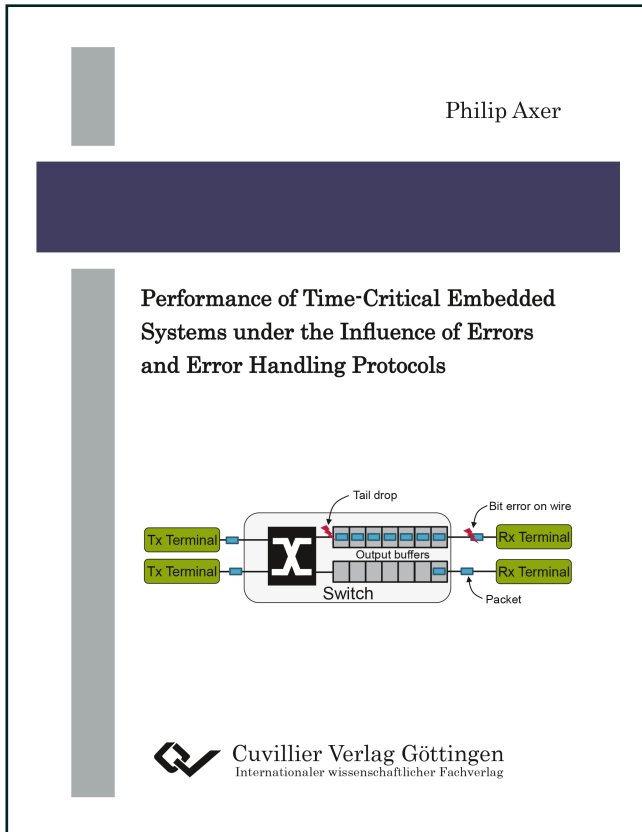




Philip Axer (Autor)

Performance of Time-Critical Embedded Systems under the Influence of Errors and Error Handling Protocols



<https://cuvillier.de/de/shop/publications/7185>

Copyright:

Cuvillier Verlag, Inhaberin Annette Jentsch-Cuvillier, Nonnenstieg 8, 37075 Göttingen, Germany

Telefon: +49 (0)551 54724-0, E-Mail: info@cuvillier.de, Website: <https://cuvillier.de>



Contents

1	Introduction	1
1.1	Motivation	1
1.2	The Role of Safety Standards	2
1.3	Development Process for Safety-Critical Systems	4
1.4	Trends	6
1.4.1	Architecture Complexity Challenge	6
1.4.2	Cyber-Physical Systems Challenge	9
1.4.3	System of Systems Challenge	9
1.4.4	Adaptability and Software Evolution Challenge	10
1.4.5	Resiliency Challenge	11
1.4.6	Mixed-Criticality Challenge	13
1.5	Integration and Verification of Mixed-Criticality Applications	14
1.6	Concepts of Dependable Computing	17
1.7	Summary and Contribution	19
1.8	Outline	20
2	Building Reliable Computer Systems	21
2.1	Traditional Fault-Tolerance Approaches	21
2.2	ASTEROID Approach	24
2.2.1	IDAMC Integrated Many-Core	27
2.2.2	Hardware-assisted State Comparison	30
2.3	Comparison and Performance Overview	33
2.4	Summary and Challenges of ASTEROID	35
3	Timing Verification of Safety-Critical Real-Time System	37
3.1	Related Work in System-Level Analyses	39



CONTENTS

3.2	System Model	40
3.2.1	Structural Model	40
3.2.2	Timing Model	42
3.3	Resource Analysis	45
3.3.1	Generalization and Formalism	46
3.3.2	Strict Priority Preemptive (SPP)	50
3.3.3	Strict Priority Non-Preemptive (SPNP)	51
3.3.4	First In - First Out (FIFO)	53
3.4	System Analysis	57
3.5	Summary	59
4	Multi-Master and Point-to-Point Communication	61
4.1	Channel Model	61
4.2	Error Models	63
4.2.1	Descriptive Parameters for Lossy Channels	64
4.2.2	Binary Symmetric Channel	66
4.2.3	Two State Gilbert Loss Model	69
4.3	Probabilistic Response-Time Analysis under Errors	71
4.3.1	Related Work	73
4.3.2	Busy-Period Fixed-Priority Arbitration	74
4.3.3	Busy-Period First-In First-Out Arbitration	78
4.3.4	Probability Computation	80
4.4	Convolution Analysis for Fixed-Priority Arbitration	85
4.4.1	Related Work	85
4.4.2	Stochastic Busy Window	89
4.4.3	Stochastic Queuing Delay and Response Time	95
4.5	Experiments	98
4.5.1	Controller Area Network	98
4.5.2	On-Chip Interconnect Arbitration	101
4.6	Summary	106
5	Switched Networks	109
5.1	Related Work	110
5.2	Error Control Protocols	111
5.2.1	Stop and Wait ARQ	111
5.2.2	Go-Back-N	112
5.3	Performance of Stop and Wait ARQ	114
5.3.1	ARQ Timing Model	114
5.3.2	Latency in the Error-Free Case	115
5.3.3	Stop and Wait Response Time	117
5.3.4	Timing Under Errors	119
5.4	Performance of Go-Back-N	121
5.4.1	Latency in the Error-Free Case	121
5.4.2	Timing under Errors	125



5.5	Experiments	127
5.5.1	Daisy Chain	127
5.5.2	Two Switches Automotive Setup	130
5.6	Summary	133
6	Multiprocessor on Chip	135
6.1	Error Detection and Recovery Model	136
6.1.1	Fault-Tolerant Tasks	136
6.1.2	Fork-Join Task Model	138
6.1.3	Failure Modes and Error Handling	141
6.2	Performance of Fork-Join Tasks	143
6.2.1	Related Work	143
6.2.2	Response-Time of Independent Tasks Under the Presence of Fork-Join Tasks	144
6.2.3	Response-Time of Fork-Join Tasks	148
6.2.4	Worst-Case Timing Evaluation of Replication	152
6.3	Reliability Prediction of Replication	155
6.3.1	Related Work	156
6.3.2	Error Model and Metrics	157
6.3.3	Formal Reliability Analysis	159
6.3.4	Experiments	165
6.4	Summary	168
7	Conclusion	171
A	Publications	175
A.1	Related to the Thesis	175
A.1.1	Reviewed	175
A.1.2	Unreviewed	177
A.2	Unrelated to the Thesis	177
	Bibliography	181