Inhaltsverzeichnis

1 Einleitung **1**

1.1 Beispiele für Auswirkungen von Fehlern 3
1.1.1 Selbstzerstörung der Ariane 5 3
1.1.2 Verlust der NASA-Sonde Mars Climate Orbiter 4
1.1.3 Bestrahlungsgerät Therac-25 4
1.1.4 Sicherheitslücke Heartbleed 5
1.2 Der Stand von Wissenschaft und Technik und dessen Nachteile . . . 6
1.2.1 Stand von Wissenschaft und Technik 6
1.2.2 Nachteile des Stands von Wissenschaft und Technik 7
1.3 Ziel der Arbeit 8
1.4 Ergebnisse der Arbeit 9
1.5 Aufbau der Arbeit 11
1.6 Darstellung von Zahlen und Speichergrößen in der Arbeit 13

2 Fehlerarten, -ursachen, -auswirkungen und -behandlung **14**

2.1 Fehlerkategorien 14
2.2 Fehlerquellen in Soft- und Hardware 15
2.3 Fehlerdichte in Software 19
2.4 Datenflussbezogene Fehler- und Angriffsarten 20
2.4.1 Inkompatibilität von Operanden 21
2.4.2 Wertebereichsverletzungen und Genauigkeitsprobleme 21
2.4.3 Fehlerhafte Operationen 22
2.4.4 Verletzung von Echtzeitbedingungen 23
2.4.5 Allgemeine Datenflussfehler 23
2.4.6 Datenverfälschung durch Fehler oder Störungen 25
2.4.7 Fehlerhafter Zugriff auf Daten 25
2.4.8 Hackerangriffe 26
2.4.9 Zusammenfassung der identifizierten datenflussbezogenen Fehler- und Angriffsarten 27
2.5 Auswirkungen von Fehlern 27
2.6 Fehlererkennung und -behandlung 30

2.6.1 Einnehmen und Halten eines sicheren Zustands 31
2.6.2 Anwendung von Redundanzmaßnahmen 31
2.6.3 Allmähliche Leistungsabsenkung 31

3 Stand von Wissenschaft und Technik **33**
3.1 Konventionelle Architekturen 34
3.1.1 Die x86-Architektur 34
3.1.2 Die ARM-Architektur 40
3.1.3 Integritätsprüfung durch ECC 41
3.1.4 Evaluation konventioneller Architekturen 42
3.2 Prozessoren für sicherheitsgerichtete Anwendungen 45
3.2.1 Aufbau der Prozessoren für sicherheitsgerichtete Anwendungen 45
3.2.2 Evaluation der Prozessoren für sicherheitsgerichtete Anwendungen 46
3.3 Datentyparchitekturen 49
3.3.1 Beispiele von Datentyparchitekturen 50
3.3.2 Evaluation der Datentyparchitekturen 52
3.4 Datenstruktur- bzw. Deskriptorarchitekturen 54
3.4.1 Beispiele von Datenstruktur- bzw. Deskriptorarchitekturen . 54
3.4.2 Evaluation der Datenstrukturarchitekturen 55
3.5 Befähigungsarchitekturen 55
3.5.1 Beispiele historischer Befähigungsarchitekturen 58
3.5.2 Beispiele moderner Befähigungsarchitekturen 60
3.5.3 Evaluation der Befähigungsarchitekturen 66
3.6 Datenflussarchitekturen 66
3.6.1 Funktionsweise von Datenflussarchitekturen 68
3.6.2 Evaluation von Datenflussarchitekturen 69
3.7 Die inhärent sichere Mikroprozessorarchitektur ISMA 71
3.7.1 Aufbau der Datenspeicherelemente in ISMA 71
3.7.2 Evaluation von ISMA 75
3.8 Application Data Integrity ADI bzw. Silicon Secured Memory SSM 77
3.8.1 Funktion von ADI bzw. SSM 77
3.8.2 Evaluation von ADI bzw. SSM 77
3.9 Dynamic Dataflow Verification DDFV 79
3.9.1 Funktion der dynamischen Datenflussprüfung 79
3.9.2 Evaluation der dynamischen Datenflussprüfung 80
3.10 Fehlererkennung durch AN(BD)-Kodierung 80
3.10.1 AN-Kodierung zur Integritätsprüfung von Datenspeicherelementen und arithmetischen Operationen 82

