Abb. 4.30 Bewachte Eingänge ... 104
Abb. 4.31 Verwaltungsfunktion ... 106
Abb. 4.32 Windows-2000-Architektur [Win2000] ... 109
Abb. 4.33 Microkernel-Architektur [Sta2003] ... 109
Abb. 4.34 Prozesszustände ... 110
Abb. 4.35 Ereigniswarteschlangen ... 111
Abb. 4.36 Prozesszustände ... 112
Abb. 4.37 Zeitgrößen eins Rechenprozesses ... 112
Abb. 4.38 Phasenlage zum Zeitpunkt Null bei Rate Monotonic Analysis (RMA) ... 114
Abb. 4.39 Phasenlagen und Ausführbarkeit ... 114
Abb. 4.40 Rate Monotonic Analysis mit Erweiterungen ... 115
Abb. 4.41 Rate Monotonic Scheduling (RMS) am Beispiel ... 115
Abb. 4.42 Earliest Deadline First (EDF) am Beispiel ... 116
Abb. 4.43 Least Laxity First (LLF) am Beispiel ... 117
Abb. 4.44 Wechselwirkung zweier Prozesse ... 118
Abb. 4.45 Prozessbeispiel ... 121
Abb. 4.46 Zeichnerische Lösung von RMS ... 123
Abb. 4.47 Zeitgrößen für EDF (Restantwortzeit RAZ) ... 124
Abb. 4.48 Least-Laxity-First-Beispiel ... 130
Abb. 4.49 Zugriff auf gemeinsame Daten ... 131
Abb. 4.50 Prioritätsinversion ... 131
Abb. 4.51 Unbounded Blocking ... 132
Abb. 4.52 Prioritätsvererbung ... 133
Abb. 4.53 Deadlock ... 133
Abb. 4.54 Ceiling-Priority-System ... 134
Abb. 4.55 Ressourcenzugriffe ... 135
Abb. 4.56 Ceiling-Prioritäten der Ressourcen ... 135
Abb. 4.57 Zusammenspiel im Beispiel bei PCP ... 136
Abb. 4.58 Beispiel mit Testnachweis ... 137
Abb. 4.59 Beispiel nach Optimierung ... 138
Abb. 4.60 Beispiel Taskset und Ressourcenverbund ... 139

Abb. 5.1 Syntaktischer Fehler in der IF-Anweisung ... 147
Abb. 5.2 Syntaktisch fehlerhafter logischer Vergleich ... 148
Abb. 5.3 Syntaktische Struktur der If-Anweisung von Ada ... 148
Abb. 5.4 Konvertierung in C ... 148
Abb. 5.5 Gleitpunktzahl als Schleifenvariable ... 148
Abb. 5.6 Inkonsistente Repräsentation von Aufzählungswerten ... 149
Abb. 5.7 Regel zur Erhöhung der Lesbarkeit [Loc2005] ... 150
Abb. 5.8 Syntaktische Struktur der IF-Anweisung in Ada ... 150
Abb. 5.9 Ergebnis statische Analyse [Gan2012] ... 151
Abb. 5.10 Einbettung von Ada ... 153
Abb. 5.11 Typsystem in Ada [Ada2012] ... 161
Abb. 5.12 Auslagerung zur Komplexitätsbeherrschung ... 163

Abb. 5.13 Benutzt-Beziehung 163
Abb. 5.14 Modul mit privatem Typ und verborgener Implementierung 164
Abb. 5.15 Hierarchisch-modulare Architektur in Ada 165
Abb. 5.16 Beispiel eines „protected type“ [Ben2009] 166
Abb. 5.17 Zeitlich begrenztes Warten auf einen Aufruf 168
Abb. 5.18 Selektive Aufrufannahme mit zeitlich begrenztem Warten 169
Abb. 5.19 Beispiel Use Case 172
Abb. 5.20 Sequenzdiagramm Tee 173
Abb. 5.21 Klassendiagramm 173
Abb. 5.22 Stereotype Task 174
Abb. 5.23 Vererbungshierarchie 174
Abb. 5.24 Zustandsautomat 175
Abb. 5.25 Transformationsvorgang 176
Abb. 5.26 Typdefinition für Ereignisannahme 176
Abb. 5.27 Benutzerdefinierte Programmbereiche 177
Abb. 5.28 Task-Zustände [Mat2013] 177
Abb. 5.29 Task-Entries 177
Abb. 5.30 Ablaufverhalten der Task 178
Abb. 5.31 Spezifikation einer statischen Typinvariante 179
Abb. 5.32 Spezifikation einer dynamischen Typinvariante 180
Abb. 5.33 Spezifikation von Default-Werten 180
Abb. 5.34 Spezifikation eines Stack-Typs 180
Abb. 5.35 Spezifikation zur Überprüfung der Wirkung von Push mit „Old“ 180

