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

Jong Gyun Choi, Poong Hyun Seong

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

Hyun Gook Kang

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 Probability....36
2.3.1 Quantification of Software Reliability....36
2.3.2 Assessment of Software Development Process....37
2.3.3 Other Issues....38
2.4 Evaluation of Fault Tolerance Features....38
2.5 Evaluation of Network Communication Safety....41
2.6 Assessment of Human Failure Probability....42
2.7 Assessment of Common-cause Failure....43
2.8 Concluding Remarks....45
References....45

3 Case Studies for System Reliability and Risk Assessment....47
Jong Gyun Choi, Hyun Gook Kang, Poong Hyun Seong
3.1 Case Study 1: Reliability Assessment of Digital Hardware Modules....48
3.2 Case Study 2: Reliability Assessment of Embedded Digital System Using Multi-state Function....51
3.2.1 Model....53
3.2.2 A Model Application to NPP Component Control System....59
3.3 Case Study 3: Risk Assessment of Safety-critical Digital System....62
3.3.1 Procedures for the PRA of Digital I&C System....63
3.3.2 System Layout and Modeling Assumptions....64
3.3.3 Quantification....67
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
References....76

Part II Software-related Issues and Countermeasures

4 Software Faults and Reliability 81
Han Seong Son, Man Cheol Kim

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 *Versus* 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
Han Seong Son, Seo Ryong Koo

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
Jong Hyun Kim, Poong Hyun Seong

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
Jun Su Ha, Poong Hyun Seong

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 HUPESS 220
9.4 Implications for HRA in ACRs 223
9.4.1 Issues Related to HRA 223
9.4.2 Role of Human Performance Evaluation for HRA 223
9.5 Concluding Remarks 223
References 224

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 Operators 233
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 Operators 237
10.3.1 Possibilities of Providing Wrong Information to Human Operators 237
10.3.2 Operators' Trust on Instruments 238
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 Model 242

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 *Versus* 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
Seung Jun Lee, Man Cheol Kim, Poong Hyun Seong
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 Results 283
12.5 Concluding Remarks 285
References 286

Acronyms and Abbreviations 289

Index 295