

Springer Series in Reliability Engineering

Series Editor

Professor Hoang Pham
Department of Industrial and Systems Engineering
Rutgers, The State University of New Jersey
96 Frelinghuysen Road
Piscataway, NJ 08854-8018
USA

Other titles in this series

The Universal Generating Function in Reliability Analysis and Optimization
Gregory Levitin

Warranty Management and Product Manufacture
D.N.P. Murthy and Wallace R. Blischke

Maintenance Theory of Reliability
Toshio Nakagawa

System Software Reliability
Hoang Pham

Reliability and Optimal Maintenance
Hongzhou Wang and Hoang Pham

Applied Reliability and Quality
B.S. Dhillon

Shock and Damage Models in Reliability Theory
Toshio Nakagawa

Risk Management
Terje Aven and Jan Erik Vinnem

Satisfying Safety Goals by Probabilistic Risk Assessment
Hiromitsu Kumamoto

Offshore Risk Assessment (2nd Edition)
Jan Erik Vinnem

The Maintenance Management Framework
Adolfo Crespo Márquez

Human Reliability and Error in Transportation Systems
B.S. Dhillon

Complex System Maintenance Handbook
D.N.P. Murthy and Khairy A.H. Kobbacy

Recent Advances in Reliability and Quality in Design
Hoang Pham

Product Reliability
D.N.P. Murthy, Marvin Rausand and Trond Østerås

Mining Equipment Reliability, Maintainability, and Safety
B.S. Dhillon

Advanced Reliability Models and Maintenance Policies
Toshio Nakagawa

Justifying the Dependability of Computer-based Systems
Pierre-Jacques Courtois

Poong Hyun Seong
Editor

Reliability and Risk Issues in Large Scale Safety-critical Digital Control Systems

With Additional Contributions by
Poong Hyun Seong
Hyun Gook Kang
Han Seong Son
Jong Gyun Choi
Man Cheol Kim
Jong Hyun Kim
Jae Whan Kim
Seo Ryong Koo
Seung Jun Lee
Jun Su Ha

 Springer

Professor Poong Hyun Seong, PhD
Department of Nuclear
and Quantum Engineering
Korea Advanced Institute of Science
and Technology (KAIST)
373-1, Guseong-dong, Yuseong-gu
Daejeon, 305-701
Republic of Korea

ISBN 978-1-84800-383-5

e-ISBN 978-1-84800-384-2

DOI 10.1007/978-1-84800-384-2

Springer Series in Reliability Engineering ISSN 1614-7839

British Library Cataloguing in Publication Data
Reliability and risk issues in large scale safety-critical
digital control systems. - (Springer series in reliability
engineering)

1. Digital control systems 2. Digital control systems -
Reliability

I. Seong, Poong Hyun
629.8'312

ISBN-13: 9781848003835

Library of Congress Control Number: 2008933411

© 2009 Springer-Verlag London Limited

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form or by any means, with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms of licences issued by the Copyright Licensing Agency. Enquiries concerning reproduction outside those terms should be sent to the publishers.

The use of registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant laws and regulations and therefore free for general use.

The publisher makes no representation, express or implied, with regard to the accuracy of the information contained in this book and cannot accept any legal responsibility or liability for any errors or omissions that may be made.

Cover design: deblik, Berlin, Germany

Printed on acid-free paper

9 8 7 6 5 4 3 2 1

springer.com

Preface

Reliability and risk issues for safety-critical digital control systems are associated with hardware, software, human factors, and the integration of these three entities. The book is divided into four parts. Each part, consisting of three chapters, deals with all entities.

Component level digital hardware reliability, existing hardware reliability theories, and related digital hardware reliability issues (Chapter 1), digital system reliability and risk including hardware, software, human factors, and integration (Chapter 2), and countermeasures using cases from nuclear power plants (Chapter 3) are presented in Part I.

Existing software reliability models and associated issues (Chapter 4), software reliability improvement techniques as countermeasures of software reliability modeling (Chapter 5), and a CASE tool called “NuSEE (nuclear software engineering environment)” which was developed at KAIST (Chapter 6) are presented in Part II.

Selected important existing human reliability analysis (HRA) methods including first- and second-generation methods (Chapter 7), human factors considered in designing and evaluating large-scale safety-critical digital control systems (Chapter 8), and a human performance evaluation tool, called “HUPESS (human performance evaluation support system)”, which was developed at KAIST as a countermeasure to human-factors-related issues (Chapter 9) are presented in Part III.

