

# Contents

Foreword . . . . .	v
Acknowledgments . . . . .	vii
List of Publications . . . . .	viii
Abstract (English) . . . . .	ix
Kurzzusammenfassung (Deutsch) . . . . .	ix
<b>1 Introduction</b>	<b>1</b>
1.1 Practical application scenarios . . . . .	3
1.2 Hypothesis . . . . .	4
1.3 Structure . . . . .	4
<b>2 System, environment and transition model</b>	<b>5</b>
2.1 System model . . . . .	5
2.2 Probabilistic influence . . . . .	7
2.2.1 Fault model . . . . .	8
2.2.2 Execution semantics and scheduling . . . . .	11
2.3 Execution traces . . . . .	13
2.4 From system model to transition model . . . . .	14
2.5 Example - traffic lights . . . . .	16
2.6 Summarizing the system model . . . . .	22
<b>3 Fault tolerance terminology and taxonomy</b>	<b>23</b>
3.1 Definitions . . . . .	24
3.1.1 Safety . . . . .	26
3.1.2 Fairness . . . . .	26
3.1.3 Liveness . . . . .	28
3.1.4 Threats . . . . .	29

3.1.5	Types and means of fault tolerance . . . . .	31
3.1.6	Fault tolerance measures . . . . .	32
3.1.7	Redundancy . . . . .	34
3.2	Self-stabilization . . . . .	34
3.3	Design for masking fault tolerance . . . . .	36
3.4	Fault tolerance configurations . . . . .	38
3.5	Unmasking fault tolerance . . . . .	40
3.6	Summarizing terminology and taxonomy . . . . .	42
<b>4</b>	<b>Limiting window availability</b>	<b>43</b>
4.1	Defining limiting window availability . . . . .	44
4.1.1	LWA vector . . . . .	46
4.1.2	LWA vector gradient . . . . .	47
4.1.3	Instantaneous window availability . . . . .	47
4.2	Computing limiting window availability . . . . .	49
4.3	Examples . . . . .	49
4.3.1	Motivational example . . . . .	49
4.3.2	Self-stabilizing traffic lights algorithm (TLA) . . . . .	50
4.3.3	Self-stabilizing broadcast algorithm (BASS) . . . . .	54
4.4	Comparing solutions . . . . .	60
4.5	Summarizing LWA . . . . .	60
<b>5</b>	<b>Lumping transition models of non-masking fault tolerant systems</b>	<b>61</b>
5.1	Equivalence classes . . . . .	63
5.2	Ensuring probabilistic bisimilarity . . . . .	64
5.3	Example . . . . .	69
5.4	Approximate bisimilarity . . . . .	70
5.5	Summarizing lumping . . . . .	71
<b>6</b>	<b>Decomposing hierarchical systems</b>	<b>73</b>
6.1	Hierarchy in self-stabilizing systems . . . . .	79
6.2	Extended notation . . . . .	81
6.3	Decomposition guidelines . . . . .	89
6.4	Probabilistic bisimilarity vs. decomposition . . . . .	91

6.5	BASS Example . . . . .	92
6.5.1	Composition method in detail . . . . .	94
6.5.2	Example interpretation . . . . .	99
6.6	Decomposability - A matter of hierarchy . . . . .	101
6.6.1	Classes of semi-hierarchical systems . . . . .	102
6.6.2	Temporal semi-hierarchy and topological symmetry . . . . .	104
6.6.3	Mixed mode heterarchy . . . . .	104
6.7	Summarizing decomposition . . . . .	104
<b>7</b>	<b>Case studies</b>	<b>105</b>
7.1	Thermostatically controlled loads in a power grid . . . . .	105
7.2	A semi-hierarchical, semi-parallel stochastic sensor network . . . . .	121
7.3	Summarizing the case studies . . . . .	128
<b>8</b>	<b>Conclusion</b>	<b>129</b>
	<b>Bibliography</b>	<b>133</b>
	<b>List of figures</b>	<b>145</b>
	<b>Appendix</b>	<b>147</b>
<b>A</b>	<b>Appendix</b>	<b>149</b>
A.1	Employed resources . . . . .	149
A.2	List of abbreviations . . . . .	149
A.3	Table of notation . . . . .	150
A.4	Definitions . . . . .	151
A.4.1	Fault tolerance trees . . . . .	151
A.4.2	Fault tolerance . . . . .	153
A.4.3	Safety . . . . .	154
A.4.4	Fairness . . . . .	155
A.4.5	Liveness . . . . .	156
A.4.6	Threats to system safety . . . . .	157
A.4.7	Availability . . . . .	157
A.4.8	Reliability . . . . .	158

---

A.5	Source code . . . . .	160
A.5.1	Simulation . . . . .	160
A.5.2	The BASS example . . . . .	160
A.5.3	The power grid example . . . . .	162
A.5.4	The WSN example . . . . .	163
A.5.5	Counterexample for the double-stroke alphabet . . . . .	164
A.5.6	MatLab source code: Computing the LWA for the TLA example .	165
A.5.7	iSat source code: Callaway's TCL example without noise . . . . .	166