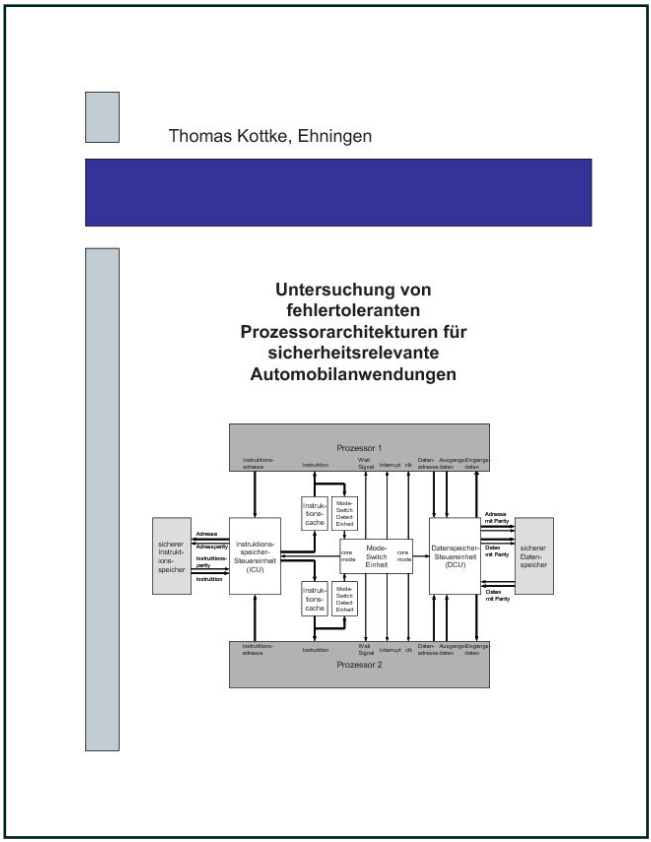
Thomas Kottke (Autor)

Untersuchung von fehlertoleranten Prozessorarchitekturen für sicherheitsrelevante Automobilanwendungen



https://cuvillier.de/de/shop/publications/2271

Copyright:
Cuvillier Verlag, Inhaberin Annette Jentzsch-Cuvillier, Nonnenstieg 8, 37075 Göttingen, Germany
Telefon: +49 (0)551 54724-0, E-Mail: info@cuvillier.de, Website: https://cuvillier.de

Inhaltsverzeichnis

Verwendete Abkürzungen und Symbole . . . xv

1 Einleitung **1**

2 Stand der Technik **3**
2.1 Fehlermodell . . . 3
2.2 Möglichkeiten zur Fehlerentdeckung . . . 4
2.2.1 Test . . . 5
2.2.2 Redundanz auf Prozessorebene . . . 6
2.2.3 Redundanz auf Prozessorkomponentenebene . . . 10

3 Sicherheitsanalyse **13**
3.1 Die theoretische Fehleranalyse . . . 13
3.2 Fehlerinjektion . . . 13
3.3 Testaufbau für die Fehlerinjektion . . . 17
3.3.1 Testumgebung für die Fehlerinjektion . . . 17
3.3.2 Einbau der Fehlerinjektoren . . . 18
3.3.3 Ansteuersoftware für die Fehlerinjektion . . . 19

4 Untersuchung der Prozessorarchitekturen **21**
4.1 Speicher . . . 22
4.1.1 Anforderungen . . . 22
4.1.2 Fehlerentdeckungsmechanismen für Speicherzellen . . . 25
4.1.3 Absicherung des Adressdecoders . . . 31
4.1.4 Zusammenfassung: . . . 37
4.2 Das generische Zweiprozessorsystem mit gemeinsamem Speicher . . . 39
4.2.1 Differenzierungsmerkmale zu bestehenden Zweiprozessorsystemen . . . 39
4.2.2 Funktionsweise und Implementierung des Zweiprozessorsystems . . . 40
4.2.3 Fehlerbehandlung . . . 45
4.2.4 Analyse der verbliebenen Einfachfehlerorte . . . 47
4.2.5 Fehlerinjektionsexperimente . . . 49
4.2.6 Erweiterung um eine Fehlerkapselung . . . 51
4.2.7 Fehlerinjektion bei dem Zweiprozessorsystem mit Fehlerkapselung . . . 54
4.2.8 Zusammenfassung des Zweiprozessorsystems . . . 56
4.3 Das rekonfigurierbare generische Zweiprozessorsystem . . . 57
4.3.1 Funktionsweise des rekonfigurierbaren Zweiprozessorsystems . . . 57
4.3.2 Implementierung des rekonfigurierbaren Zweiprozessorsystems . . . 60
4.3.3 Theoretische Fehleranalyse . . . 64

