Inhaltsverzeichnis

1 Einleitung 1

1.1 Wieso die automotive spezifische Sicherheitsnorm ISO 26262:2011? 1

1.1.1 ISO 26262:2011, Edition 15.11.2011 2

1.1.2 Fachausschuss für Kraftfahrzeuge 3

1.1.3 Stand der Technik 3

1.1.4 ISO 26262:2011 – eine anwendbare Norm 3

1.1.5 Beweislastumkehr 4

1.2 Stufenweise zum ASIL-konformen Produkt 4

1.2.1 Klare Zuordnung von Verantwortung 5

1.2.2 Prozessmodell und Reifegrade von Prozessen 6

2 Was Sie in diesem Buch erwartet 7

2.1 Allgemeine Hinweise 7

Zielgruppe für dieses Fachbuch 9

2.2 Voraussetzungen und Annahmen unseres Projekts »Joy« mit dem Produkt »Joystick-Sensor« 9

Rechte Dritter 10

2.3 Wegweiser durch das Buch 11

2.4 Projektsteckbrief »Joy« 11

2.4.1 Die Innovation 12

2.4.2 Produktinformationen 13

2.5 Die beteiligten Firmen 16

2.6 Das Joy-Entwicklungsteam 17

2.7 Rechtliche Grundlagen und Pflichten 19

3 Das Phasenmodell 21
3.1 Organisatorische Anforderungen ... 21
3.2 Prozessmodelle und funktionales Sicherheitsmanagement ... 22
3.3 Das Phasenmodell der ISO 26262:2011 ... 22
3.4 Schaffung einer Sicherheitskultur ... 25
3.4.1 Projektbeispiel ... 25
3.4.2 Fragenkatalog zur Sicherheitskultur ... 26
3.4.3 Hinweis World Cafe und Open Space ... 30
3.5 Management der funktionalen Sicherheit ... 30
Vorgehen und Voraussetzungen ... 30
3.6 Funktionales Sicherheitsmanagement im Projekt Joy ... 31
3.7 Sicherheitspolitik und Sicherheitsplan der safehicle GmbH ... 32
Maßnahmen zur Sicherstellung der funktionalen Sicherheit ... 32
3.8 Aktivitäten im Sicherheitslebenszyklus ... 33
3.8.1 Praxisbeispiel Projektstory ... 33
3.8.2 Managementaktivitäten ... 35
3.8.3 Bestätigungsmaßnahmen ... 36
3.9 Unterstützende Prozesse ... 37
Tailoring-Anpassungsrichtlinien ... 37

4 Spezifische Rollen im Sicherheitslebenszyklus 39
4.1 Das effektive Team ... 39
4.1.1 Projektbeispiel Ressourcenplanung ... 40
4.1.2 Schulungsbedarf methodisch feststellen ... 41
4.2 Qualifikation ... 42
4.3 Der Sicherheitsmanager im Projekt Joy ... 44
4.4 Rollenbeschreibung FSM ... 45
4.4.1 Projektbeispiel ... 46
4.4.2 Der Sicherheitskoordinator im Projekt Joy ... 47
4.5 Rollenbeschreibung Sicherheitskoordinator ... 47
4.6 Weitere Rollen im Sicherheitslebenszyklus ... 49
4.6.1 Rolle Vertriebsverantwortlicher und Produktspezialist ... 49
4.6.2 Sachbearbeiter in der Angebotsabteilung ... 49
4.6.3 Verantwortlicher für Auftragsabwicklung ... 50

4.6.4 Produktspezialist ASIL (Mitarbeiter aus dem Produktmanagement) 50
4.6.5 Projektmanager 50
4.6.6 Entwicklungspersonal und Validationspersonal 51
4.6.7 Montagepersonal 51
4.6.8 Prüfer und Personal zur Inbetriebnahme 52
4.6.9 Sachbearbeiter im Service/Sachbearbeiter in der Auftragsabwicklung 52
4.6.10 Servicetechniker in der Werkstatt 52
4.6.11 Unabhängiger Dritter (Assessment) 53
4.7 Rollenvielfalt 53