The integrated large-scale safety-critical control system, which consists of hardware and software that is usually handled by humans, is presented in Part IV. This book emphasizes the need to consider hardware, software, and human factors, not separately, but in an integrated manner. Instrument failure significantly affecting human operator performance was demonstrated in many cases, including the TMI-2 incidents. These issues are discussed in Chapter 10. An analytical HRA method for safety assessment of the integrated digital control systems including human operators, which is based on Bayes’ theorem and information theory, is discussed in Chapter 11. Using this method, it is concluded that human operators are crucial in reliability and risk issues for large-scale safety-critical digital control systems. An operator system which supports human cognitive behavior and actions, “INDESCO (integrated decision support system to aid the cognitive activities of operators)” which was developed at KAIST is discussed in Chapter 12.

This book can be read in different ways. If a reader wants to read only the current issues in any specific entity, he/she can read the first two chapters of either Part I, II, or III, or the first chapter of Part IV. If a reader wants to read only countermeasures developed at KAIST in any specific entity, he/she may read either Chapter 3, 6, or 9, or Chapters 11 and 12.

There are many co-authors of this book. Part I was mainly written by Drs. Jong Gyun CHOI and Hyun Gook KANG from KAERI (Korea Atomic Energy Research Institute). Part II was mainly written by Professor Han Seong SON from Joongbu University and Dr. Seo Ryong KOO from Doosan Heavy Industries and Construction Co., Ltd.. The main writers of Part III are Mr. Jae Whan KIM from KAERI, Dr. Jong Hyun KIM from KHNP (Korea Hydro and Nuclear Power) Co., Ltd., and Dr. Jun Su HA from KAIST. The integration part, Part IV, was mainly written by Drs. Man Cheol KIM and Seung Jun LEE from KAERI.

Last but not least, I would like to thank Mrs. Shirley Sanders and Professor Charles Sanders for their invaluable support for English editing of this entire book. Without their help, this book might have not been published.

Republic of Korea
May 2008

Poong Hyun Seong

Professor
Department of Nuclear
and Quantum Engineering
Korea Advanced Institute
of Science and Technology (KAIST)

Contents

| | |
|-----------------------------------|-------|
| List of Contributors | xv |
| List of Figures | xvii |
| List of Tables | xxiii |

Part I Hardware-related Issues and Countermeasures

| | |
|---|----|
| 1 Reliability of Electronic Components | 3 |
| <i>Jong Gyun Choi, Poong Hyun Seong</i> | |
| 1.1 Mathematical Reliability Models..... | 5 |
| 1.2 Permanent Failure Models of the Electronic Components | 7 |
| 1.3 Intermittent Failure Models of the Electronic Components..... | 13 |
| 1.4 Transient Failure Models of the Electronic Components | 15 |
| 1.5 Concluding Remarks..... | 20 |
| References | 21 |
| 2 Issues in System Reliability and Risk Model | 25 |
| <i>Hyun Gook Kang</i> | |
| 2.1 System Reliability Models | 27 |
| 2.1.1 Simple System Structure | 29 |
| 2.1.2 Complicated System Structure..... | 31 |

- 2.2 Modeling of the Multi-tasking of Digital Systems.....32
 - 2.2.1 Risk Concentration.....32
 - 2.2.2 Dynamic Nature.....35
- 2.3 Estimation of Software Failure Probability36
 - 2.3.1 Quantification of Software Reliability36
 - 2.3.2 Assessment of Software Development Process.....37
 - 2.3.3 Other Issues38
- 2.4 Evaluation of Fault Tolerance Features.....38
- 2.5 Evaluation of Network Communication Safety41
- 2.6 Assessment of Human Failure Probability42
- 2.7 Assessment of Common-cause Failure43
- 2.8 Concluding Remarks.....45
- References45

- 3 Case Studies for System Reliability and Risk Assessment47**
Jong Gyun Choi, Hyun Gook Kang, Poong Hyun Seong
 - 3.1 Case Study 1: Reliability Assessment of Digital Hardware Modules48
 - 3.2 Case Study 2: Reliability Assessment of Embedded Digital System Using Multi-state Function51
 - 3.2.1 Model53
 - 3.2.2 A Model Application to NPP Component Control System.....59
 - 3.3 Case Study 3: Risk Assessment of Safety-critical Digital System62
 - 3.3.1 Procedures for the PRA of Digital I&C System.....63
 - 3.3.2 System Layout and Modeling Assumptions64
 - 3.3.3 Quantification67
 - 3.3.4 Sensitivity Study for the Fault Coverage and the Software Failure Probability.....69
 - 3.3.5 Sensitivity Study for Condition-based HRA Method.....73
 - 3.4 Concluding Remarks.....76
 - References76

