Safety Engineering

Das Praxisbuch für funktionale Sicherheit

DAS INHALTS-VERZEICHNIS

Auf einen Blick

1 Einführung 17

2 Der Weg durch das Buch 21

3 Normen 37

4 Ausfälle und Fehler 57

5 Softwaresicherheit 73

6 Hardwaresicherheit 113

7 Kenngrößen 133

8 Gefahrenanalyse 159

9 Kenngrößenbestimmung 187

10 Fehlerbaumanalyse 213

11 Risikograph 249

12 Layer of Protection Analysis 265

13 Zuverlässigkeitsblockdiagramme 281

14 Markov-Prozess 305

15 Markov Decision-Prozess 321

16 Reliability, Availability, Maintainability und Serviceability 341

17 Binary Decision Diagramms 367

Inhalt

Vorwort 15

1 Einführung 17

2 Der Weg durch das Buch 21

2.1 Einleitende Kapitel 22

2.2 Methoden zur qualitativen Analyse und Mischformen 28

2.3 Methoden zur quantitativen Analyse 31

3 Normen 37

3.1 Überblick 37

3.2 Fallbeispiel: Deepwater Horizon 44

3.3 Die Norm IEC-61508 45

3.3.1 Konzept und Planung 46

3.3.2 Entwicklung 49

3.3.3 Integration 50

3.3.4 Betrieb und Instandhaltung 50

3.3.5 Außerbetriebsetzung 50

3.3.6 Dokumente nach IEC-61508 51

3.4 Weitere Normen 51

3.4.1 Die Norm ISO-26262 52

3.4.2 Die Norm IEC-61511 53

3.4.3 Die Norm ISA-TR-84.0.02 53

3.4.4 Die Norm DIN-19250 54

3.4.5 Die Norm DIN-VDE-0801 54

3.5 Die Norm IEC-62061 und die Norm ISO-13849 55

3.6 Abschließende Bemerkungen 56

4 Ausfälle und Fehler 57

4.1 Fallbeispiele 57
4.1.1 Das Seveso-Unglück 57
4.1.2 Das Metrounglück der Red Line in New York 58

4.2 Definitionen 59
4.2.1 Sicherheit 59
4.2.2 Risiko 60
4.2.3 Schaden 60
4.2.4 Zuverlässigkeit 60
4.2.5 Verfügbarkeit 61

4.3 Ausfall und Fehler 61
4.3.1 Zufällige Ausfälle der Hardware 62
4.3.2 Systematische Ausfälle 62

4.4 Fehlermöglichkeiten 62

4.5 Fehlerraten 63
4.5.1 Sicherheitsrelevanter Faktor 65
4.5.2 Diagnostic Coverage-Faktor 65
4.5.3 Safe Failure Fraction 66

4.6 Fehlertoleranz 67
4.6.1 Hardwareredundanz 69
4.6.2 Softwareredundanz 69
4.6.3 Zeitredundanz 69
4.6.4 Informationsredundanz 69
4.6.5 Beispiel von Redundanz mit einem ASIC 70

4.7 Minimale Schnittmenge und Fehler gemeinsamer Ursache 71

4.8 Abschließende Bemerkungen 72

5 Softwaresicherheit 73

5.1 Fallbeispiel: Flight 965 73

5.2 Softwareentwicklung 74
5.2.1 Modularisierung und strukturierte Programmierung 77
5.2.2 Entwurfs- und Codierungsrichtlinien 78
5.2.3 Rechnergestützte Entwurfswerkzeuge 79
5.2.4 Statischer Quellcode-Analysator 80
5.2.5 Dynamischer Quellcode-Analysator 81

5.2.6 Quellcode-Speicher bzw. Repository ... 81
5.2.7 Quellcode-Beautifier ... 81
5.2.8 Quellcode-Reviewing ... 82
5.2.9 Defensive Programmierung ... 82
5.2.10 Semiformale Methoden ... 84
5.2.11 Verweise im Dokument Software Safety Requirements ... 85