5 Konfigurations- und Änderungsmanagement 55
5.1 Konfigurationsmanagement 55
5.1.1 Aufgabe des Konfigurationsmanagements 55
5.1.2 Aktivitäten im KM am Projektbeispiel 56
5.1.3 Meilensteine – Baselines – Schnittstellen – Zugriffe 56
5.1.4 Tooleinsatz und Lieferung von KM-Items 57
5.2 Der Konfigurationsmanager 58
5.3 Änderungsmanagement nach ISO 26262:2011 59
5.4 Planung des CM im Team der Fa. safehicle 61
Änderungen unter dem Aspekt der funktionalen Sicherheit 61
5.5 Aspekte zur Prozessanpassung 62
5.6 Zustimmungsprozess 63
Beispiel-Fragenkatalog 64
5.7 Schnittstellenmodifikation und Zustimmung 64
Betrachtung der technischen Schnittstellen-modifikation 65
5.8 Exkurs Retrospektive 67
5.8.1 Methoden der Retrospektive 67
5.8.2 Durchführung der Retrospektive 68

6 Initialisierung des Sicherheitslebenszyklus und Development Interface Agreement 71
6.1 Initialisierung 71
6.2 Lieferantenauswahl 71

6.3 Qualifikationsanfrage und Auswahlbericht ... 72
6.4 Development Interface Agreement ... 74
Zusammenarbeit in der Lieferkette mit dem OEM ... 75
6.5 DIA-Vorgehen am Beispiel des Projekts Joy ... 76
6.6 Initialisierung des Sicherheitslebenszyklus ... 77
Projekt Joy – Zuordnung von Phasen und Aufgaben ... 77
6.7 Exkurs Ausschreibung und Unterbeauftragung ... 78

7 Das Konzept des Automotive Safety Integrity Level 81
7.1 Historie und Hintergrund zum ASIL ... 81
7.1.1 Risikoreduktion ... 82
7.1.2 Vom Sicherheitsziel zum Sicherheitskonzept im Projekt Joy ... 83
7.2 Die Bedeutung von ASIL in den Tabellen der Norm ... 84
7.3 ASIL-abhängige Anforderungen und Empfehlungen ... 85
7.4 Grundlagen der ASIL-Dekomposition ... 87
7.4.1 Dekompositionsansatz Joystick-Sensor ... 87
7.4.2 Dekomposition von Sicherheitsanforderungen ... 87
7.4.3 Grenzen und Einschränkungen der Dekomposition ... 90
7.4.4 Aspekt der Verfügbarkeit ... 91
7.4.5 Kurzes Projektbeispiel für sicheren Zustand ... 91
7.5 Vorteile und Implikationen durch die Anwendung der ISO 26262 ... 92
7.5.1 Verbesserte Prozessqualität ... 92
7.5.2 Verbesserte Geschäftsbeziehungen ... 92
7.5.3 Verbesserte Produktqualität ... 93
7.5.4 Finanzieller Nutzen ... 93
7.6 Quantitative und qualitative Methoden ... 94
7.6.1 Qualitative Methode ... 94
7.6.2 Quantitative Methode ... 94
7.7 Sicherheitsanalyse ... 95
7.7.1 Qualitative und quantitative Methoden im Projekt Joy ... 97
7.7.2 Erkenntnistheorie ... 97

8 Gefährdungs- und Risikoanalyse 99
8.1 Ermittlung von Gefahren und Klassifikation ... 99
8.2 Durchführung der Analyse – Projektbeispiel ... 100
Bericht zur Gefährdungs- und Risikoanalyse ... 101
8.3 Vorgehen in der Produktlebenszyklusphase ... 102
8.4 Wechselwirkungen mit anderen Systemen ... 102
8.5 Risikobewertung ... 102
Gefährdungs- und Risikoanalyse durch den Zulieferer am Projektbeispiel ... 103
8.6 Methode zur Risikobewertung ... 104
8.7 ASIL-Bestimmung ... 107
8.8 Konkrete Beispiele aus dem Projekt Joy ... 109
8.8.1 Beispiel »Vortrieb« ... 113
8.8.2 Beispiel »Bremskraft« ... 116
8.8.3 Beispiel »Lenkwinkel« ... 119
8.9 Abschluss der G&R ... 120

