	P	0%	0,00E+00	0%			0,00E+00	SM1 SM2	100%	0,00E+00
	Bias current generator	SR	One or more outputs are stuck (high or low)	Regulated voltage out of the expected range (VA_UV-VA_OV)	P	10%	2,00E-05	0%	SM1 SM2	99,9%	2,00E-08	SM1 SM2	100%	0,00E+00
		SR	One or more outputs are floating (e.g. open circuit)	Regulated voltage out of the expected range (VA_UV-VA_OV)	P	10%	2,00E-05	0%	SM1 SM2	99,9%	2,00E-08	SM1 SM2	100%	0,00E+00
		SR	Incorrect reference current (i.e. outside the expected range)	Regulated voltage out of the expected range (VA_UV-VA_OV)	P	10%	2,00E-05	0%	SM1 SM2	99,9%	2,00E-08	SM1 SM2	100%	0,00E+00

© ISO 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO PAS 19451-1-2016 (2017)

Table 8 *(continued)*

Part	Sub-part	Safety Related Component or No Safety Related Component	Failure Mode	Potential Effect of Failure Mode in Absence of Safety Mechanism (SM) on IC level[a]	Fault Model[b]	Failure distribution	Failure rate (FIT)	Amount of Safe Faults	Safety mechanism(s) preventing the violation of the safety requirement	Failure mode coverage with respect to violation of safety requirement	Residual or Single Point Fault failure rate/ FIT	Safety mechanism(s) to prevent latent faults	Failure mode coverage with respect to Latent failures	Latent Multiple Point Fault failure rate/FIT
Linear voltage regulator	Bias current generator	SR	Reference current accuracy too low , including drift	Regulated voltage within the expected range but with low accuracy	P	10%	2,00E-05	0%	SM3	97,0%	6,00E-07	SM3	100%	0,00E+00
		SR	Reference current affected by spikes	Regulated voltage with low accuracy for a limited time period if the spike is not filtered out; No effect otherwise	P	10%	2,00E-05	50%			1,00E-05	SM1 SM2	100%	0,00E+00
		SR	Reference current oscillation within the expected range	Regulated voltage within the expected range but with low accuracy	P	10%	2,00E-05	0%	SM3	97,0%	6,00E-07	SM3	100%	0,00E+00
		SR	One or more bias currents outside the expected range while reference current is correct	Regulated voltage with low accuracy or out of regulation	P	10%	2,00E-05	0%	SM3	97,0%	6,00E-07	SM3	100%	0,00E+00
		SR	One or more bias currents accuracy too low , including drift	Regulated voltage within the expected range but with low accuracy	P	10%	2,00E-05	0%	SM3	97,0%	6,00E-07	SM3	100%	0,00E+00

© ISO 2016 – All rights reserved

Full document details: ISO PAS 19451-1:2016 (2017)

Table 8 *(continued)*

Part	Sub-part	Safety Related Component or No Safety Related Component	Failure Mode	Potential Effect of Failure Mode in Absence of Safety Mechanism (SM) on IC level[a]	Fault Model[b]	Failure distribution	Failure rate (FIT)	Amount of Safe Faults	Safety mechanism(s) preventing the violation of the safety requirement	Failure mode coverage with respect to violation of safety requirement	Residual or Single Point Fault failure rate/FIT	Safety mechanism(s) to prevent latent faults	Failure mode coverage with respect to Latent failures	Latent Multiple Point Fault failure rate/FIT
Linear voltage regulator	Bias current generator	SR	One or more bias currents affected by spikes	Regulated voltage with low accuracy for a limited time period if the spike is not filtered out; No effect otherwise	P	10%	2,00E-05	50%			1,00E-05	SM1 SM2	100%	0,00E+00
		SR	One or more bias currents oscillation within the expected range	Regulated voltage within the expected range but with low accuracy	P	10%	2,00E-05	0%	SM3	97,0%	6,00E-07	SM3	100%	0,00E+00
ADC	ADC	NSR			P	100%	7,00E-03				0,0E+00			0,0E+00
						Σ					0,00017			0,0E+00
						Total failure rate	0,0206							
						Total Safety Related	0,0136							
						Total Not Safety Related	0,0070							
										Single Point Faults Metric	98,8%			
												Latent Faults Metric		100%

[a] Depending on complexity it can be beneficial to have a dedicated entry in the FMEA giving more details about the potential root causes and the end effect of each failure mode.

[b] Fault model can be permanent fault (P) or transient fault (T); the example is limited to permanent faults.

© ISO 2016 – All rights reserved

Documents Document Sharing Hub

Full document details: ISO PAS 19451-1:2016 (2017)

5.3.6 Dependent failures analysis

As stated in ISO 26262-9:2011, 7.4.2, the analysis of dependent failures is performed on a qualitative basis because no general and sufficiently reliable method exists for quantifying such failures.

The steps reported in Clause 10 are applicable also for analogue and mixed signal components. In the dependent failures analysis, there are aspects that can be clearly considered when addressing analogue components, parts or sub-parts.

