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

Véhicules routiers — Sécurité fonctionnelle —
Partie 11: Lignes directrices sur l'application de l'ISO 26262 aux semi-conducteurs
Contents

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
5.18 Example of quantitative analysis ................................................................. 69
5.19 Example of techniques or measures to detect or avoid systematic failures
during design of a digital component .......................................................... 70
5.10 Verification using fault injection simulation ........................................... 74
5.11 Example of safety documentation for a digital component .................... 75
5.12 Examples of safety mechanisms for digital components and memories ........ 76
5.13 Overview of techniques for digital components and memories ................ 77

5.2 Analogue/mixed signal components .......................................................... 80
5.2.1 About analogue and mixed signal components ....................................... 80
5.2.2 Analogue and mixed signal components and failure modes .................. 82
5.2.3 Notes about safety analysis ................................................................. 91
5.2.4 Examples of safety mechanisms ........................................................... 94
5.2.5 Avoidance of systematic faults during the development phase .............. 97
5.2.6 Example of safety documentation for an analogue/mixed-signal component 100

5.3 Programmable logic devices .................................................................. 101
5.3.1 About programmable logic devices ..................................................... 101
5.3.2 Failure modes of PLD ......................................................................... 105
5.3.3 Notes on safety analyses for PLDs ....................................................... 106
5.3.4 Examples of safety mechanisms for PLD .............................................. 112
5.3.5 Avoidance of systematic faults for PLD .............................................. 113
5.3.6 Example of safety documentation for a PLD ...................................... 116
5.3.7 Example of safety analysis for PLD ................................................... 116

5.4 Multi-core components ........................................................................ 116
5.4.1 Types of multi-core components .......................................................... 116
5.4.2 Implications of ISO 26262 series of standards for multi-core components 117

5.5 Sensors and transducers ...................................................................... 119
5.5.1 Terminology of sensors and transducers ............................................ 119
5.5.2 Sensors and transducers failure modes .............................................. 120
5.5.3 Safety analysis for sensors and transducers ....................................... 125
5.5.4 Examples of safety measures for sensors and transducers .................... 126
5.5.5 About avoidance of systematic faults for sensors and transducers .......... 130
5.5.6 Example of safety documentation for sensors and transducers ............. 131

Annex A (informative) Example on how to use digital failure modes for diagnostic coverage evaluation ................................................................. 132

Annex B (informative) Examples of dependent failure analysis ....................... 136

Annex C (informative) Examples of quantitative analysis for a digital component 150

Annex D (informative) Examples of quantitative analysis for analogue component 155

Annex E (informative) Examples of quantitative analysis for PLD component ........ 169

Bibliography ............................................................................................... 175
Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO’s adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 22 Road vehicles Subcommittee SC 32 Electrical and electronic components and general system aspects.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

A list of all parts in the ISO 26262 series can be found on the ISO website.
Introduction

The ISO 26262 series of standards is the adaptation of IEC 61508 series of standards to address the sector specific needs of electrical and/or electronic (E/E) systems within road vehicles.

This adaptation applies to all activities during the safety lifecycle of safety-related systems comprised of electrical, electronic and software components.

Safety is one of the key issues in the development of road vehicles. Development and integration of automotive functionalities strengthen the need for functional safety and the need to provide evidence that functional safety objectives are satisfied.

With the trend of increasing technological complexity, software content and mechatronic implementation, there are increasing risks from systematic failures and random hardware failures, these being considered within the scope of functional safety. ISO 26262 series of standards includes guidance to mitigate these risks by providing appropriate requirements and processes.

To achieve functional safety, the ISO 26262 series of standards:

a) provides a reference for the automotive safety lifecycle and supports the tailoring of the activities to be performed during the lifecycle phases, i.e., development, production, operation, service and decommissioning;

b) provides an automotive-specific risk-based approach to determine integrity levels [Automotive Safety Integrity Levels (ASILs)];

c) uses ASILs to specify which of the requirements of ISO 26262 are applicable to avoid unreasonable residual risk;

d) provides requirements for functional safety management, design, implementation, verification, validation and confirmation measures; and

e) provides requirements for relations between customers and suppliers.

The ISO 26262 series of standards is concerned with functional safety of E/E systems that is achieved through safety measures including safety mechanisms. It also provides a framework within which safety-related systems based on other technologies (e.g. mechanical, hydraulic and pneumatic) can be considered.

The achievement of functional safety is influenced by the development process (including such activities as requirements specification, design, implementation, integration, verification, validation and configuration), the production and service processes and the management processes.

Safety is intertwined with common function-oriented and quality-oriented activities and work products. The ISO 26262 series of standards addresses the safety-related aspects of these activities and work products.

Figure 1 shows the overall structure of the ISO 26262 series of standards. The ISO 26262 series of standards is based upon a V-model as a reference process model for the different phases of product development. Within the figure:

— the shaded "V"s represent the interconnection among ISO 26262-3, ISO 26262-4, ISO 26262-5, ISO 26262-6 and ISO 26262-7;

— for motorcycles:
  — ISO 26262-12:2018, Clause 8 supports ISO 26262-3;
  — ISO 26262-12:2018, Clauses 9 and 10 support ISO 26262-4;

— the specific clauses are indicated in the following manner: “m-n”, where “m” represents the number of the particular part and “n” indicates the number of the clause within that part.
Figure 1 — Overview of the ISO 26262 series of standards