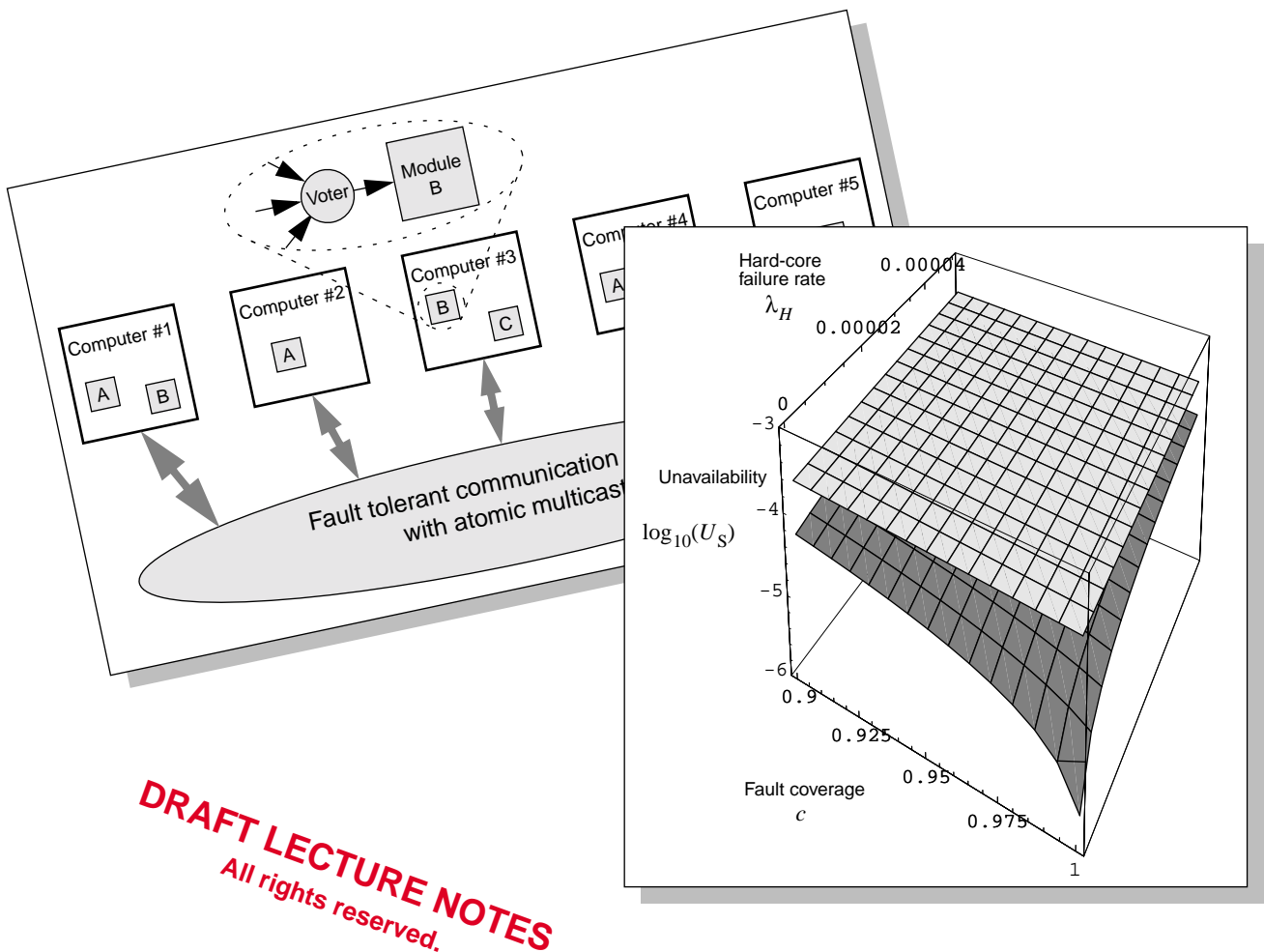


Dependable Computing Systems and Communication Networks

Design and Evaluation



Bjarne E. Helvik

Department of Telematics, NTNU
19. January 2001

Table of Content

1	Basics	1
1.1	Introduction	1
1.1.1	Definition	1
1.1.2	Dependability notions	2
1.1.3	Why bother about the dependability	2
1.1.4	Service and system	4
1.2	Fault, errors and failures	7
1.2.1	Types of faults	9
1.2.2	Fault - error - failure pathology	12
1.2.3	Failure modes and semantics	13
1.3	The failure process	16
1.3.1	The first failure	16
1.3.2	Examples	19
1.3.3	Failure intensity.	24
1.4	Dependability attributes	28
1.4.1	Reliability	29
1.4.2	Availability	31
1.4.3	Safety	33
1.5	Approaches to dependable systems	34
1.6	Restoration of service, maintenance	37
1.6.1	Maintenance and repair	38
1.6.2	Reload and restart	45
1.7	Simple dependability models	46
1.7.1	Markov models of a non fault-tolerant system	47
1.7.2	System structure - Reliability block diagrams	52
1.8	Comments	66
1.8.1	Concept and terminology	66
1.8.2	Failure statistics of some systems	66
2	Fault-tolerance	71
2.1	Basic types of redundancy	71
2.2	Modular redundancy	72
2.2.1	Principle	72
2.2.2	Reliability of TMR and NMR systems without repair	74
2.2.3	TMR simplex	76
2.2.4	Reliability of a TMR system with repair	77
2.2.5	The number of modules needed	79
2.2.6	Multistage TMR systems	80
2.2.7	When to use modular redundancy	83

2.3	Stand-by redundancy	84
2.3.1	Principle	84
2.3.2	Cold and lukewarm standbys	85
2.3.3	Synchronous systems and hot standbys	89
2.3.4	Loadshared systems	99
2.4	Information redundancy	105
2.5	Time redundancy	105
2.6	Other forms of redundancy	106
2.7	Building fault tolerant systems	106
2.7.1	Fault and error handling	106
2.7.2	Ensuring consistency	107
2.7.3	layered FT architecture	107
2.7.4	The design, modelling and analysis cycle	107