5.3 Modul- und Integrationstests ... 85
5.3.1 Verifikation ... 86
5.3.2 Validierung ... 86
5.3.3 Modul-Logging ... 86
5.3.4 Testabdeckung ... 88
5.3.5 Blackboxtest ... 92
5.3.6 Leistungstest ... 93
5.3.7 Software und Hardwareintegration ... 94
5.3.8 Ticketmanagementsystem ... 97
5.3.9 Konfigurationsmanagementsystem ... 99

5.4 Überblick über Entwicklungspläne und Testpläne ... 100

5.5 Softwareentwicklungsprozess und Bauplan ... 101
5.5.1 Softwareentwicklungsprozess ... 102
5.5.2 Bauplan ... 108
5.5.3 Bezug zum Fallbeispiel ... 111

5.6 Abschließende Bemerkungen ... 111

6 Hardwaresicherheit 113

6.1 Fallbeispiel: Das Spaceshuttle-Challenger-Unglück ... 113

6.2 Hardwareentwicklung ... 114
6.2.1 Hardware Description Language ... 117
6.2.2 Sprachen für speicherprogrammierbare Steuerungen ... 118
6.2.3 Ablaufsprachen ... 119
6.2.4 Sicherheitstechniken realisiert durch Hardware ... 121

6.3 Überblick über Entwicklungs-, Integrations- und Testpläne ... 124

6.4 Hierarchische Struktur der Hardware ... 125

6.5 Bestimmung des Sicherheitsintegritätslevels ... 127
6.5.1 Route-1H-Methode ... 127
6.5.2 Route-2H-Methode ... 130

6.6 Abschließende Bemerkungen ... 131

7 Kenngrößen 133

7.1 Fallbeispiel: Starfighter ... 133

7.2 Wahrscheinlichkeit eines Ausfalls ... 135
7.2.1 Additionsoperation ... 135
7.2.2 Komplementäroperation ... 137
7.2.3 Multiplikationsoperation ... 137
7.2.4 Bedingte Wahrscheinlichkeit ... 138

7.3 Zuverlässigkeit und Ausfallwahrscheinlichkeit ... 138

7.4 Dichtefunktionen der Ausfallhäufigkeit ... 139
7.4.1 Dichtefunktion der Exponentialverteilung ... 142
7.4.2 Dichtefunktion der Weibullverteilung ... 143
7.4.3 Dichtefunktion der Normalverteilung ... 143
7.4.4 Dichtefunktion der Lognormalverteilung ... 144

7.5 Statistische Kennzahlen ... 145
7.5.1 Mittlere Betriebszeit ... 145
7.5.2 Mittlere Reparaturzeit ... 146
7.5.3 Mittlere Ausfallzeit ... 147

7.6 Ausfallrate ... 148

7.7 Nichtverfügbarkeit und Ausfallrate des Sicherheitssystems ... 151
7.7.1 Probability for Dangerous Failure on Demand, PFD ... 151
7.7.2 Mittlere Ausfallzeit bei nicht-entdeckbarem Fehler ... 154
7.7.3 Mittlere Ausfallzeit bei entdeckbarem Fehler ... 155
7.7.4 Mittlere Ausfallzeit bei entdeckbarem und nicht-entdeckbarem Fehler ... 155
7.7.5 Average Frequency of dangerous Failures, PFH ... 156

7.8 Abschließende Bemerkungen ... 158

8 Gefahrenanalyse 159

8.1 Fallbeispiel: Das Unglück in Bhopal, Indien ... 159

8.2 Methoden zur Gefahrenanalyse ... 160
8.2.1 Qualitative Methoden zur Gefahrenanalyse ... 161
8.2.2 Quantitative Methoden zur Gefahrenanalyse ... 161

8.3 Failure Mode Effect Analysis ... 162
8.3.1 Ziele von FMEA ... 163

8.3.2 Schritte von FMEA ... 164
8.3.3 Vorgehen bei der Analyse ... 169
8.4 Das ALARP-Prinzip ... 175
8.5 Hazard and Operability ... 178
8.5.1 Definitionen ... 180
8.5.2 Vorbereitung ... 181
8.5.3 Analyse ... 181
8.5.4 Dokumentation ... 182
8.5.5 Vorgehen bei der HAZOP-Untersuchung ... 183
8.6 Abschließende Bemerkungen ... 185

