Contents

1 Introduction 1

1.1 Motivation . . . 1

1.2 Background and state of the art . . . 3

1.3 Novel contributions . . . 15

1.4 Organization . . . 16

2 Safety-related Systems (SRSs) 19

2.1 Preliminaries . . . 19

2.2 Failure . . . 21

2.2.1 Definition . . . 21

2.2.2 Random hardware failure vs. systematic failure . . . 21

2.2.3 Failure modes . . . 24

2.3 Maintenance . . . 28

2.3.1 Preliminaries . . . 28

2.3.2 Corrective maintenance . . . 29

2.3.3 Preventive maintenance . . . 30

2.4 Figures of merit . . . 32

2.4.1 Preliminaries . . . 32

2.4.2 Reliability and frequency of a dangerous failure (PFH) . . . 32

2.4.3 Availability and probability of dangerous failure on demand (PFD) 33

3 Modeling via Stochastic and Deterministic Timed Automata (SDTAs) 37

3.1 Preliminaries . . . 37

3.2 SDTA definition . . . 38

3.2.1 Preliminaries . . . 38

3.2.2 Deterministic timed events . . . 38

3.2.3 Exponential stochastic timed events . . . 39

3.2.4 Model of an SRS . . . 40

3.3 Procedure to model SRS with multiple elements . . . 47

3.3.1 Preliminaries . . . 47

3.3.2 The SRS element . . . 47

3.3.3 Parallel composition 50
3.3.4 Dependent SRS elements 51
3.3.5 SRS elements with common-cause failures 52
3.4 Discussion on SDTAs 54

4 Probabilistic evaluation of the SDTAs via Multi-phase Continuous-time Markov Chains (MP-CMCs) 57
4.1 Preliminaries 57
4.2 MP-CMC definition 57
4.3 SDTA transformation into MP-CMC 61
4.4 Preventive maintenance (PM) plans and strategies 65
4.4.1 Preliminaries 65
4.4.2 Definition of PM plan 65
4.4.3 Restrictions on PM plans 65
4.4.4 Definition of PM strategies 68

5 Model analysis and validation 71
5.1 Preliminaries 71
5.2 Analyzed models 71
5.2.1 Preliminaries 71
5.2.2 One element model 73
5.2.3 Three element model 75
5.2.4 Results 76
5.3 Validation 78
5.3.1 Preliminaries 78
5.3.2 Model of Torres-Echeverría et al. 78
5.3.3 Model of Brissaud et al. 79
5.3.4 Model of IEC 61508 80
5.3.5 Results 80
5.4 Sensitivity analysis 86
5.4.1 Preliminaries 86
5.4.2 Theoretical framework 86
5.4.3 Results 88

6 Optimization of preventive maintenance plans 93
6.1 Preliminaries 93
6.2 Optimization problems 93
6.3 Optimization algorithm 94
6.3.1 Preliminaries 94
6.3.2 Nelder-Mead method 95

6.4 Heuristic approach to minimize the maximum PFD 98
6.5 Results 100
6.5.1 Preliminaries 100
6.5.2 Models without redundancy 102
6.5.3 Models with redundancy 106
6.5.4 Models with redundancy and common-cause failures 110
6.6 General conclusions 113

7 Summaries **117**
7.1 Summary in English 117
7.2 Outlook 118
7.3 Extended summary in German – Kurzfassung in deutscher Sprache 119

A Model of SRS element with reduced number of states **123**

B State classification of selected *MooN* element structures **127**

C Models of selected dependent SRS elements **129**

D Nomenclature **133**

Bibliography **141**

About the author **145**