# Contents

Abstract

List of figures

List of tables

List of equations

List of acronyms

I The context 0

1 Introduction 1

  1.1 Background 1

  1.2 The problem statement 2

  1.2.1 Research questions 2

  1.3 Motivation 2

  1.4 Software in safety-critical systems 5

  1.5 Software in nuclear reactors 6

  1.6 Software failures in nuclear industry 6

  1.7 Issues in software reliability quantification 7

  1.8 Need for a new approach 8

  1.9 This thesis 9

  1.9.1 Assumptions and limitations 9

  1.9.2 Structure 11
## Contents

2  Related work 13
   2.1  In formal methods ................................. 13
   2.2  In model checking ................................. 18
   2.3  In safety-critical software development, V&V .......... 19
   2.4  In software testing and test coverage .................. 20
   2.5  In mutation testing and test adequacy ................. 23
   2.6  In software reliability growth models (SRGM) .......... 26
   2.7  In Bayesian belief network ......................... 27
   2.8  In architecture based approaches ..................... 27
   2.9  Summary ........................................... 31

3  Background information 32
   3.1  Instrumentation and control in nuclear reactors .......... 32
   3.2  Case studies used in the present study ................. 34
      3.2.1  Fresh subassembly handling system ............... 34
      3.2.2  Reactor start-up system ........................ 35
      3.2.3  Steam generator tube leak detection system .......... 35
      3.2.4  Core temperature monitoring system............... 36
      3.2.5  Radioactive gaseous effluent system ................ 37
      3.2.6  Safety grade decay heat removal system ............. 39

II  Studies on software reliability 40

4  Research methodology 41
   4.1  Software reliability definition ...................... 41
   4.2  Choice of case-studies .............................. 42
   4.3  Method ............................................ 42
   4.4  Experimental details ............................... 43
      4.4.1  Software under test ........................... 43
      4.4.2  Software testing ............................... 44
      4.4.3  Parallel processing ............................. 44
6.3.1 Factors affecting the estimated reliability .................. 81
6.3.2 Achieving target reliability ........................................... 81
6.3.3 Properties of the software ........................................... 82
6.4 Results, discussions, and critical review ......................... 83
6.5 Summary of results ..................................................... 85

7 Some properties of software reliability .......................... 86
  7.1 Software reliability vs. number of faults in the software .... 86
  7.2 Software reliability vs. results of static, dynamic analysis .. 87
  7.3 Software reliability vs. safety ................................... 93
  7.4 Summary of results ................................................... 94

8 Summary and open problems ........................................ 96
  8.1 Contributions .......................................................... 96
  8.2 Observations ........................................................... 97
  8.3 Open problems ........................................................ 98
  8.4 Conclusion ............................................................. 99

III Appendices ............................................................ 100

A Semi-formal software specification .............................. 101
  A.1 List of Drakon notations ............................................. 101
  A.2 An example of semi-formal specification ..................... 103

B List of mutant operators .............................................. 109

C Data for PCA of mutant characteristics ........................ 111

References ................................................................. 121

Figure citations .......................................................... 137