9 Spezifikation der funktionalen und technischen Sicherheitsanforderungen 121
9.1 Funktionale Sicherheitsanforderungsspezifikation ... 121
9.2 Spezifikationsvorgehen Joy und Joystick-Sensor ... 122
9.2.1 Funktionale Sicherheitsanforderungsspezifikation ... 122
9.2.2 Technische Sicherheitsanforderungen des Subsystems ... 122
9.2.3 Technische Anforderungsumsetzung zur Risikoreduktion ... 123
9.2.4 Projektbeispiel Joy ... 125
9.3 Systemvalidierung ... 126
9.4 Zuverlässigkeit, funktionale Sicherheit und Verfügbarkeit ... 127
Konflikt zwischen Kosten und Verfügbarkeit ... 127
9.5 Sicherheits-Assessment ... 128
9.5.1 Unabhängigkeit ... 129
9.5.2 Planung des Sicherheits-Assessments ... 130
9.5.3 Agenda zum Sicherheits-Assessment im Projekt Joy ... 130
9.5.4 Ableitung von Maßnahmen ... 134

10 Verifikations- und Validationsplanung 135
10.1 Allgemeine Hinweise zu V+V ... 135
Definition zu V+V im Projekt Joy ... 137
10.2 Handlungsfelder der Verifikation ... 138
10.2.1 Verifikationsspezifikation ... 139
10.2.2 Testbericht ... 140
10.3 Handlungsfelder der Validation ... 141
10.3.1 Umfang der Validationsplanung ... 142
10.3.2 Gemeinsame Validationsplanung und Planungsinhalt ... 143
10.4 Hardware-Software-Integration ... 145
10.5 Systemintegrationstests ... 146
10.6 Integrationstestmethoden ... 148
10.6.1 Fault-Injection-Test ... 149
10.6.2 Back-to-Back-Test ... 149
10.6.3 Schnittstellenprüfungen ... 150
10.6.4 Erfahrungsbasierte Tests ... 150
10.7 Integration und Tests auf Fahrzeugebene ... 151
10.8 Validationsplanung der Hardware ... 152
10.8.1 Hardwareintegration und Hardware-Integrationstest ... 153
10.8.2 Methoden im Projekt Joy ... 154
10.8.3 Bewertung der Verletzung von Sicherheitszielen im Hinblick auf zufällige Hardwarefehler ... 155
10.8.4 Validation der Metriken für zufällige Hardwarefehler ... 156
10.8.5 Bewertung der Metriken der Hardwarearchitektur ... 156
10.8.6 Input und Output zur Bewertung des Hardwaredesigns ... 157
10.8.7 Projektbeispiel Hardwaredesign-Review ... 157
10.9 Softwaremodultest ... 158
10.9.1 Methoden zur Ableitung und Durchführung von Softwaremodultestfällen ... 159
10.9.2 Softwareintegration und Test ... 160
10.9.3 Softwareintegrationstest ... 161
10.10 Projektbeispiel Softwaretest ... 162
10.11 Verifikation der Software-Sicherheitsanforderungen ... 163
10.12 Analyse und Validierung mechatronischer Systeme ... 165

11 Produktentwicklung auf Systemebene 167
11.1 2000 Anforderungen in der Konzeptphase ... 167
11.2 Übersicht ... 168
11.3 Initialisierung der Produktentwicklungsphase auf Systemebene ... 169
11.4 Spezifikation der technischen Sicherheitsanforderungen ... 171
11.4.1 Spezifikation von Sicherheitsmechanismen ... 172
11.4.2 Hardware-Fehlerklassen und Metriken ... 173
11.4.3 Vorgehensmodell zu den zufälligen Hardwarefehlern ... 175
11.5 Technische Sicherheitsanforderungen im Projekt Joy ... 176
11.5.1 Der Weg zu technischen Sicherheitsanforderungen ... 176
11.5.2 Projektbeispiel ... 178
11.5.3 Fehler in der internen Verarbeitung ... 179
11.5.4 Redundanz im Systemdesign ... 180
11.5.5 Anforderungen an die Übermittlung der Sensordaten ... 181
11.6 Systemdesign ... 182
11.6.1 Vermeidung systematischer Fehler ... 183
11.6.2 Erkennungsmaßnahmen für zufällige Fehler ... 183
11.6.3 Projektbeispiel ... 183
11.6.4 Fault Tree Analysis (FTA) ... 185
11.6.5 Alternative Metrik »CutSet-Methode« für Hardwarefehler ... 186
11.6.6 Grenzwerte der Metriken ... 187
11.7 Spezifikation des Hardware-Software-Interface (HSI) ... 188
11.8 Verifikation des Systemdesigns ... 189
11.9 Item-Integration und Tests ... 190
11.10 Zusammenfassung ... 190