4.3.4 Performanzanalyse 70
4.3.5 Fehlerinjektionsexperimente 72
4.3.6 Ergebnisse der Fehlerinjektion 73
4.3.7 Zusammenfassung 75
4.4 Prozessor mit Eigenfehlererkennung 77
4.4.1 Funktionsweise und Implementierung des Prozessors mit Eigenfehlererkennung 77
4.4.2 Fehleranalyse der verbleibenden Single Points of Failure 82
4.4.3 Fehlerinjektion beim Rechner mit Eigenfehlererkennung 83
4.5 Befehlsdecoder mit Parity Prediction 84
4.5.1 Implementierung des Befehlsdecoders mit Parity Prediction 84
4.5.2 Fehlerinjektion bei dem Prozessor mit Eigenfehlererkennung mit einem durch Parity Prediction abgesicherten Befehlsdecoder 86
4.5.3 Zusammenfassung 86
4.6 Der rekonfigurierbare superskalare Prozessor 88
4.6.1 Funktionsweise des superskalaren Prozessors 88
4.6.2 Implementierung des superskalaren Prozessors 89
4.6.3 Theoretische Fehleranalyse 93
4.6.4 Performanzanalyse 96
4.6.5 Fehlerinjektionsexperimente 96
4.6.6 Zusammenfassung 99
4.7 Kontrollflußüberwachung 100
4.7.1 Implementierung der Kontrollflußüberwachung 101
4.7.2 Fehlerinjektionsexperimente 102
4.7.3 Zusammenfassung 103

5 Vergleich der Prozessorarchitekturen 104
5.1 Fehlerentdeckung 104
5.2 Fehlerkapselung 105
5.3 Kosten 105
5.3.1 Fläche 105
5.3.2 Entwicklungsaufwand 106
5.4 Performanz 107
5.5 Schlussfolgerungen 108

6 Zusammenfassung und Ausblick 110
6.1 Zusammenfassung 110
6.2 Ausblick 111

A Fehlererkennungs- und Fehlerkorrekturcodes 113
A.1 Hamming Distanz 113
A.2 Parity Code 113
A.3 Hamming Code 114
A.4 Residuen / Modulo Codes 115
A.5 Berger Code 115
A.6 Bose-Lin Code 116

B Fehlerinjektionsexperimente an Einzelkomponenten **117**

C Flächenbetrachtungen **119**
C.1 Gattergrößen nach der MOSIS-Bibliothek 119
C.2 Fläche der einzelnen Prozessoren 120
C.2.1 Fläche des Referenzprozessors SPEAR 120
C.2.2 Fläche des generischen Zweiprozessorsystems 120
C.2.3 Fläche des rekonfigurierbaren Zweiprozessorsystems 121
C.2.4 Fläche des Prozessors mit Eigenfehlererkennung 122
C.2.5 Fläche des rekonfigurierbaren superskalaren Prozessors 122

D Ergänzungen zum rekonfigurierbaren Zweiprozessorsystem **124**
D.1 Performanzanalyse des rekonfigurierbaren Zweiprozessorsystems 124
D.2 Zustandsautomaten des rekonfigurierbaren Zweiprozessorsystems 129

E Flächenkalkulation der Datenspeicherabsicherung **132**

Literaturverzeichnis **135**

Publikationsliste **145**

Lebenslauf **147**