9 Kenngrößenbestimmung 187

9.1 Fallbeispiel: Fords Pinto Memo ... 187
9.2 Bestimmung der Ausfallrate aus Handbüchern ... 188
9.2.1 Part-Stress-Analyse ... 189
9.2.2 Part-Count-Analyse ... 190
9.2.3 Die Norm IEC-61709 ... 191
9.3 Parameterfreie statistische Methoden ... 192
9.4 Parametrisierte statistische Methoden ... 195
9.4.1 Parametrisierte statistische Methoden mit unzensierten Daten ... 195
9.4.2 Parametrisierte statistische Methoden mit zensierten Daten ... 198
9.5 Datensammlung ... 201
9.5.1 Anforderungen an die Daten ... 203
9.5.2 Prozess für die Datensammlung ... 205
9.5.3 Strukturierung der Daten ... 206
9.5.4 Beispieltabellen für die Datenbank ... 208
9.6 Abschließende Bemerkungen ... 211

10 Fehlerbaumanalyse 213

10.1 Fallbeispiel: Der Three-Miles-Island-Reaktorunfall ... 213
10.2 Anwendung der Fehlerbaumanalyse ... 215
10.2.1 Systemanalyse ... 217
10.2.2 Definition des unerwünschten Ereignisses ... 218

10.2.3 Aufstellung des Fehlerbaums ... 219
10.2.4 Auswertung des Fehlerbaums ... 219
10.2.5 Dokumentation, Präsentation und Schlussfolgerung ... 220

10.3 Symbole ... 220
10.3.1 Ereignisse und Kommentarboxen ... 221
10.3.2 Gatter ... 221

10.4 Fehlerbaumerstellung ... 226

10.5 Fehlerbaumanalyse ... 230
10.5.1 Qualitative Auswertung ... 230
10.5.2 Quantitative Auswertung ... 234

10.6 Weitere Analysetechniken ... 236
10.6.1 Sensitivitätsanalyse ... 236
10.6.2 Monte Carlo-Analyse ... 242

10.7 Abschließende Bemerkungen ... 246

11 Risikograph 249

11.1 Fallbeispiel: Das Zugunglück bei East Palastine, Ohio ... 249

11.2 Risikograph nach IEC-61508 ... 250
11.2.1 Parameter des Risikographen ... 252
11.2.2 Kalibrierung des Risikograph ... 259

11.3 Risikograph nach ISO-26262 ... 261

11.4 Abschließende Bemerkungen ... 263

12 Layer of Protection Analysis 265

12.1 Fallbeispiel: Das Brandunglück im St.-Gotthard-Tunnel ... 265

12.2 Funktionale Sicherheit mit Schutzebenen ... 266

12.3 Typische Schutzebenen ... 267
12.3.1 Allgemeiner Prozessentwurf ... 267
12.3.2 Basisprozesskontrollsystem ... 268
12.3.3 Alarme ... 268
12.3.4 Weitere Maßnahmen zur Risikominimierung und eingeschränkter Zugang ... 269

12.3.5 Unabhängige Schutzebenen ... 269
12.3.6 SIS als IPL ... 271
12.3.7 Risikoreduzierung durch Aneinanderreihung der Schutzebenen ... 272

12.4 Layer-of-Protection-Analyse, die Erweiterung von HAZOP ... 273
12.4.1 Protection Layers ... 274
12.4.2 Auswertung der LOPA ... 276

12.5 Anwendung von LOPA am Fallbeispiel ... 277

12.6 Abschließende Bemerkungen ... 279

13 Zuverlässigkeitsblockdiagramme 281

13.1 Fallbeispiel: Jakarta Incident ... 281

13.2 Modellierung der Zuverlässigkeit ... 283
13.2.1 Zuverlässigkeitsblockdiagramm und Funktionsblockdiagramm ... 284
13.2.2 Zwei Beispiele von Quadschaltungen ... 284
13.2.3 Arten von Redundanzen ... 285