12 Dokumentation und Arbeitsprodukte 191
12.1 Anforderungen an die Dokumentation ... 191
Kennzeichnung und geforderte Informationen ... 193
12.2 »Wer schreibt, der bleibt« oder »allzu viel ist ungesund« – Projektbeispiel ... 194
Planung und Konfliktlösung im Team ... 194
12.3 Phasenübergreifende Dokumentation ... 195

12.4 Schlüsseldokumente der ISO 26262:2011 – Teil 2 »Funktionales Sicherheitsmanagement« 196
12.4.1 Übergeordneter Sicherheitsmanagementplan 197
12.4.2 Qualifikationsnachweise 197
12.4.3 Anerkanntes dokumentiertes Qualitätsmanagement-system 198
12.4.4 Der Sicherheitsplan 198
12.5 Der Sicherheitsnachweis 200
12.5.1 Der Sicherheitsnachweis – Safety Case (FS-Arbeitsprodukte) 200
12.5.2 Referenzen und relevante Dokumente 200
12.5.3 Referenzen zu zentralen sicherheitsrelevanten Dokumenten 200
12.5.4 Definitionen, Begriffe, Abkürzungen 201
12.5.5 Sicherheitsplan 201
12.5.6 Item-Definition 201
12.5.7 Compliance-Matrix 201
12.5.8 Meeting-Protokolle 201
12.5.9 Arbeitsprodukte aus Planungsprozessen 202
12.5.10 Arbeitsprodukte aus der Initialisierung des Sicherheitslebenszyklus 202
12.5.11 Arbeitsprodukte aus den unterstützenden Prozessen 202
12.5.12 Statusberichte 202
12.5.13 Sicherheitskontrollplanung für die Produktion 202
12.5.14 Auszüge aus der G&R 203
12.5.15 Funktionales Sicherheitskonzept 203
12.5.16 Sicherheitsanforderungsspezifikation 203
12.5.17 Arbeitsprodukte aus Verifikation und Validation 203
12.5.18 Sicherheitsanalyse und Sicherheitsberichte 204
12.5.19 Sicherheitsargumente 204
12.5.20 Safety-To-do-Liste aus dem Sicherheitsnachweis 205
12.5.21 Der Assessmentplan und Prozesskonformität 205
12.5.22 Zusammenfassung 206

12.6 Schlüsseldokumente der ISO 26262:2011 – Teil 3 »Konzeptphase« 206
12.6.1 Item-Definition 206
12.6.2 Arbeitsprodukt Einflussanalyse 207
12.6.3 Gefährdungs- und Risikoanalyse 207
12.6.4 Funktionales Sicherheitskonzept 208