2.8	Software fault tolerance	109
3	Prediction of hardware failure rates	110
3.1	Phases in a component's life	111
3.1.1	The bathtub curve	111
3.1.2	Burn in	115
3.2	Prediction models	115
3.2.1	Models for assembled units	118
3.3	Factors influencing the failure rate	118
3.3.1	Complexity and technology	118
3.3.2	Temperature	120
3.3.3	Quality and learning	123
3.3.4	Voltage	124
3.3.5	Environment	125
4	Modelling of software dependability	127
4.1	The software failure process	127
4.1.1	Software with completed execution	128
4.1.2	Continuously operating software	131
4.2	Software as system elements	134
4.2.1	Dependence on the environment	135
4.2.2	Error persistence and propagation	135
4.2.3	Tolerance of design faults by change of conditions	142
4.3	Software and development process metrics	145
4.3.1	Software metrics	148
4.3.2	Development process metrics	153
4.3.3	Closing remarks	160
4.4	Software reliability growth models	162

4.4.1	Duane model	164
4.4.2	Musa's model	168
4.4.3	Littlewood-Verall model	175
4.4.4	Other models	182
4.4.5	Concluding remarks	182
5	Network dependability	183
5.1	Topologies	184
5.2	Network dependability modelling	188
5.2.1	Network failure modes	188
5.2.2	What is the dependability of a network?	190
5.2.3	Connectivity models	190
5.2.4	Capacity models	192
5.3	Studying reduced failure sets 198	
5.4	Redundancy strategies	200
5.4.1	Protection	201
5.4.2	Reconfiguration	202
5.4.3	Self-healing	203
5.4.4	Service restoration in layered networks	216
	References	222
	Appendix A Notation	228
A.1	Acronyms and abbreviations	228
A.2	Mathematical	229
	Appendix B ITU-T E.800 terms and concepts	230
	Appendix C Dependability modelling and analysis; Basic considerations	232
C.1	Introduction	232
C.2	Dependability modelling framework	232
C.2.1	Results	233
C.2.2	Activities	233
C.3	Models	234
C.4	Quantitative analysis	236
C.5	Common mistakes	237