Analogue circuits are by nature sensitive to noise and interference among different blocks or functions. For this reason, structures to guarantee sufficient independence by means of isolation and separation (e.g. by implementing barriers and/or guard-rings or placing circuits at certain distances or separating the power supply distribution and even the ground layer) are implemented for functional reasons. In fact, substrate, power supply and global signals like bias, clock or reset are often considered as a source of interference and special care is taken to reduce such effect. This good design practice, usually followed for functional reasons, provides benefits in terms of dependent failure avoidance.

Analogue circuits can be very sensitive to process variation resulting in mismatches in the device behaviour. To ensure the "same" transfer function of two blocks, as in the case of redundant parts, the symmetry of the design and physical layout is a key factor. In such cases, special attention is taken to ensure exactly the same layout of the two blocks including orientation, symmetrical placing, routing etc.; therefore diversity is not always a viable solution to improve the common cause failure avoidance for analogue circuits.

As a consequence of these aspects, the dependent failure initiators are often addressed by techniques ensuring isolation or separation instead of with techniques aiming to differentiate their effects.

In other cases, diversity can still be a valid technique to achieve the detection or avoidance of dependent failures. For instance, in a dual channel approach, using two diverse ADC architectures (e.g. successive approximation ADC and sigma delta ADC) can reduce significantly the probability of common cause failures.

5.3.7 Verification of architectural metrics computation

This subclause is addressing a specific part of the safety analysis verification: the verification of the architectural safety metrics and in particular the fraction of safe faults and the failure mode coverage as defined in ISO 26262-10:2012, 8.1.

Possible approaches include:

— Expert judgment founded on an engineering approach given that any data, either qualitative or quantitative, is supported by rationale and relevant arguments included in the safety case.

NOTE 1 In some cases, such arguments can be derived from the functional characterization of the HW elements responsible for the claimed parameters. The aim of the functional characterization is the systematic failure avoidance and not the HW random failure but, in some cases, it can be used as evidence to prove the level of coverage with respect to a specific failure mode: This is the case in which the aim of a safety mechanism is to detect 100 % of one of more failure modes and this capability is guaranteed by design.

EXAMPLE 1 A voltage monitor is a typical safety mechanism used to detect overvoltage and under-voltage failure modes affecting the voltage regulator. If, during the HW design verification, the functional characterization of the voltage monitor shows that:

— any event leading to a regulated voltage outside the expected range defined in the specification for enough time to make the supplied HW circuit malfunction is detected by the voltage monitor; and

— any event leading to a variation of the regulated voltage inside the range defined in the specification for any time does not prevent the correct behaviour of the HW circuit supplied by the regulator;

© ISO 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO PAS 19451-1-2016 (2017)

then such characterizations can be used as arguments to claim a detection equal to 100 % of the mentioned failure modes.

— As mentioned in ISO 26262-5:2011, Table 11 and ISO 26262-10:2012, A.3.8.2, fault injection simulation during the development phase is a valid method to verify completeness and correctness of safety mechanism implementation with respect to hardware safety requirements and fault injection using design models can be successfully used to assist the verification. This method can be applied to analogue and mixed signal components.

NOTE 2 The fault injection campaign can be limited to a subset of faults or failures that are judged to be critical in a specific case. The most critical failure modes are identified taking into account their distribution, their claimed amount of safe faults, their claimed level of detection and the safety mechanisms or safety requirements responsible for those levels.

EXAMPLE 2 A failure mode is deemed too complex for expert judgement. This specific failure mode is a candidate to be characterized using fault injection.

— A combination of both methods, i.e. fault injection which supports expert judgment by providing arguments and evidence for the cases judged more critical and/or addressable by fault injection method alone.

5.4 Examples of safety mechanisms

The following tables give a non-exhaustive list of examples of commonly used analogue safety mechanisms and complement the information contained in ISO 26262-5:2011, Annex D.

Some analogue safety mechanisms have a digital output signal which is used to control the reaction to a failure and bring the component to a safe state. In many cases, this information is stored so that it can be communicated through a digital interface. Other analogue safety mechanisms control or suppress a fault from resulting in the violation of a safety requirement and do not interface with the digital domain.

To comply with ISO 26262-5:2011, 8.4.8, the safety mechanisms described in the following tables can require additional measures to detect faults affecting them that, as dual point faults, can lead to the violation of the safety goal.

The examples included in the following tables are not exhaustive and other techniques can be used.

Table 9 — Power supply

Safety mechanism/ measure	See overview of techniques	Notes
Over and under voltage monitoring	5.4.2	Typically an analogue circuit with an output latched in a digital core.
Voltage clamp (limiter)	5.4.3	Typically used to suppress voltage transients or spikes.
Over-current monitoring	5.4.4	Typically an analogue circuit with an output latched in digital core.
Current limiting	5.4.5	Typically an analogue circuit with feedback to an analogue control loop (e.g. to disable regulator main pass element).
Power on reset	5.4.6	Functional block which keeps the circuit in a known initialized state until power supply rails and/or the clock signal are stable.