Part II Software-related Issues and Countermeasures

| | |
|--|-----|
| 4 Software Faults and Reliability | 81 |
| <i>Han Seong Son, Man Cheol Kim</i> | |
| 4.1 Software Faults | 81 |
| 4.1.1 Systematic Software Fault | 82 |
| 4.1.2 Random Software Fault | 83 |
| 4.1.3 Software Faults and System Reliability Estimation | 84 |
| 4.2 Quantitative Software Reliability Models | 84 |
| 4.2.1 A Classification of Quantitative Software Reliability Models | 85 |
| 4.2.2 Time-related Software Reliability Models <i>Versus</i> Non-time-related Software Reliability Models | 86 |
| 4.2.3 Issues in Software Reliability Quantification | 87 |
| 4.2.4 Reliability Growth Models and Their Applicability | 89 |
| 4.3 Qualitative Software Reliability Evaluation | 91 |
| 4.3.1 Software Fault Tree Analysis | 92 |
| 4.3.2 Software Failure Mode and Effect Analysis | 98 |
| 4.3.3 Software Hazard and Operability Studies | 99 |
| 4.4 Concluding Remarks | 100 |
| References | 101 |
| 5 Software Reliability Improvement Techniques | 105 |
| <i>Han Seong Son, Seo Ryong Koo</i> | |
| 5.1 Formal Methods | 106 |
| 5.1.1 Formal Specification | 107 |
| 5.1.2 Formal Verification | 108 |
| 5.1.3 Formal Methods and Fault Avoidance | 108 |
| 5.2 Verification and Validation | 110 |
| 5.2.1 Lifecycle V&V | 112 |
| 5.2.2 Integrated Approach to V&V | 113 |
| 5.3 Fault Tolerance Techniques | 116 |
| 5.3.1 Diversity | 116 |

5.3.2 Block Recovery 117

5.3.3 Perspectives on Software Fault Tolerance..... 118

5.4 Concluding Remarks..... 119

References..... 119

6 NuSEE: Nuclear Software Engineering Environment 121

Seo Ryong Koo, Han Seong Son, Poong Hyun Seong

6.1 NuSEE Toolset 123

6.1.1 NuSISRT 123

6.1.2 NuSRS..... 127

6.1.3 NuSDS 130

6.1.4 NuSCM 132

6.2 Concluding Remarks..... 133

References..... 134

Part III Human-factors-related Issues and Countermeasures

7 Human Reliability Analysis in Large-scale Digital Control Systems 139

Jae Whan Kim

7.1 First-generation HRA Methods 140

7.1.1 THERP 140

7.1.2 HCR 141

7.1.3 SLIM..... 142

7.1.4 HEART 142

7.2 Second-generation HRA Methods 143

7.2.1 CREAM..... 143

7.2.2 ATHEANA..... 148

7.2.3 The MDTA-based Method 151

7.3 Concluding Remarks..... 159

References..... 160

| | |
|--|------------|
| 8 Human Factors Engineering in Large-scale Digital Control Systems..... | 163 |
| <i>Jong Hyun Kim, Poong Hyun Seong</i> | |
| 8.1 Analyses for HMI Design..... | 164 |
| 8.1.1 Function Analysis | 164 |
| 8.1.2 Task Analysis..... | 166 |
| 8.1.3 Cognitive Factors | 169 |
| 8.2 HMI Design..... | 173 |
| 8.2.1 Computer-based Information Display | 174 |
| 8.2.2 Automation..... | 180 |
| 8.2.3 Computerized Operator Support Systems..... | 183 |
| 8.3 Human Factors Engineering Verification and Validation..... | 187 |
| 8.3.1 Verification..... | 187 |
| 8.3.2 Validation | 188 |
| 8.4 Summary and Concluding Remarks..... | 190 |
| References | 191 |
| | |
| 9 HUPESS: Human Performance Evaluation Support System | 197 |
| <i>Jun Su Ha, Poong Hyun Seong</i> | |
| 9.1 Human Performance Evaluation with HUPESS | 199 |
| 9.1.1 Needs for the Human Performance Evaluation..... | 199 |
| 9.1.2 Considerations and Constraints in Development of HUPESS | 199 |
| 9.2 Human Performance Measures | 202 |
| 9.2.1 Plant Performance | 202 |
| 9.2.2 Personnel Task Performance..... | 206 |
| 9.2.3 Situation Awareness (SA)..... | 208 |
| 9.2.4 Workload | 212 |
| 9.2.5 Teamwork..... | 216 |
| 9.2.6 Anthropometric and Physiological Factors..... | 216 |
| 9.3 Human Performance Evaluation Support System (HUPESS) | 217 |
| 9.3.1 Introduction | 217 |
| 9.3.2 Configuration of HUPESS..... | 217 |

