STATISTICAL ESTIMATION OF THE UNAVAILABILITY OF THE MNR SAFETY AMPLIFIER

By

IMRE VENCEL

A Thesis

Submitted to the School of Graduate Studies

in Partial Fulfillment of the Requirements

for the Degree

Master of Engineering

McMaster University

© Copyright by Imre Vencel, May 2000

MASTER OF ENGINEERING (1999)
(Engineering Physics)

McMaster University
Hamilton, Ontario

TITLE: Statistical Estimation of the Unavailability of the MNR Safety Amplifier

AUTHOR: Imre Vencel, B.Sc. (Belgrade University)

SUPERVISOR: Professor Wm. J. Garland

NUMBER OF PAGES: xii, 161

ABSTRACT

Unavailability of the McMaster Nuclear Reactor (MNR) Safety Amplifier is calculated and showed to be within acceptable limits. Treated as a system of moderate complexity, the MNR Safety Amplifier reliability parameters are studied in detail utilizing a fault tree technique. This technique is recommended by IAEA and widely adopted in nuclear engineering as a main route for performing probabilistic risk assessment. A fault tree is developed and reliability parameters are calculated using a commercial software application FaultTree+™. Component failure data were collected from IAEA technical documents or other reliable sources when available. Uncertainty and importance analyses have been performed. In addition to the failure rates obtained from external documents, the Safety Amplifier checkout procedures were incorporated into the effective repair rates, thus forming the complete model for the basic events of the fault tree. The cut-set analysis methodology was utilized in order to assure that the final results would be reasonably biased, i.e. conservative enough. For the same reason, only the reliability data with established bounds of confidence were used. The resulting reliability parameters indicate that the failures of the Safety Amplifier caused by external means may be much more frequent than those caused by random failures of the individual components.

™ FaultTree+ is a trademark of Isograph Ltd.

ACKNOWLEDGEMENTS

Many people have helped me in one way or another in the preparation of this thesis. I wish to thank my supervisor, William J. Garland, for his much-valued critical readings and constant support during the writing of this thesis. My thanks go also to my colleges Simon Day, John Kennedy, and Robert Pasuta, for their comments and constructive suggestions. Special thanks go to my parents, without whose continued encouragement and support this work would have never been completed.

I want to express my appreciation for the financial support provided by the Engineering Physics Department and School of Graduate Studies at McMaster University. Also, I am grateful for the financial support provided by the Ontario Ministry of Education and Training Student Opportunity Trust Funds Program. This financial support came from the funds established by family, friends and colleagues of Robert John Morris.

