ISO 26262-10:2018-12 (E)

Road vehicles - Functional safety - Part 10: Guidelines on ISO 26262

Contents

Page

Foreword ... **vi**

Introduction ... **viii**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **2**

4 Key concepts of ISO 26262 ... **2**
4.1 Functional safety for automotive systems (relationship with IEC 61508[1]) ... 2
4.2 Item, system, element, component, hardware part and software unit ... 4
4.3 Relationship between faults, errors and failures ... 5
4.3.1 Progression of faults to errors to failures ... 5
4.4 FTTI and emergency operation tolerant time interval ... 6
4.4.1 Introduction ... 6
4.4.2 Timing model — Example control system ... 7

5 Selected topics regarding safety management ... **9**
5.1 Work product ... 9
5.2 Confirmation measures ... 9
5.2.1 General ... 9
5.2.2 Functional safety assessment ... 10
5.3 Understanding of safety cases ... 12
5.3.1 Interpretation of safety cases ... 12
5.3.2 Safety case development lifecycle ... 13

6 Concept phase and system development ... **13**
6.1 General ... 13
6.2 Example of hazard analysis and risk assessment ... 13
6.2.1 General ... 13
6.2.2 HARA example 1 ... 13
6.2.3 HARA example 2 ... 14
6.3 An observation regarding controllability classification ... 14
6.4 External measures ... 15
6.4.1 General ... 15
6.4.2 Example of vehicle dependent external measures 1 ... 15
6.4.3 Example of vehicle dependent external measures 2 ... 15
6.5 Example of combining safety goals ... 16
6.5.1 Introduction ... 16
6.5.2 General ... 16
6.5.3 Function definition ... 16
6.5.4 Safety goals applied to the same hazard in different situations ... 16

7 Safety process requirement structure — Flow and sequence of the safety requirements ... **17**

8 Concerning hardware development ... **19**
8.1 The classification of random hardware faults ... 19
8.1.1 General ... 19
8.1.2 Single-point fault ... 19
8.1.3 Residual fault ... 20
8.1.4 Detected dual-point fault ... 20
8.1.5 Perceived dual-point fault ... 20
8.1.6 Latent dual-point fault ... 21
8.1.7 Safe fault ... 21
8.1.8 Flow diagram for fault classification and fault class contribution calculation ... 21
8.1.9 How to consider the failure rate of multiple-point faults related to software-based safety mechanisms addressing random hardware failures ... 25
8.2 Example of residual failure rate and local single-point fault metric evaluation ... 25

8.2.1 General ... 25
8.2.2 Technical safety requirement for sensor A_Master ... 25
8.2.3 Description of the safety mechanism ... 26
8.2.4 Evaluation of example 1 described in Figure 12 ... 29
8.3 Further explanation concerning hardware ... 37
8.3.1 How to deal with microcontrollers in the context of an ISO 26262 series of standards application ... 37
8.3.2 Safety analysis methods ... 37
8.4 PMHF units — Average probability per hour ... 44
9 Safety Element out of Context ... 47
9.1 Safety Element out of Context development ... 47
9.2 Use cases ... 48
9.2.1 General ... 48
9.2.2 Development of a system as a Safety Element out of Context example ... 49
9.2.3 Development of a hardware component as a Safety Element out of Context example ... 51
9.2.4 Development of a software component as a Safety Element out of Context example ... 53
10 An example of proven in use argument ... 55
10.1 General ... 55
10.2 Item definition and definition of the proven in use candidate ... 56
10.3 Change analysis ... 56
10.4 Target values for proven in use ... 56
11 Concerning ASIL decomposition ... 57
11.1 Objective of ASIL decomposition ... 57
11.2 Description of ASIL decomposition ... 57
11.3 An example of ASIL decomposition ... 57
11.3.1 General ... 57
11.3.2 Item definition ... 57
11.3.3 Hazard analysis and risk assessment ... 58
11.3.4 Associated safety goal ... 58
11.3.5 System architectural design ... 58
11.3.6 Functional safety concept ... 59
12 Guidance for system development with safety-related availability requirements ... 60
12.1 Introduction ... 60
12.2 Notes on concept phase when specifying fault tolerance ... 61
12.2.1 General ... 61
12.2.2 Vehicle operating states in which the availability of a functionality is safety-related ... 61
12.2.3 Prevention of hazardous events after a fault ... 61
12.2.4 Operation after fault reaction ... 62
12.2.5 Fault tolerant item example ... 63
12.2.6 ASIL decomposition of fault tolerant items ... 68
12.3 Availability considerations during hardware design phase ... 69
12.3.1 Random hardware fault quantitative analysis ... 69
12.4 Software development phase ... 71
12.4.1 Software fault avoidance and tolerance ... 71
12.4.2 Software fault avoidance ... 71
12.4.3 Software fault tolerance ... 71
13 Remark on "Confidence in the use of software tools" ... 72
14 Guidance on safety-related special characteristics ... 73
14.1 General ... 73
14.2 Identification of safety-related special characteristics ... 74
14.3 Specification of the control measures of safety-related special characteristics ... 74
14.4 Monitoring of the safety-related special characteristics ... 75
Annex A (informative) **Fault tree construction and applications ... 76**
Bibliography ... 79