

Inhalt

Vorwort vom Autor	V
Der Autor	XIII
1 Einleitung	1
1.1 Begriffe und Übersetzungen aus der ISO 26262.....	2
1.2 Fehlerbegriffe der ISO 26262	5
2 Warum Funktionssicherheit im Automobil?	7
2.1 Risiko, Sicherheit und Funktionssicherheit im Automobil	8
2.2 Qualitätsmanagementsystem	13
2.2.1 Qualitätsmanagementsysteme aus Sicht der ISO 26262	19
2.3 Qualitätsvorausplanung	20
2.4 Prozessmodelle	23
2.4.1 V-Modelle	24
2.4.2 Wasserfallmodell.....	31
2.4.3 Spiralmodell.....	32
2.5 Management der Funktionalen Sicherheit im Automobil- und Sicherheitslebenszyklus.....	35
2.5.1 Sicherheitslebenszyklus für die Automobilentwicklung	37
2.5.2 Sicherheitslebenszyklus gemäß ISO 26262	39
3 Systemengineering	43
3.1 Geschichtliche und philosophische Hintergründe.....	43
3.2 Technische Zuverlässigkeit.....	46
3.2.1 Grundlage der Zuverlässigkeit	49
3.2.2 Zuverlässigkeit und Sicherheit.....	53
3.3 Architekturentwicklung	56
3.3.1 Stakeholder von Architekturen	58
3.3.2 Sichten einer Architektur.....	62
3.3.3 Horizontale Abstraktionsebene.....	64

3.4	Anforderungs- und Architekturentwicklung	75
3.5	Anforderungs- und Designspezifikation.....	77
4	Systemengineering zur Entwicklung von Anforderungen und Architektur....	85
4.1	Funktionsanalyse	90
4.2	Gefahren- und Risikoanalyse.....	94
4.2.1	Gefahren- und Risikoanalyse gemäß ISO 26262	96
4.2.2	Sicherheitsziele.....	104
4.3	Sicherheitskonzepte	107
4.3.1	Funktionales Sicherheitskonzept.....	110
4.3.2	Technisches Sicherheitskonzept.....	121
4.3.3	Mikrokontroller-Sicherheitskonzepte.....	126
4.4	Systemanalysen	130
4.4.1	Methoden zur Systemanalyse.....	131
4.4.2	Sicherheitsanalysen gemäß ISO 26262.....	136
4.4.2.1	Fehlerpropagation	142
4.4.2.2	Fehlerpropagation in der Horizontalen und Vertikalen	149
4.4.2.3	Induktive Sicherheitsanalyse	153
4.4.2.4	Deduktive Sicherheitsanalyse	156
4.4.2.5	Quantitative Sicherheitsanalysen.....	162
4.4.2.6	Architekturmetriken.....	166
4.4.2.7	Top-Fehlermetrik (PMHF).....	170
4.4.2.8	Fehlermetriken bei Sensoren oder anderen Komponenten	174
4.4.2.9	Analyse der abhängigen Fehler (Analysis of dependent failures).....	176
4.4.2.10	Sicherheitsanalysen im Sicherheitslebenszyklus.....	182
4.5	Verifikation während der Entwicklung.....	188
4.6	Produktentwicklung auf Systemebene	191
4.7	Produktentwicklung auf Komponentenebenen	195
4.7.1	Mechanikentwicklung.....	198
4.7.2	Elektronikentwicklung	200
4.7.3	Softwareentwicklung.....	205
5	Systemengineering in der Produktrealisierung.....	215
5.1	Produktrealisierung.....	215
5.1.1	Produktdesign zur Realisierung.....	216
5.1.2	Mechanik.....	216

5.1.3	Elektronik.....	218
5.1.4	Software.....	218
6	Systemintegration	221
6.1	Verifikationen und Tests	222
6.1.1	Grundlagen zu Verifikation und Test	226
6.1.2	Verifikation basierend auf Sicherheitsanalysen	228
6.1.3	Testmethoden	232
6.1.4	Integration technischer Elemente.....	233
6.2	Validierung.....	235
6.3	Modellbasierende Entwicklung.....	237
6.3.1	Modelle für die Funktionale Sicherheit	240
6.3.2	Grundlage für Modelle.....	243
6.3.3	Modellbasierende Sicherheitsanalyse.....	244
6.4	Freigaben	246
6.4.1	Prozessfreigaben.....	247
6.4.2	Freigabe zur Serienproduktion	249
7	Bestätigung der funktionalen Sicherheit.....	251
7.1	Reviews zur Bestätigung der Normerfüllung.....	255
7.2	Prozessanalyse zur funktionalen Sicherheit.....	256
7.3	Bewertung / Assessment der funktionalen Sicherheit	260
7.4	Sicherheitsnachweis.....	261
	Index.....	265