9.3.3 Integrated Measurement, Evaluation, and Analysis
with HUPESS220

9.4 Implications for HRA in ACRs223

9.4.1 Issues Related to HRA223

9.4.2 Role of Human Performance Evaluation for HRA223

9.5 Concluding Remarks.....223

References224

Part IV Integrated System-related Issues and Countermeasures

10 Issues in Integrated Model of I&C Systems and Human Operators.....233

Man Cheol Kim, Poong Hyun Seong

10.1 Conventional Way of Considering I&C Systems
and Human Operators233

10.2 Interdependency of I&C Systems and Human Operators.....234

10.2.1 Risk Concentration on I&C Systems.....235

10.2.2 Effects of Instrument Faults on Human Operators.....236

10.2.3 Dependency of I&C Systems on Human Operators.....236

10.3 Important Factors in Situation Assessment of Human Operators237

10.3.1 Possibilities of Providing Wrong Information
to Human Operators237

10.3.2 Operators’ Trust on Instruments238

10.3.3 Different Difficulties in Correct Diagnosis
of Different Accidents.....238

10.4 Concluding Remarks.....238

References.....240

**11 Countermeasures in Integrated Model of I&C Systems
and Human Operators.....241**

Man Cheol Kim, Poong Hyun Seong

11.1 Human Operators’ Situation Assessment Model242

| | |
|---|-----|
| 11.1.1 Situation Assessment and Situation Awareness | 242 |
| 11.1.2 Description of Situation Assessment Process | 242 |
| 11.1.3 Modeling of Operators' Rules..... | 243 |
| 11.1.4 Bayesian Inference..... | 245 |
| 11.1.5 Knowledge-driven Monitoring | 246 |
| 11.1.6 Ideal Operators <i>Versus</i> Real Human Operators..... | 247 |
| 11.2 An Integrated Model of I&C Systems and Human Operators | 248 |
| 11.2.1 A Mathematical Model for I&C Systems and Human Operators..... | 248 |
| 11.3 An Application to an Accident in an NPP | 249 |
| 11.3.1 Description on the Example Situation | 249 |
| 11.3.2 A Probable Scenario for the Example Situation..... | 251 |
| 11.3.3 Quantitative Analysis for the Scenario..... | 252 |
| 11.3.4 Consideration of All Possible Scenarios..... | 254 |
| 11.3.5 Consideration of the Effects of Context Factors | 255 |
| 11.4 Discussion | 259 |
| 11.5 Concluding Remarks..... | 263 |
| References | 264 |

| | |
|--|------------|
| 12 INDESCO: Integrated Decision Support System to Aid the Cognitive Activities of Operators | 265 |
| <i>Seung Jun Lee, Man Cheol Kim, Poong Hyun Seong</i> | |
| 12.1 Main Control Room Environment..... | 266 |
| 12.2 Cognitive Process Model for Operators in NPPs | 268 |
| 12.2.1 Human Cognitive Process Model..... | 268 |
| 12.2.2 Cognitive Process Model for NPP Operators..... | 269 |
| 12.3 Integrated Decision Support System to Aid Cognitive Activities of Operators (INDESCO)..... | 271 |
| 12.3.1 Architecture of INDESCO..... | 271 |
| 12.3.2 Decision Support Systems for Cognitive Process | 272 |
| 12.4 Quantitative Effect Estimation of Decision Support Systems..... | 275 |
| 12.4.1 Target System of the Evaluation | 275 |

12.4.2 HRA Event Trees.....276

12.4.3 Assumptions for Evaluations.....279

12.4.4 Evaluation Scenarios.....282

12.4.5 Evaluation Results283

12.5 Concluding Remarks.....285

References.....286

Acronyms and Abbreviations.....289

Index.....295

List of Contributors

Poong Hyun Seong

Department of Nuclear and Quantum Engineering,
Korea Advanced Institute of Science and Technology (KAIST)

