

Contents

- 1 Introduction 1**
 - 1.1 Definitions and Translations from the ISO 26262 2
 - 1.2 Error Terms of the ISO 26262 5
 - References 6
- 2 Why Functional Safety in Road Vehicles? 7**
 - 2.1 Risk, Safety and Functional Safety in Automobiles 7
 - 2.2 Quality Management System. 13
 - 2.2.1 Quality Management Systems from the Viewpoint of ISO 26262 17
 - 2.3 Advanced Quality Planning 18
 - 2.4 Process Models 20
 - 2.4.1 V-Models. 21
 - 2.4.2 Waterfall Model 30
 - 2.4.3 Spiral Model 31
 - 2.5 Automotive and Safety Lifecycles 33
 - 2.5.1 Safety Lifecycles for the Development of Automotive Products 35
 - 2.5.2 Safety-Lifecycles According to ISO 26262 36
 - 2.5.3 Security-Versus Safety Lifecycles 38
 - References 38
- 3 System Engineering 41**
 - 3.1 Historic and Philosophic Background. 41
 - 3.2 Reliability Engineering. 43
 - 3.2.1 Foundation/Basis of Reliability 45
 - 3.2.2 Reliability and Safety 49
 - 3.3 Architecture Development 51
 - 3.3.1 Stakeholder of Architectures 53
 - 3.3.2 Views of Architecture 56
 - 3.3.3 Horizontal Level of Abstraction 58
 - 3.4 Requirements and Architecture Development 66

3.5	Requirements and Design Specification	68
	References	74
4	System Engineering for Development of Requirements and Architecture	75
4.1	Function Analysis	78
4.2	Hazard and Risk Analysis.	80
4.2.1	Hazard Analysis and Risk Assessment according to ISO 26262	81
4.2.2	Safety Goals.	90
4.3	Safety Concepts	93
4.3.1	The Functional Safety Concept	96
4.3.2	Technical Safety Concept.	106
4.3.3	Microcontroller Safety Concept.	110
4.4	System Analyses	114
4.4.1	Methods for the System Analysis	115
4.4.2	Safety Analysis According to ISO 26262	119
4.4.3	Safety and Security Error Propagation	177
4.5	Verification During Development	177
4.6	Product Development at System Level	179
4.7	Product Development at Component Level	183
4.7.1	Mechanical Development	186
4.7.2	Electronic Development	187
4.7.3	Software Development.	192
	References	199
5	System Engineering in the Product Development.	201
5.1	Product Realization	201
5.1.1	Product Design for Development.	202
5.1.2	Mechanics	202
5.1.3	Electronics	204
5.1.4	Software	204
5.2	Functional Safety and Timing Constraints.	206
5.2.1	Safety Aspects of Fault-Reaction-Time-Interval.	206
5.2.2	Safety Aspects and Real-Time Systems	207
5.2.3	Timing and Determinism	209
5.2.4	Scheduling Aspects in Relation to Control-Flow and Data-Flow Monitoring	211
5.2.5	Safe Processing Environment	214
6	System Integration.	217
6.1	Verifications and Tests	218
6.1.1	Basic Principles for Verifications and Tests	225
6.1.2	Verification based on Safety Analyses	228
6.1.3	Verification of Diverse Objectives such as Safety and Security	232

6.1.4	Test Methods	233
6.1.5	Integration of Technical Elements	234
6.2	Safety Validation.	236
6.3	Model Based Development.	239
6.3.1	Models for Functional Safety	241
6.3.2	Foundation for Models.	244
6.3.3	Model Based Safety Analysis	245
6.4	Approvals/Releases	246
6.4.1	Process Releases	247
6.4.2	Release for Series Production	248
6.4.3	Production Part Approval Process (PPAP)	249
	References	251
7	Confirmation of Functional Safety	253
7.1	Confirmation Reviews	257
7.2	Functional Safety Audits	261
7.3	Assessment of Functional Safety	262
7.4	Safety Case	263
	References	265
	Index	267

<http://www.springer.com/978-3-319-33360-1>

Functional Safety for Road Vehicles
New Challenges and Solutions for E-mobility and
Automated Driving

Ross, H.-L.

2016, XV, 269 p. 128 illus., 101 illus. in color.,

Hardcover

ISBN: 978-3-319-33360-1