

Contents

1	Introduction	1
1.1	Motivation	1
1.2	Management Summary	2
1.3	Scope and Methodology	3
2	Safety Assessment	5
2.1	Terms and Definitions	6
2.2	Mathematical Foundations	8
2.3	Methods and Techniques	9
2.3.1	Failure Mode and Effects Analysis	10
2.3.2	Hazard and Operability Study	11
2.3.3	Preliminary Hazard Analysis	12
2.3.4	Cause Effect Diagrams	13
2.3.5	Markov Chains	14
2.3.6	Petri Nets	15
2.3.7	Fault Trees	16
2.3.8	Reliability Block Diagrams	20
2.3.9	Event Trees	21
2.3.10	Cause Consequence Analysis	22
2.3.11	Goal Structuring Notation	23
3	Software Fault Tolerance	25
3.1	Fault Tolerant Systems	26
3.1.1	Error Recovery	27
3.1.2	Redundancy	28
3.2	Software Fault Tolerance Mechanisms	29
3.2.1	N-Version Programming	29
3.2.2	N-Copy Programming	31
3.2.3	Two-Pass Adjudicators	32
3.2.4	Recovery Blocks	33
3.2.5	Retry Blocks	35
3.2.6	Consensus Recovery Blocks	36
3.2.7	Acceptance Voting	37
3.2.8	Distributed Recovery Blocks	38
3.2.9	N-Self Checking Programming	40

3.3	Adjudicators	41
3.3.1	Acceptance Tests	41
3.3.2	Voting	42
3.4	Safety Analysis of Software Fault Tolerance Mechanisms	43
4	Worst-Case Execution Time Analysis	53
4.1	Overview of Timing Analysis Techniques	55
4.2	Techniques of WCET Estimation	56
4.3	Static WCET Analysis	57
4.4	Measurement-Based WCET Analysis	58
4.5	Probabilistic Approaches	58
5	Failure-Dependent Timing Analysis - Meta-Models and Basic Principles	67
5.1	Generic Component Meta-Model	67
5.2	Component Fault Tree Analysis Meta-Model	70
5.3	Failure-Dependent Timing Analysis Meta-Model	74
5.4	Analysis Formalism	76
6	Failure-Dependent Timing Analysis - Methods and Tools	83
6.1	Tool Architecture	83
6.2	Requirements and Settings	85
6.3	Import of .mdl Files	86
6.4	Safety Analysis in Enterprise Architect	96
6.5	The Failure-Dependent Timing Analysis Diagram	108
6.6	Variant Analysis	111
6.7	Failure Injection	112
6.8	Real Time Workshop and Compiler	120
6.9	Worst-Case Execution Time Analysis	120
6.10	Extraction of Probabilities	122
6.11	Representation of Results	123
7	Conclusion and Future Work	127
	Literature	129
	Appendix	138
A	Generated Fault Trees	139
A.1	Generated Fault Trees for Variants	139
A.2	Generated Fault Trees for Measure Points	147