Hyun Gook Kang

Integrated Safety Assessment Division,
Korea Atomic Energy Research Institute (KAERI)

Han Seong Son

Department of Game Engineering, Joongbu University

Jong Gyun Choi

I&C and Human Factors Division, KAERI

Man Cheol Kim

Integrated Safety Assessment Division, KAERI

Jong Hyun Kim

MMIS Team, Nuclear Engineering and Technology Institute (NETEC),
Korea Hydro and Nuclear Power (KHNP) Co., Ltd.

Jae Whan Kim

Integrated Safety Assessment Division, KAERI

Seo Ryong Koo

Nuclear Power Plant BG, Doosan Heavy Industries and Construction Co., Ltd.

Seung Jun Lee

Integrated Safety Assessment Division, KAERI

Jun Su Ha

Center for Advanced Reactor Research, KAIST

List of Figures

| | | |
|--------------|---|----|
| Figure 1.1. | Functional state of the component | 4 |
| Figure 1.2. | Bathtub curve..... | 8 |
| Figure 1.3. | Generic process of estimating the reliability through stress and damage models..... | 13 |
| Figure 1.4. | Soft-error mechanisms induced by energetic particles | 17 |
| Figure 1.5. | Ratio of the SERs of 0.18 μm 8 Mb SRAM induced by various particles | 18 |
| Figure 2.1. | Series system | 28 |
| Figure 2.2. | Dual redundant system | 30 |
| Figure 2.3. | Standby and automatic takeover system..... | 31 |
| Figure 2.4. | Markov model for standby and automatic takeover system..... | 31 |
| Figure 2.5. | Fault tree for standby and automatic takeover system..... | 32 |
| Figure 2.6. | Schematic diagram of signal processing using analog circuit and digital processor unit | 33 |
| Figure 2.7. | The fault trees for the systems shown in Figure 2.6..... | 34 |
| Figure 2.8. | The fault tree model of a three-train signal-processing system which performs 2-out-of-3 auctioneering | 35 |
| Figure 2.9. | Schematic diagram of a typical watchdog timer application | 39 |
| Figure 2.10. | Fault tree model of the watchdog timer application in Figure 2.9.... | 40 |
| Figure 2.11. | System unavailability along the coverage factor of watchdog timer in Figure 2.9..... | 40 |
| Figure 2.12. | The schematic of the concept of the safety function failure mechanism..... | 43 |

| | | |
|--------------|--|----|
| Figure 3.1. | Functional block diagram of a typical digital hardware module..... | 48 |
| Figure 3.2. | Hierarchical functional architecture of digital system at board level | 52 |
| Figure 3.3. | Coverage model of a component at level i | 53 |
| Figure 3.4. | Logic gates | 54 |
| Figure 3.5. | Modeling of a series system composed of two components | 55 |
| Figure 3.6. | Model of a software instruction execution..... | 56 |
| Figure 3.7. | Model of a software module operation..... | 57 |
| Figure 3.8. | Control flow of example software..... | 58 |
| Figure 3.9. | Logic gate of example software..... | 59 |
| Figure 3.10. | Logic network of the application software | 60 |
| Figure 3.11. | State probability of the system without fault-handling techniques.. | 61 |
| Figure 3.12. | State probability of the system with fault-handling techniques of hardware components | 61 |
| Figure 3.13. | State probability of the system with consideration of software operational profile but without consideration of fault-handling techniques..... | 62 |
| Figure 3.14. | Schematic diagram of a typical RPS | 65 |
| Figure 3.15. | The signal flow in the typical RPS..... | 66 |
| Figure 3.16. | The detailed schematic diagram of watchdog timers and CP DO modules | 66 |
| Figure 3.17. | System unavailability along fault coverage and software failure probability when identical input and output modules are used..... | 71 |
| Figure 3.18. | System unavailability along fault coverage and software failure probability when two kinds of input modules and the identical output modules are used..... | 72 |
| Figure 3.19. | System unavailability along fault coverage and software failure probability when two kinds of input modules and two kinds of output modules are used..... | 72 |
| Figure 3.20. | Comparison among single HEP methods and the CBHRA method for AFAS generation failure probabilities..... | 75 |

