
Contents

1	Safety Goals and Risk-informed Decision Making	1
1.1	Introduction	1
1.2	Safety Goals and Health Objectives	2
1.2.1	Safety Goal Policy Statement (1986)	2
1.2.2	Qualitative Safety Goals	3
1.2.3	Quantitative Health Objectives (QHOs)	3
1.2.4	Individual and Societal Risks	3
1.2.5	QHOs and Fatality Statistics	4
1.2.6	Adequate Protection and QHOs	6
1.2.7	Temporary Plant-configuration Goals	6
1.3	Subsidiary Numerical Objectives	6
1.3.1	Accident and Public Confidence	6
1.3.2	CDF and LERF Objectives	8
1.3.3	Subsidiary Objectives	9
1.3.4	Prevention and Mitigation	9
1.4	Acceptance Guidelines for Risk Increase	10
1.4.1	Permanent Change	10
1.4.2	Temporary Change	12
1.5	Treatment of Uncertainties	14
1.6	Risk-informed Integrated Decision Making	16
1.6.1	Deterministic Approach	16
1.6.2	Probabilistic Approach: PRA	17
1.6.3	Integrated Decision Making	17
1.6.4	Decision Making Principles	17
1.6.5	Defense-in-depth	18
1.6.6	Sufficient Safety Margins	22
1.7	Tolerability of Risk and ALARP	22
1.7.1	Radiation Fatality Risk	22
1.7.2	TOR Requirements	24
1.7.3	Applying TOR Framework	26
1.8	Explicit Consideration of Societal Risk	26

1.8.1	Individual and Societal Risk	26
1.8.2	Graphical Representation of Societal Risk	27
1.8.3	Example: Individual and Societal Risks	29
1.9	Concluding Remarks	32
2	Categorization by Safety Significance	35
2.1	Introduction	35
2.2	Safety Integrity Level: IEC 61508 and IEC 61511	35
2.2.1	Hazardous Situation and Event	35
2.2.2	Definition of Function	36
2.2.3	Functional Safety System	36
2.2.4	Example: Reactor Scram System	37
2.2.5	Example: Risk-averse Safety Goal	38
2.2.6	Safety Integrity Level	38
2.2.7	Example: High-demand Mode	40
2.2.8	Semiquantitative Method using Subsidiary Objective... ..	42
2.2.9	Layer of Protection Analysis	46
2.2.10	Safety-layer Matrix	49
2.2.11	Risk Graph	51
2.2.12	Category for Machinery Safety: EN 954	52
2.3	SSC Categorization Guideline: NEI 00-04	52
2.3.1	Safety-related SSCs	53
2.3.2	Quality-assurance Program	54
2.3.3	Safety-significance Categorization	55
2.3.4	Internal Event Assessment Example	58
2.4	Safety Significance of Human Actions: NUREG-1764	62
2.4.1	Human-factors Engineering Review	62
2.4.2	Step 1: Quantitative Assessment	63
2.4.3	Step 2: Qualitative Assessment	65
2.4.4	Step 3: Integrated Assessment	67
2.5	Concluding Remarks	67
3	Realization of Category Requirements	69
3.1	Introduction	69
3.2	Uncertainty	69
3.3	Guidelines, Standards, and Regulations	70
3.4	Management of Dependent Failures	71
3.4.1	Types of Dependencies	71
3.4.2	Common-cause Failures	73
3.4.3	Safety Principles for Dependency	74
3.5	Safety Margins	78
3.6	Human-factors Review for HSS Human Actions	79
3.7	Early Detection and Treatment	80
3.7.1	Detection Examples	80
3.7.2	Diagnostic Coverage	81

