

OTTO-VON-GUERICKE-UNIVERSITÄT MAGDEBURG



OTTO VON GUERICKE
UNIVERSITÄT
MAGDEBURG

INF

FAKULTÄT FÜR
INFORMATIK

Qualitative and Quantitative Formal Model-Based Safety Analysis

– Push the Safety Button –

Dissertation

zur Erlangung des akademischen Grades
Doktoringenieur (Dr.-Ing.)

angenommen durch die Fakultät für Informatik
der Otto-von-Guericke-Universität Magdeburg

von: DIPL.-INF. MATTHIAS GÜDEMANN
geb. am 11.06.1980 in Augsburg

Gutachter:

Jun.-Prof. Dr. Frank Ortmeier
Prof. Dr. Jean-Jacques Lesage
Prof. Dr. Rudolf Kruse

Ort und Datum des Promotionskolloquiums: Magdeburg, 29.09.2011

Contents

1. Introduction	1
1.1. Main Contribution	3
1.2. Outline of the Dissertation	4
2. Safety Analysis Overview	5
2.1. Motivation and Concepts	6
2.2. Structured Approaches	8
2.2.1. Fault Tree Analysis	8
2.2.2. Failure Modes And Effects Analysis	9
2.2.3. Why-Because Analysis	10
2.2.4. System-Theoretic Analysis Model and Processes	11
2.3. Failure Logic Modeling	11
2.3.1. Failure Propagation and Transformation Notation	12
2.3.2. Hierarchically Performed Hazard Origin and Propagation Studies	12
2.3.3. AltaRica	13
2.4. Failure-Injection Based Analysis Techniques	13
2.4.1. ESACS and ISAAC Project	14
2.4.2. COMPASS Project	14
2.4.3. AVACS Project	15
2.5. Formal Model-Based Safety Analysis	15
3. Formal Basics	19
3.1. Motivation	20
3.2. Syntax of the Formal Models	21
3.3. Semantics of the Formal Models	25
3.3.1. Parallel Composition	26
3.3.2. Quantitative Formal Models	28
3.3.3. Qualitative Formal Model	36
3.4. Temporal Logics	40
3.4.1. Syntax and Semantics of CTL*	40
3.4.2. Syntax and Semantics of PCTL	42
3.5. Graphical Representation of SAML Models	44
3.6. Related Work	45

4. SAML Modeling for Safety Analysis	49
4.1. Motivation	50
4.2. Example Case Study	51
4.3. Hardware and Software Modeling	52
4.3.1. Software Modeling	52
4.3.2. Hardware Modeling	53
4.3.3. Case Study Model	53
4.4. Physical Environment Modeling	54
4.4.1. Temporal Resolution	54
4.4.2. Case Study Model	55
4.5. Failure Mode Modeling	55
4.5.1. Qualitative Formal Failure Modeling	56
4.5.2. Quantitative Failure Mode Modeling	57
4.5.3. Failure Effect Modeling	65
4.6. Related Work	70
5. Formal Safety Analysis	73
5.1. Motivation	74
5.2. Qualitative Model-Based Safety Analysis	75
5.2.1. Deductive Cause Consequence Analysis	75
5.2.2. Ordered Minimal Critical Sets	77
5.2.3. Adaptive DCCA	81
5.3. Quantitative Model-Based Safety Analysis	86
5.3.1. Probabilistic DCCA	86
5.3.2. Probabilistic DCCA for Reactive Systems	88
5.3.3. Adaptive pDCCA	88
5.4. Related Work	93
6. Transformation and Analysis of SAML Models	97
6.1. Motivation	98
6.2. Implementation of Transformations	99
6.3. Transformation for Quantitative Analysis	100
6.3.1. Example Transformation	100
6.3.2. Transformation to PRISM	102
6.4. Transformation for Qualitative Analysis	104
6.4.1. Example Transformation	105
6.4.2. Formal Transformation	109
6.4.3. Transformation to NuSMV	116
6.5. Related Work	118

7. Case Studies	121
7.1. Radio-Based Railroad Control	122
7.1.1. Description	122
7.1.2. Modeling	123
7.1.3. Results	133
7.2. Hot Spare Backup System	136
7.2.1. Description	136
7.2.2. Modeling	137
7.2.3. Results	139
7.3. Self-Adaptive Production Cell	142
7.3.1. Restore Invariant Approach	142
7.3.2. Description of the Case Study	143
7.3.3. Modeling	145
7.3.4. Results	156
7.4. Related Work	158
8. Conclusion And Outlook	161
8.1. Summary and Conclusion	162
8.1.1. Summary	162
8.1.2. Conclusion	163
8.2. Outlook	164
A. Proofs	167
B. Peer-Reviewed Publications	177