| | | |
|--------------|--|-----|
| Figure 4.1. | Estimated total numbers of inherent software faults calculated by Jelinski–Moranda model and Goel–Okumoto NHPP model | 91 |
| Figure 4.2. | An example of software fault tree template | 93 |
| Figure 4.3. | A part of fault tree of Wolsong PDLTrip | 95 |
| Figure 4.4. | Timed automata for PDLCond trip condition | 96 |
| Figure 4.5. | Screen dump of the UPPAAL outputs..... | 97 |
| Figure 5.1. | Major features of IE approach | 114 |
| Figure 5.2. | Overall scheme of IE approach..... | 115 |
| Figure 6.1. | Software V&V tasks during the lifecycle | 122 |
| Figure 6.2. | Overall features of NuSEE | 122 |
| Figure 6.3. | Inspection view of NuSISRT | 124 |
| Figure 6.4. | Schematic diagram of requirements traceability | 125 |
| Figure 6.5. | Traceability view of NuSISRT | 126 |
| Figure 6.6. | An example of similarity calculation | 126 |
| Figure 6.7. | Structure view of NuSISRT..... | 127 |
| Figure 6.8. | Editing windows of NuSRS..... | 129 |
| Figure 6.9. | Part of NuSCR specification for the RPS | 129 |
| Figure 6.10. | Partial application results of NuSCR for RPS..... | 130 |
| Figure 6.11. | Features of NuSDS | 131 |
| Figure 6.12. | Software design specification of the BP | 132 |
| Figure 6.13. | Document management view and change request view of NuSCM..... | 133 |
| Figure 7.1. | Relations between CPC score and control modes | 147 |
| Figure 7.2. | The basic structure of the MDTA | 152 |
| Figure 8.1. | A coupling of a system, tasks, and operators..... | 164 |
| Figure 8.2. | A part of HTA for SGTR accident..... | 167 |
| Figure 8.3. | Typical form of decision ladder | 168 |
| Figure 8.4. | A typical form of information flow model | 169 |
| Figure 8.5. | A general information-processing model | 171 |
| Figure 8.6. | Bar graphs for pressurizer variables..... | 176 |
| Figure 8.7. | Polygonal display..... | 176 |
| Figure 8.8. | Integral display (a symbol for indicating wind)..... | 177 |

Figure 8.9. Information-rich display..... 178

Figure 8.10. COSS and cognitive activities 185

Figure 8.11. COSS paradigms..... 186

Figure 8.12. Relations among the chapters in Part III..... 191

Figure 9.1. Factors for human performance evaluation 198

Figure 9.2. Key considerations and constraints in development of HUPESS ..202

Figure 9.3. Optimal solution of a scenario in hierarchical form207

Figure 9.4. A computerized system for the eye fixation analysis213

Figure 9.5. HUEPSS H/W configuration218

Figure 9.6. Eye-tracking system with five measurement cameras.....219

Figure 9.7. HUPESS software configuration219

Figure 9.8. Evaluation procedure with HUEPSS.....220

Figure 9.9. Overall scheme for the evaluation with HUEPSS.....221

Figure 9.10. Main functions of HUPESS.....224

Figure 10.1. An example of how I&C systems and human operators
are considered in conventional PRA models234

Figure 10.2. The concept of risk concentration of I&C systems235

Figure 10.3. Some important aspects of the Bhopal accident.....237

Figure 10.4. The way I&C systems and human operators are considered
in current PRA technology239

Figure 10.5. The way I&C systems and human operators should
be considered in an integrated model.....240

Figure 11.1. Model for operators’ rules.....244

Figure 11.2. Structure of the developed model and the definition
of the variables248

Figure 11.3. Trends of various plant parameters by CNS
for the example situation250

Figure 11.4. Generated alarms by CNS for the example
situation (the LOCA occurs at 3 minutes).....251