Contents

Introduction …………………………………………………………………………..1

Chapter 1. MNR Safety Amplifier Decomposition

1.1. Introduction to Fault Tree Analysis ………………………………………10

1.2. Uncertainty Propagation in a Fault Tree ……..……………………………12

1.3. Modular Decomposition. Threads …………..……………………………15

1.4. Repairable Systems with Supervision ..……..……………………………24

1.5. Subsystems and the Unit Prototype …………..……………………………28

1.6. I/O Modes ………………………………..…………………………...33

1.7. Insufficiencies of the Traditional Reliability Theory ……..………………34

1.8. Reliability Functions of the Multi-input Systems .…………………………38

1.9 Initiating Events that may lead to Improbable Failures
of the Safety Amplifier ……………………………………………………41

Chapter 2. MNR Safety Amplifier Subsystem Analysis

2.1. UIC Subsystem ……………………...……..……………………………42

2.2. SDA Subsystem ……………………..……..……………………………44

2.3. SRY Subsystem ……………………………………………………………51

2.4. Slow Scram Subsystem Interdependencies ……………………………55

  2.4.1. Calculation of Availabilities by Event Space Decomposition Method ……………………………………………..55

  2.4.2. Calculation of Availabilities by Minimal Cut Set Approximation Method ……………………………………………..59

2.5. Divider …………………………………………………………………..62

2.6. FSP Subsystem …………………………………………………………..66

2.7. Implementation of the Dual Filament Burn-Out Feature that has Acceptably Low Resulting Unavailability ………………………68

2.8. Fast vs. Slow Scram: R49 Failure Case ………………………………70

Chapter 3. Uncertainty and Related Issues

3.1. Uncertainty ……………………………………………………………78

  3.1.1. Origins of Uncertainty ………………………………………..78

  3.1.2. Models with Independent Second Moment …………………..80

3.2. Minimal Cut Set Method ………………………………………………81

  3.2.1. Minimal Cut Set Approximation ………………………………81

  3.2.2. The Bias ……………………………………………………………83

3.3. Confidence ………………………………………………………………86

  3.3.1. Interval estimation ………………………………………………86

  3.3.2. How does the FaultTree+ Calculate the Confidence? ……………87

3.4. Are we too conservative? ………………………………………………..87

3.5. Sensitivity 88

3.6. Importance 90

3.6.1. Deterministic view 90

3.6.2. Stochastic view 91

3.6.3. Other Importance Measures 92

Chapter 4. Common Cause Failures

4.1. Power Supply 96

4.2. Operator Error 97

4.3. Failure on Demand 98

4.4. External Common Cause Failures 102

4.5. Beta Factor Method 103

Chapter 5. Results of the Fault Tree Analysis

5.1. Component Reliability Data 105

5.1.1. Conversion Factors 105

5.1.2. Reliability Database 107

5.2. Basic Event Model Construction 108

5.3. List of Results 109

Conclusion 152

Appendix 1: Principle of Total Probability 156

Appendix 2: An Example of an Incoherent System 158

List of References 160

List of Figures

Figure 1-1. System in the standby parallel mode 11

Figure 1-2. Fault Tree Symbols 12

Figure 1-3. The comparison between absolute and relative sizes of intersections for various event-frequency pairs 13

Figure 1-4. The connectivity between the UIC chambers and the Safety Amplifier 17

Figure 1-5. Fault trees of the Safety Amplifier 19

Figure 1-6. MNR Safety Amplifier Electronic Circuit 21

Figure 1-7. MNR Safety Amplifier Success Signal Propagation Chart 22

Figure 1-8. MNR Safety Amplifier Success Signal Propagation Chart, Matrix Form 23

Figure 1-9. Timeline Diagram of a System with Two Active Parallel Units 25

Figure 1-10. Typical Unit of the Safety Amplifier 28

Figure 1-11. Signal Flow and Information Channels 30

Figure 1-12. Symbol Denoting the Typical Unit in Signal Flow Charts 32

Figure 1-13. Multiple Inputs Enclosed in a Supergraph 40

Figure 2-1. UIC-1 Unit 43

Figure 2-2. SDA-1 Unit 45

Figure 2-3. Operating U-I Characteristics with CAS on the Interface ....…………….49

Figure 2-4. Parallel Thread Designed as: Dormant Closed Line (DCL, left),
and Dormant Opened Line (DOL, right)… .....……………………………..51

Figure 2-5. SRY-1 Unit ……………………..……………………………………..53

Figure 2-6. SSS-1 Reliability Graph and a Sample Cut Set ……..………………...61

Figure 2-7. DIV Subsystem ..………………………………………..……………..62

Figure 2-8. Predicted Failure Rates of Fixed Composition Resistors …..………….....63

Figure 2-9. V3 (or FSP-1) Unit …....…………………..…………………………..67

Figure 2-10. Figure 2-10. Equivalent Single Filament Circuit for
Dual Filament Burn-out ………………………………………………….70

Figure 3-1. Reliability Graph ....….....………………………………………...……82

Figure 5-1. Top Portion of the Safety Amplifier Fault Tree (UIC Input) ……….……113

Figure 5-2. Top Portion of the Safety Amplifier Fault Tree (Log-N Input) …………..114

Figure 5-3. FSP Subsystem Fault Tree Branch: 2.5 Out of 4 Logic …………………115

Figure 5-4. FSP Subsystem Fault Tree Branch (Simplified) ……..…………………116

Figure 5-5. FST Subsystem Fault Tree Branch ..…...…………..…………………117

Figure 5-6. SST Subsystem Fault Tree Branch (Collapsed) …………………………118

Figure 5-7. SST Subsystem Fault Tree Branch (Expanded) ……..…………………119

Figure 5-8. UIC Subsystem Fault Tree Branch ...……………………………………120

Figure 5-9. Safety Amplifier Fault Tree (UIC Input, Expanded) ……..……………121

List of Tables

Table 1-1. Components of the Typical Unit That Correspond to Different Modular Units ……………………..……………………………31

Table 2-1. Electronic Systems Reliability ……………………………………………..64

Table 5-1. Safety Amplifier Root Event Summary …………………………………...110

Table 5-2. Safety Amplifier Root Importance Ranking ...……………………………111

Table 5-3. Minimal Cut Sets with Highest Unavailabilities ....………………………111

Table 5-4. Gate Summary ……………………………...………………………122