

ISO 26262-11:2018-12 (E)

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

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

5.1.1	About digital components	60
5.1.2	Fault models of non-memory digital components	60
5.1.3	Detailed fault models of memories	61
5.1.4	Failure modes of digital components	62
5.1.5	Example of failure mode definitions for common digital blocks	62
5.1.6	Qualitative and quantitative analysis of digital component	66
5.1.7	Notes on quantitative analysis of digital components	67
5.1.8	Example of quantitative analysis	69
5.1.9	Example of techniques or measures to detect or avoid systematic failures during design of a digital component	70
5.1.10	Verification using fault injection simulation	74
5.1.11	Example of safety documentation for a digital component	75
5.1.12	Examples of safety mechanisms for digital components and memories	76
5.1.13	Overview of techniques for digital components and memories	77
5.2	Analogue/mixed signal components	80
5.2.1	About analogue and mixed signal components	80
5.2.2	Analogue and mixed signal components and failure modes	82
5.2.3	Notes about safety analysis	91
5.2.4	Examples of safety mechanisms	94
5.2.5	Avoidance of systematic faults during the development phase	97
5.2.6	Example of safety documentation for an analogue/mixed-signal component	100
5.3	Programmable logic devices	101
5.3.1	About programmable logic devices	101
5.3.2	Failure modes of PLD	105
5.3.3	Notes on safety analyses for PLDs	106
5.3.4	Examples of safety mechanisms for PLD	112
5.3.5	Avoidance of systematic faults for PLD	113
5.3.6	Example of safety documentation for a PLD	116
5.3.7	Example of safety analysis for PLD	116
5.4	Multi-core components	116
5.4.1	Types of multi-core components	116
5.5	Sensors and transducers	119
5.5.1	Terminology of sensors and transducers	119
5.5.2	Sensors and transducers failure modes	120
5.5.3	Safety analysis for sensors and transducers	125
5.5.4	Examples of safety measures for sensors and transducers	126
5.5.5	About avoidance of systematic faults for sensors and transducers	130
5.5.6	Example of safety documentation for sensors and transducers	131
Annex A (informative)	Example on how to use digital failure modes for diagnostic coverage evaluation	132
Annex B (informative)	Examples of dependent failure analysis	136
Annex C (informative)	Examples of quantitative analysis for a digital component	150
Annex D (informative)	Examples of quantitative analysis for analogue component	155
Annex E (informative)	Examples of quantitative analysis for PLD component	169
Bibliography	175