3.10.2 ANB-Kodierung: Hinzufügen der Adressprüfung B 84
3.10.3 ANBD-Kodierung: Hinzufügen der Aktualitätsprüfung D . . 86
3.10.4 Realisierung der AN(BD)-Kodierung 87
3.10.5 Evaluation der AN(BD)-Kodierung 87
3.11 Datenflussüberwachung in Netzwerken und sicherheitsgerichteten Feldbussen 91
3.11.1 Netzwerkprotokolle TCP/IP 91
3.11.2 Sicherheitsgerichtete Feldbusprotokolle 95
3.11.3 Evaluation der Datenflussüberwachung in Netzwerken und sicherheitsgerichteten Feldbussen 101
3.12 Zusammenfassung des Stands von Wissenschaft und Technik 104
3.12.1 Zusammenfassung der Fehlererkennungsmöglichkeiten 104
3.12.2 Zusammenfassende Kritik am Stand von Wissenschaft und Technik 108

4 Eine Datenspezifikationsarchitektur **111**
4.1 Systemaufbau und Fehlerbehandlung 112
4.1.1 Grundlegender Systemaufbau technischer Prozesse 112
4.1.2 Aufbau eines auf einer Datenspezifikationsarchitektur basierenden Systems 113
4.1.3 Fehlerbehandlung in einer Datenspezifikationsarchitektur . . 116
4.2 Sammlung relevanter Dateneigenschaften 119
4.3 Realisierung der Datenflussüberwachung 122
4.3.1 Einleitende Erläuterungen 122
4.3.2 Datenwert und dessen Genauigkeit 128
4.3.3 Wertebereich 140
4.3.4 Datentyp 148
4.3.5 Einheit 161
4.3.6 Zugriffsrechte und Initialisierungsstatus 175
4.3.7 Quelle, Verarbeitungsweg und Ziel 184
4.3.8 Zeitschritt 203
4.3.9 Frist 220
4.3.10 Zykluszeit 226
4.3.11 Integritätsprüfung und Adresse 239
4.3.12 Signatur und Adresse 244
4.3.13 Redundante diversitäre arithmetisch-logische Einheit 253
4.4 Übersicht der Kennungen in Daten- und Befehlsspeicherelementen . 257
4.5 Übersicht der speziellen Register 261
4.6 Pseudocode einer Instruktion 261

4.7 Anforderungen an die Systemkomponenten 272
4.7.1 Schnittstellen zu konventionellen Systemkomponenten 272
4.7.2 Hochpräzise synchronisierte Uhren 273
4.8 Konfiguration der Systemkomponenten 273
4.8.1 Konfiguration der Datenquellen 274
4.8.2 Konfiguration der Datenverarbeitungseinheiten 274
4.8.3 Konfiguration der Datensenken 276
4.8.4 Konfiguration der Systemüberwachungseinheit 277
4.8.5 Erkennung konfigurationsbezogener Inkonsistenzen 277
4.9 Anforderungen an Begutachtungen und Audits 278
4.10 Realisierung der Datenspezifikationsarchitektur als Datenflussarchitektur 279
4.10.1 Erweiterung der Funktionsblöcke um Lebenszeichen und Diagnose 280
4.10.2 Verbesserung der Fehlererkennung durch zusätzliche Erweiterungen 283
4.10.3 Weiterhin bestehende Einschränkungen 286

5 Evaluation der Datenspezifikationsarchitektur 287
5.1 Evaluation der Datenabbildung der DSA 287
5.2 Einordnung der entstandenen Architektur 290
5.3 Evaluation anhand der Fehlererkennungsmöglichkeiten 291
5.4 Evaluation anhand der Fehlerbeispiele 295
5.4.1 Selbstzerstörung der Ariane 5 295
5.4.2 Verlust der NASA-Sonde Mars Climate Orbiter 296
5.4.3 Bestrahlungsgerät Therac 25 296
5.4.4 Sicherheitslücke Heartbleed 296
5.5 Evaluation der Speicherausnutzung 298
5.5.1 Speicherausnutzung der Datenspeicherelemente 298
5.5.2 Speicherausnutzung der Befehlsspeicherelemente 301
5.5.3 Evaluation der Speicherausnutzung 304

6 Zusammenfassung und Weiterführungsmöglichkeiten 306
6.1 Zusammenfassung der Ergebnisse der Arbeit 306
6.2 Weiterführungsmöglichkeiten 308

Literaturverzeichnis 310