Figure 11.5. Bayesian network model for the example situation when the
operators are unaware of the occurrence of the accident.....252

| | |
|--|-----|
| Figure 11.6. Bayesian network model for the example situation when the containment radiation is increasing is observed..... | 253 |
| Figure 11.7. Change in operator understanding of plant status after observation of an increase in containment radiation..... | 257 |
| Figure 11.8. Change of operator understanding of plant status as operators monitor indicators..... | 257 |
| Figure 11.9. Change of reactor trip failure probability as operators monitor indicators..... | 258 |
| Figure 11.10. A brief summary of the assumptions for the effects of context factors on the process of situation assessment of human operators..... | 259 |
| Figure 11.11. Changes of reactor trip failure probability as function of time ($0 \text{ sec} < \text{Time} < 500 \text{ sec}$)..... | 260 |
| Figure 11.12. Changes in reactor trip failure probability as function of time ($100 \text{ sec} < \text{Time} < 500 \text{ sec}$)..... | 260 |
| Figure 11.13. Effect of the adequacy of HMI..... | 262 |
| Figure 11.14. Effect of time of day (circadian rhythm)..... | 262 |
| Figure 12.1. Independent support system and combined support system..... | 267 |
| Figure 12.2. The operation process of human operators in large-scale systems..... | 269 |
| Figure 12.3. The operation process of a large-scale system with indirect support systems..... | 270 |
| Figure 12.4. The operation process of a large-scale system with direct and indirect support systems..... | 270 |
| Figure 12.5. The conceptual architecture of INDESCO..... | 271 |
| Figure 12.6. DSSs based on human cognitive process model..... | 272 |
| Figure 12.7. The architecture of an application..... | 276 |
| Figure 12.8. HRA event tree in the case of no DSS..... | 277 |
| Figure 12.9. HRA event tree when all DSSs are used..... | 277 |
| Figure 12.10. BBN model for the evaluation..... | 278 |
| Figure 12.11. BBN model for Case 7..... | 282 |
| Figure 12.12. BBN model for Case 1..... | 284 |

List of Tables

| | | |
|------------|--|-----|
| Table 1.1. | Mathematical relationship between the representative reliability measures..... | 6 |
| Table 1.2. | Mathematical reliability measures about three representative failure distribution models..... | 7 |
| Table 3.1. | Failure status of a typical digital hardware module | 49 |
| Table 3.2. | Failure rates of the typical PLC modules | 51 |
| Table 3.3. | Function table of the series system | 55 |
| Table 3.4. | Selection function set table of the example software | 58 |
| Table 3.5. | Information on control system hardware..... | 59 |
| Table 3.6. | The conditions of a human error in the case of the 4-channel single-parameter functions (O: available, X: unavailable) | 75 |
| Table 4.1. | Category of probability of failure mode..... | 99 |
| Table 4.2. | Severity category for software FMEA | 100 |
| Table 6.1. | Summary of each tool | 134 |
| Table 7.1. | Definitions or descriptions of the common performance conditions (CPCs) in CREAM..... | 144 |
| Table 7.2. | The association matrix between the cognitive activities and the cognitive functions..... | 144 |
| Table 7.3. | Types of cognitive function failures and nominal failure probability values | 147 |
| Table 7.4. | Control modes and probability intervals | 148 |
| Table 7.5. | Composition of event groups for evaluating the contribution of plant dynamics to a diagnosis failure..... | 153 |

| | | |
|-------------|--|-----|
| Table 7.6. | Operator error probabilities assigned to the selected items | 155 |
| Table 7.7. | An example of required functions for two events, SLOCA and ESDE | 157 |
| Table 7.8. | The non-recovery probability assigned to two possible recovery paths (adapted from CBDTM)..... | 158 |
| Table 8.1. | Multiple barriers for the NPP safety | 165 |
| Table 8.2. | Fitts' list | 181 |
| Table 8.3. | Comparison of empirical measures for workload | 189 |
| Table 11.1. | Change in operators' understanding of the plant status..... | 254 |
| Table 11.2. | Possible observations and resultant operator understanding of plant status after observing increased containment radiation | 256 |
| Table 11.3. | Effect of adequacy of organization (safety culture) | 260 |
| Table 11.4. | Effect of working conditions | 261 |
| Table 11.5. | Effect of crew collaboration quality..... | 261 |
| Table 11.6. | Effect of adequacy of procedures | 261 |
| Table 11.7. | Effect of stress (available time)..... | 261 |
| Table 11.8. | Effect of training/experience | 261 |
| Table 11.9. | Effect of sensor failure probability | 261 |
| Table 12.1. | HEPs for the reading of indicators..... | 280 |
| Table 12.2. | HEPs for omission per item of instruction when the use of written procedures is specified | 280 |
| Table 12.3. | HEPs for commission errors in operating manual controls | 281 |
| Table 12.4. | Results of the first evaluation for the reactor trip operation | 284 |
| Table 12.5. | Results of the second evaluation for the failed SG isolation operation | 285 |