13.3 Strukturen mit RBD ... 287
13.3.1 Zeitunabhängige Serien- und Parallelstrukturen ... 287
13.3.2 Gemischte Strukturen ... 290
13.3.3 RBD-Strukturen mit Vernetzungen ... 291
13.3.4 Zeitabhängige RBD ... 293
13.3.5 RBD und Fehlerbäume ... 294
13.3.6 doon-Architekturen ... 296
13.3.7 Teilsysteme aus Einzelkomponenten und aus redundanten Komponenten ... 300

13.4 Abschließende Bemerkungen ... 304

14 Markov-Prozess 305

14.1 Fallbeispiel: Das Seilbahnunglück am Monte Mottarone ... 305

14.2 Theoretische Grundlagen ... 307
14.2.1 Zustände und Zustandswechsel ... 307
14.2.2 Übergangsratenmatrix ... 313

14.3 Markov-Prozess eines einfachen Systems ... 314

14.4 Markov-Prozess eines einfachen redundanten Systems ... 315

14.5 Markov-Prozess eines redundanten Systems mit entdeckbaren und nicht-entdeckbaren Ausfällen ... 317
14.6 Abschließende Bemerkungen ... 319

15 Markov Decision-Prozess 321

15.1 Fallbeispiel: Das Autopilotsystem des Tesla Model S ... 321
15.2 Einführung in den Markov Decision-Prozess ... 322
15.3 Grundlagen des MDP ... 324
15.4 Belohnungsfunktionen ... 329
15.5 Optimale Belohnungsfunktionen ... 331
15.5.1 Berechnung der Belohnungen über Iterationen ... 333
15.6 Ausflug in die künstliche Intelligenz ... 334
15.6.1 Neuronales Netz ... 335
15.6.2 Replay Memory ... 337
15.6.3 Algorithmus ... 338
15.7 Abschließende Bemerkungen ... 340

16 Reliability, Availability, Maintainability und Serviceability 341

16.1 Fallbeispiel: Das Kursk-Unglück ... 341
16.2 Das einfache System ... 342
16.2.1 Zuverlässigkeit des einfachen Systems ... 343
16.2.2 Verfügbarkeit des einfachen Systems ... 344
16.3 Das serielle System ... 346
16.3.1 Zuverlässigkeit des seriellen Systems ... 347
16.3.2 Verfügbarkeit des seriellen Systems ... 348
16.4 Das parallele System ... 349
16.4.1 Zuverlässigkeit des parallelen Systems ... 350
16.4.2 Verfügbarkeit des parallelen Systems ... 355
16.5 Die 1oo2-Architektur ... 356
16.5.1 Zuverlässigkeit der 1oo2-Architektur ... 357
16.5.2 Verfügbarkeit des 1oo2-Architektur ... 358

16.6 Bestimmung der PFDavg von unterschiedlichen Architekturen ... 358
16.6.1 PFDavg der 1oo2-Architektur ... 360
16.6.2 PFDavg der 2oo2-Architektur ... 362
16.6.3 PFDavg der 1oo3-Architektur ... 362
16.6.4 PFDavg der doon-Architektur ... 363

16.7 Abschließende Bemerkungen ... 364

17 Binary Decision Diagramms 367

17.1 Fallbeispiel: Permissive Action Link ... 367

17.2 Fehlerbäume und Zustandsräume ... 369

17.3 Binary Decision Diagrams über den shannonschen Zerlegungssatz ... 371
17.3.1 Der shannonsche Zerlegungssatz ... 374
17.3.2 Und-Gatter, Oder-Gatter und 2oo3-Architektur ... 374
17.3.3 Und-Gatter ... 374
17.3.4 Oder-Gatter ... 376
17.3.5 2oo3-Architektur ... 377

17.4 Aufbau von BDD aus Zustandsraum und Reduktion ... 379

17.5 Aufbau von BDD aus FT ... 382

17.6 Anwendung von BDD am Fallbeispiel ... 384

17.7 Abschließende Bemerkungen ... 385

Literaturverzeichnis ... 387
Index ... 395