© ISO 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO PAS 19451-1-2016 (2017)

Table 10 — Analogue I/O

Safety mechanism/ measure	See overview of techniques	Notes
Resistive pull up/down	5.4.1	Typically used on input signals to avoid floating conditions due to pin failure or external pin interconnect failure.
Filter	5.4.8	Analogue or digital circuit, typically used to suppress high frequency signal variation, like an output from analogue over and under voltage monitoring circuit.

Table 11 — Component

Safety mechanism/ measure	See overview of techniques	Notes
Analogue watchdog	5.4.7	
Thermal monitor	5.4.9	Typically an analogue circuit with an output latched in digital core, or feedback to an analogue circuit control loop (e.g. to disable affected circuit).
ADC monitoring	5.4.11	An analogue circuit typically controlled and evaluated by a digital circuit.
Analogue BIST	5.4.10	Typically an analogue circuit controlled by a digital circuit that verifies correct functionality of analogue safety mechanisms like under/over voltage monitoring, current limit protection and thermal protection circuits.

Table 12 — Analogue to digital converter

Safety mechanism/ measure	See overview of techniques	Notes
ADC attenuation detection	5.4.12	Typically an analogue circuit controlled by a digital circuit that validates the ADC conversion path by measuring a known and stable signal value.
Stuck on ADC channel detection	5.4.13	Typically an analogue circuit controlled by a digital circuit that validates the ADC conversion path by measuring a known and stable signal value.

5.4.1 Resistive pull up/down

Aim: To define a default voltage for a circuit node.

Description: A resistor is connected from a circuit node to either a supply voltage or ground to define a default voltage in the event that the driving signal becomes disconnected/high impedance. Commonly used on I/O pins.

EXAMPLE An un-driven or disconnected device/module input pin would be at an unknown voltage level. A pull-up resistor to the I/O supply voltage (or module supply voltage) or pull-down resistor to ground is used to keep the input at a known voltage level. The circuit itself could be a passive resistor or an active circuit like a current mirror.

5.4.2 Over and under voltage monitoring

Aim: To detect, as early as possible, when a regulated voltage is outside the specified range.

© ISO 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO PAS 19451-1-2016 (2017)

Description: The regulated voltage is compared via a differential input pair to a low and/or a high analogue reference voltage representing the limits of the specified operating range. The monitor output will change state when the regulated voltage is outside of the defined voltage window indicating a fault.

EXAMPLE A window comparator is used to monitor the output of a LDO regulator with reference voltages set to the minimum and maximum specified voltage levels in regulation.

5.4.3 Voltage clamp (limiter)

Aim: To prevent the voltage of a circuit node from exceeding the maximum voltage that can be safely supported.

Description: A voltage clamp limits the positive and/or negative voltage of a circuit node to an acceptable level determined by system and/or device process capability. Voltage clamps can be biased or unbiased. Unbiased clamps typically use Zener diodes to define the reference voltage while biased clamps use a voltage source in combination with specialized diodes (Zener, Schottky) to define the acceptable voltage level. Voltage clamps are typically used to protect against transient events.

EXAMPLE An ESD protection circuit is a specialized voltage clamp typically implemented on I/O pins. It is designed to shunt the energy of a high voltage electrostatic discharge on the I/O pins away from the internal circuitry to ensure that internal circuitry is not exposed to excessive voltage levels during the ESD event.

5.4.4 Over-current monitoring

Aim: To detect, as early as possible, when the output current exceeds a certain value.

Description: The implementation of over-current monitoring can vary. A typical approach for a voltage regulator circuit with an MOS output device is to add a sense FET in parallel with a regulator main FET. The sense FET current, which is proportional to the main FET current, flows across a sense resistor. The voltage drop across the sense resistor is amplified and monitored by a voltage monitor.

NOTE The output of an over-current monitor is a digital output which is subsequently used as feedback to an analogue circuit control loop, and/or latched in a digital core which interfaces to the control and/or status monitoring circuits.

5.4.5 Current limiter

Aim: To limit output current to a maximum level in order to maintain a safe operating area of the output device and prevent electrical overstress.

Description: A closed loop system using negative feedback from a current monitor to reduce the drive to the output device thereby limiting the output current.

5.4.6 Power on reset

Aim: To hold the outputs of a system in a known state (typically off) until internal nodes have stabilized upon power up or power reset conditions.

Description: Typically, a bandgap-derived voltage reference is compared to an attenuated supply voltage in order to detect the minimum specified supply voltage which will ensure correct operation. Hysteresis is typically required to prevent oscillation as the attenuated supply voltage exceeds the reference voltage.

EXAMPLE An under-voltage monitor is a mechanism used to detect and drive power-on reset.

5.4.7 Analogue watchdog

Aim: To monitor proper operation of an oscillator.

© ISO 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO PAS 19451-1-2016 (2017)