Abb. 6.1 Safety und IT-Security als zweiseitige Sicherheitsanforderung 186
Abb. 6.2 Risikobegriff [VDI2010] 189
Abb. 6.3 Redundanz und Funktionsdegradierung 189
Abb. 6.4 Safety Life Cycle [IEC2010] 191
Abb. 6.5 Safety Integrity Levels (nach [IEC1998]) 192
Abb. 6.6 Vorgehen und Entscheidungslogik zur Erzeugung von Sicherheit (Safety), vgl. [Kel2018]) 194
Abb. 6.7 Herausforderungen nach dem ZVEI [ZVEI2006] 196
Abb. 6.8 Funktionsebenen in der Security (vgl. auch [BSI2012]) 200
Abb. 6.9 Anzahl der Produkte in industriellen Bereichen mit Schwachstellen im Jahr 2017 („Number of vulnerable products used in different industries“, [Kas2018]) 202
Abb. 6.10 Angriffspunkte bei Windkraftanlagen nach [Rei2018] 203
Abb. 6.11 Verteilung der festgestellten Typen von Schwachstellen bei ICS-Systemen im Jahr 2017 („Most common vulnerability types“, [Kas2018]) 204
Abb. 6.12 Zeitliche Entwicklung der Schwachstellen „Execute Code“, „Buffer Overflow“ und „Memory Corruption“ bei ICS-Systemen [CVE2018] 205
Abb. 6.13 Zeitliche Entwicklung der entdeckten Schwachstellen bei ICS-Systemen [CVE2018] 205

Abb. 6.14 Schwachstellen bei SCADA-Systemen [NST2010] 206
Abb. 6.15 Beispielhaftes IT-Security-Konzept bei SCADA-Systemen [Sie2018] 207
Abb. 6.16 Ebenen in der semantischen Absicherung gegen Cyber-Angriffe im Smart Energy Grid (vgl. [Hag2016]) 208
Abb. 6.17 Diversität zur Manipulationsentdeckung [Ghe2011] 214
Abb. 6.18 Zertifizierte und offene Software 215
Abb. 6.19 Rückwirkungsfreie Schnittstelle über Stellvertreter 216
Abb. 6.20 Best Practices für Safety/Security [Ibr2004] 217
Abb. 6.21 Mathematische Definition einer Funktion mit definierter Eingabe- und Ausgabemenge 224
Abb. 6.22 Formale Definition einer Funktion entsprechend definierter Eingabemenge 224
Abb. 6.23 Nichtausschließliche Funktionsrealisierung mit zusätzlichen Freiheitsgraden 224
Abb. 6.24 Zeitliche Entwicklung der höchsten Kritikalität (grün) von Schwachstellen [NIST2018] 225
Abb. 6.25 Zeitliche Entwicklung von Schwachstellen im Detail [NIST2018] 226

Abb. 7.1 Beispielhafte LZP und Temperaturverlauf 232
Abb. 7.2 Vergleich gemessene/theoretische CTP eines binären Toluol-Ethanol-Gemisches 233
Abb. 7.3 Vergleich gemessene/theoretische CTP eines Nicht-Toluol-Ethanol-Gemisches 233
Abb. 7.4 Sensor als Hubsystem 234
Abb. 7.5 Tasks des Sensorsystems mit Zeitangaben 235
Abb. 7.6 Hubmagnetensteuerung 237
Abb. 7.7 Tasks des Sensorsystems mit Zeitangaben 238
Abb. 7.8 Sensorsystem mit Hubsensor und Rechnerplatine 238
Abb. 7.9 INSPECT-pro-control-System [Ker2001] 239
Abb. 7.10 Inspect-Komponenten 240
Abb. 7.11 Inspect-Benutzerschnittstellen 242
Abb. 7.12 Generierung von PSM aus PIM durch Transformation 243
Abb. 7.13 Profil für den MDA-Ansatz beim INSPECT-pro-control-System [Ker2001] 244
Abb. 7.14 Modellierter Zustandsautomat [Ker2001] 246
Abb. 7.15 Generiertes Schema für eine nebenläufige Task [Ker2001] 246
Abb. 7.16 Generierter Quelltext für Annahme von Entry-Aufrufen [Ker2001] 247

Tabellenverzeichnis

Tab. 1.1 Vergleich der Softwareumfänge und Fehlerraten in technischen Systemen (nach Tab. A.1) 4
Tab. 1.2 Erfolg bei Softwareprojekten [Stan2013] 6
Tab. 1.3 Kostenanteil von Elektronik [FAST2005] 10
Tab. 1.4 Typische Fehlerverteilung im Entwicklungsprozess [Linh2013] 12

Tab. 3.1 Funktionsbeispiel 67

Tab. 4.1 Beispielprozesse für LLF 128
Tab. 4.2 Laxity-Berechnung und LLF-Ausführung 129
Tab. 4.3 Vergleich EDF und RMA/RMS 142

Tab. 6.1 Expositionseinordnung 222
Tab. 6.2 Klassenfestlegung 223

Tab. 7.1 Tasks und geforderte Eigenschaften 236

Lizenz zum Wissen.

Sichern Sie sich umfassendes Technikwissen mit Sofortzugriff auf tausende Fachbücher und Fachzeitschriften aus den Bereichen: Automobiltechnik, Maschinenbau, Energie + Umwelt, E-Technik, Informatik + IT und Bauwesen.

Exklusiv für Leser von Springer-Fachbüchern: Testen Sie Springer für Professionals 30 Tage unverbindlich. Nutzen Sie dazu im Bestellverlauf Ihren persönlichen Aktionscode **C0005406** auf *www.springerprofessional.de/buchaktion/*

Jetzt 30 Tage testen!

Springer für Professionals.
Digitale Fachbibliothek. Themen-Scout. Knowledge-Manager.

- Zugriff auf tausende von Fachbüchern und Fachzeitschriften
- Selektion, Komprimierung und Verknüpfung relevanter Themen durch Fachredaktionen
- Tools zur persönlichen Wissensorganisation und Vernetzung

www.entschieden-intelligenter.de

Springer für Professionals

Springer