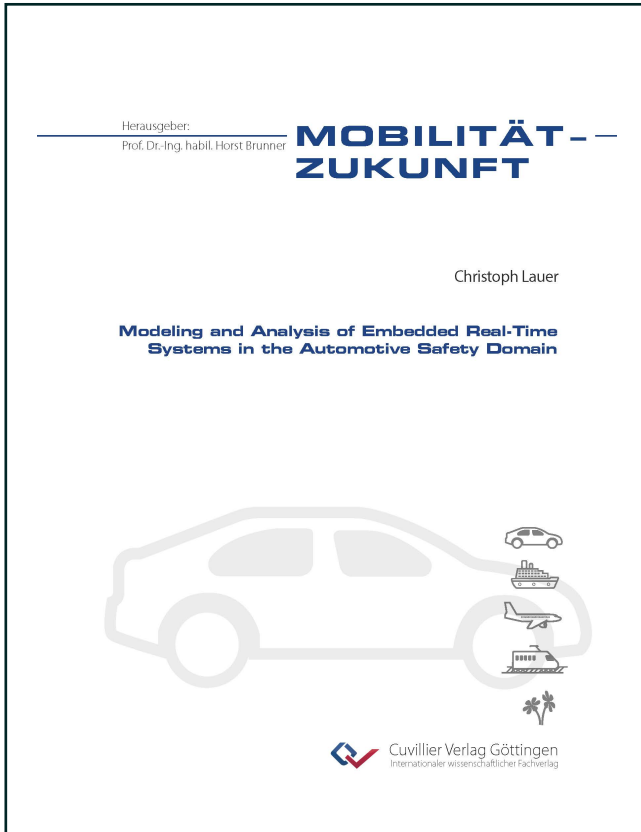




Christoph Lauer (Autor)
**Modeling and Analysis of Embedded Real-Time
Systems in the Automotive Safety Domain**



<https://cuvillier.de/de/shop/publications/8847>

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

Abstract	v
Zusammenfassung	vii
Contents	xiii
1 Introduction	3
1.1 Trends in Automotive Safety Engineering	4
1.2 Technological Trends in Safety Electronics	6
1.3 Model Based Analysis	8
2 Modeling Scope and Research Question	11
2.1 Research Question	13
2.2 Modeling and Analysis Approaches	14
2.2.1 Environment Perception Architectures Analysis	14
2.2.2 Dependability Analysis	16
2.2.3 Real-Time Analysis on process level	17
2.2.4 Real-Time Analysis on system level	19
3 Analysis of Environment Perception Architectures	21
3.1 Background and Related Work	22
3.2 Modeling and Simulation of Multi-Sensor Data Fusion Ar- chitectures	24
3.2.1 Simulation Model	24
3.2.2 Scenario Selection	28
3.3 Output Analysis	31
3.3.1 Simulation Control	31



CONTENTS

3.3.2	Simulation Measures	33
3.3.3	Findings	35
3.4	Analysis and Conclusions	41
4	Model-Based Fault Tree Analysis	45
4.1	Background and Related Work	46
4.2	System Meta Model	49
4.2.1	Architecture Modeling	49
4.2.2	Application Modeling	50
4.2.3	Fault Modeling	51
4.3	Fault Tree Synthesis	51
4.3.1	Simple Fault Propagation	52
4.3.2	Application Specific Fault Detection	54
4.3.3	Architecture Specific Fault Detection	55
4.3.4	Transformation Algorithm	56
4.4	Output Analysis	61
4.4.1	System Architecture	61
4.4.2	Sample Applications	61
4.4.3	Output Analysis	62
4.5	Future Work	65
4.6	Analysis and Conclusions	66
5	Formal Analysis of Real-Time Behavior	69
5.1	Related Work	70
5.1.1	Real-time Analysis on Process Level	71
5.1.2	Traditional Scheduling Approaches	71
5.1.3	Event-Stream Model Based Response-Time Analysis	77
5.1.4	Busy-window Based	80
5.1.5	Discussion	81
5.2	Response-Time Analysis Foundations	83
5.2.1	Computational Model	83
5.2.2	Analysis Using Offset Information	83
5.2.3	Feasibility in general terms and automotive specific	86
5.3	Application in Complex Automotive Systems	87



5.3.1	Response-Time Analysis for Single-clock reference . . .	87
5.3.2	Response-Time Analysis for Multiple-clock references	89
5.4	Application to a Real-World System	92
5.4.1	System Design	92
5.4.2	System Model	94
5.4.3	Analysis Results	95
5.4.4	Visualization of the Critical Instant	96
5.5	Computational Workload	97
5.6	Summary and Conclusions	100
6	Simulation of Real-Time Behavior	103
6.1	Related Work	104
6.2	Simulation of Timing Attributes	106
6.3	Simulation Model	107
6.3.1	Controller and Operating System Model	107
6.3.2	Communication Channel Model	110
6.3.3	End-to-End Delay of Distributed Applications	111
6.4	Simulation Control	113
6.5	Average-Case Analysis of a Real-World Example	116
6.6	Summary and Conclusions	122
7	Results	125
7.1	Environment Perception Strategy	125
7.1.1	Fusion Architectures	126
7.1.2	Layout of a Proactive Safety Application	126
7.2	Virtual integration	127
7.2.1	Proactive Algorithm Layout	127
7.2.2	Application Integration and Synchronization	128
7.2.3	Gateway function	129
7.3	Functional Safety	129
8	Conclusions and Outlook	131
	Bibliography	139