13 Abhängige Dokumentation und Arbeitsprodukte 211

13.1 Allgemein 211
13.2 Schlüsseldokumente der ISO 26262:2011 – Teil 4 »Produktentwicklung auf Systemebene« 212
13.2.1 Validationsplan und Validationsberichte 213
13.2.2 Sicherheits-Assessment auf Systemebene 214
13.2.3 Dokumentation zur Produktionsfreigabe 214
13.2.4 Technische Sicherheitsanforderungen 215
13.2.5 Das technische Sicherheitskonzept 215
13.3 Schlüsseldokumente der ISO 26262:2011 – Teil 5 »Produktentwicklung auf Hardwareebene« 216
13.3.1 Sicherheitsplan auf Hardwareebene 216
13.3.2 Spezifikationen auf Hardwareebene 217
13.3.3 Dokumentation des Hardwaredesigns 218
13.3.4 Sicherheitsanalyse 218
13.3.5 Dokumentation der Hardware-Architekturmetriken ... 219
13.3.6 Hardwareintegration und Hardwaretest 220
13.4 Schlüsseldokumente der ISO 26262:2011 – Teil 6 »Softwarerealisierung« 221
13.4.1 Planung und Initiierung 222
13.4.2 Software-Sicherheitsanforderungen sowie Verifikationsplanung 222
13.4.3 Softwareentwurf 223
13.4.4 Softwaremoduldesign und Softwareumsetzung 223
13.4.5 Softwaremodultest 224
13.4.6 Softwareintegration und Test 224
13.4.7 Konfigurationsdaten und Kalibrierungsdaten 226

13.5 Schlüsseldokumente der ISO 26262:2011 – Teil 7 »Produktion und Betrieb« ... 227
13.5.1 Produktionsplan und Produktionskontrollplan ... 228
13.5.2 Betrieb, Wartung und Stilllegung ... 228
13.6 Schlüsseldokumente der ISO 26262:2011 – Teil 8 »Unterstützende Prozesse« ... 229
13.7 Schlüsseldokumente der ISO 26262:2011 – Teil 9 ... 230
»ASIL- und sicherheitsorientierte Analysen« ... 230
13.7.1 ASIL-Dekomposition ... 230
13.7.2 Kriterien für die Koexistenz von Elementen ... 230
13.7.3 Analyse abhängiger Fehler und Ausfälle ... 230
13.7.4 Sicherheitsanalyse ... 231
13.8 Zusammenfassung ... 231

14 Reviews 233

14.1 Allgemein ... 233
14.1.1 Vorgehensweise bei Reviews ... 234
14.1.2 Reviewtechniken ... 235
14.1.3 Abhängigkeit zwischen ASIL und Reviewtechnik ... 237
14.2 Lesetechniken ... 238
14.2.1 Einführung ... 238
14.2.2 Ad hoc ... 240
14.2.3 Checklistenbasierte Lesetechnik ... 241
14.2.4 Reading by stepwise abstraction ... 242
14.2.5 Fehlerklassenbasiertes Lesen ... 243
14.2.6 Perspektivenbasiertes Lesen ... 244
14.2.7 Zusammenfassung ... 245

15 Vertrauen in Softwarewerkzeuge 247

15.1 Vertrauen in und Qualifikation von Softwarewerkzeugen ... 247
15.2 Weshalb eine sorgfältige Werkzeugauswahl wichtig ist ... 248
15.3 Vertrauensgrad – Tool Confidence Level ... 251
15.3.1 Werkzeug-Qualifizierungsplan ... 254
15.3.2 Werkzeugdokumentation ... 254
15.3.3 Werkzeug-Bug-Report ... 255

15.3.4 Bewertung des Werkzeug-Entwicklungsprozesses 255
15.3.5 Überprüfung der Leistungsfähigkeit des Werkzeugs 255
15.3.6 Qualifizierungsbericht im Projekt Joy 256
15.4 Exkurs: Betriebsbewährtheit 257

16 Retrospektive **261**
16.1 Die Planung sicherheitsgerichteter Items 261
16.2 Firma safehicle – Prozessveränderungen aus den Planungsaktivitäten 263
Auswertungsbericht 265
16.3 Zusammenfassung 268

17 Ausblick **269**
Abschließende Worte der Autoren 269

A Anhang **271**
A.1 Arbeitshilfen-Checklisten zur Planung 271
A.2 Beispiel für Sicherheitskultur 280
A.3 Fundamentaler Testprozess 281
German Testing Board (GTB) 282
A.4 Psychologische Ursachen von Fehlern 282
A.4.1 Denkfallen als Fehlerursache 283
A.4.2 Zusammenfassung 285

B Glossar **287**

C Abkürzungsverzeichnis **293**

D Normen und Standards **297**

E Webadressen **299**

F Literaturverzeichnis **301**

Stichwortverzeichnis **305**