3.7.3	Safe-failure Fraction	82
3.7.4	System Behavior on Detection of Failure	82
3.7.5	Hardware Fault Tolerance by SFF and SIL	83
3.8	Level of Defense-in-depth	85
3.9	Performance Evaluation after Categorization	86
3.9.1	Evaluation of Changes of Special Treatment	86
3.9.2	SIS Quantification	87
3.10	Concluding Remarks	94
4	Hazard Identification and Risk Reduction	95
4.1	Introduction	95
4.2	Hazard, Source and Risk	95
4.2.1	Classification of Hazards	96
4.2.2	Typical Measures for Hazards	96
4.3	Hazard Association	97
4.3.1	HAZOP	97
4.3.2	Abnormal-event Vocabularies	98
4.3.3	Function Names	100
4.4	FMEA	101
4.5	Master Logic Diagram	103
4.6	Risk-reduction Measures	103
4.6.1	Definition of Initiating Events	103
4.6.2	Four Major Steps	105
4.6.3	Inherently Safer Design	105
4.6.4	Prevention and Mitigation	105
4.6.5	Initiating-event Prevention	105
4.6.6	Initiating-event Mitigation	108
4.6.7	Accident Mitigation	110
4.7	Concluding Remarks	111
5	Probabilistic Risk Assessment: PRA	113
5.1	Introduction	113
5.2	PRA with or without Material Hazards	113
5.2.1	Initiating Event and Risk Profiles	113
5.2.2	PRA without Material Hazards	114
5.2.3	PRA with Material Hazards	116
5.2.4	Nuclear Power Plant PRA: WASH-1400	117
5.2.5	NUREG-1150 and ASME PRA Quality Standard	121
5.3	Three PRA Levels	122
5.4	Level 1 PRA – Accident Frequency	123
5.4.1	Accident-frequency Analysis	123
5.4.2	ASME Level 1 Quality Standard	124
5.4.3	Plant Familiarization	124
5.4.4	Initiating-event Analysis	125
5.4.5	Event-tree Construction	126

5.4.6	System Models: Fault-tree Constuction	130
5.4.7	Accident-sequence Screening and Quantification	130
5.4.8	Dependent Failure Analysis	131
5.4.9	Human-reliability Analysis	131
5.4.10	Database Analysis	132
5.4.11	Grouping of Accident Sequence	132
5.4.12	Uncertainty Analysis	133
5.4.13	Products from Level 1 PRA	133
5.5	Level 2 PRA – Accident Progression and Source Term	133
5.5.1	Accident-progression Analysis	133
5.5.2	Source-term Analysis	134
5.6	Level 3 PRA – Offsite Consequence	134
5.7	Risk Calculations	134
5.7.1	Level 3 PRA Risk Profile	134
5.7.2	Level 2 PRA Risk Profile	137
5.7.3	Level 1 PRA Risk Profile	138
5.7.4	Uncertainty of Risk Profiles	138
5.8	Evaluation of Seismic Hazards	138
5.8.1	Seismic Hazard Curve	139
5.8.2	Calculation of Damage Probability	142
5.9	External Event PRA Standards	143
5.10	Concluding Remarks	143
6	Basic Event Quantification	145
6.1	Introduction	145
6.2	What are Basic Events?	145
6.3	Basic Two-state Transition Diagram	146
6.3.1	Repair-to-failure Process Parameters	147
6.3.2	Failure-to-repair Process Parameters	151
6.3.3	Combined Process Parameters	153
6.4	Relations between Reliability Parameters	155
6.4.1	Process up to Failure Occurrence	155
6.4.2	Process up to Repair Completion	156
6.4.3	Combined Process	156
6.5	Constant Failure and Repair Rate Model	158
6.5.1	Process up to Failure Occurrence	158
6.5.2	Process up to Repair Completion	159
6.5.3	Combined Process	160
6.5.4	Instantaneous Repair and Poisson Process	162
6.5.5	Fractional Time Availability	162
6.6	Estimation of Distribution Parameters	163
6.6.1	Exponential Distribution and Random Failure	163
6.6.2	Weibull Distribution and Early Failure	164
6.6.3	Weibull Distribution and Wearout Failure	166
6.7	Lognormal Distribution	168

6.8	Stress and Response Model	170
6.8.1	Case of Normal Distribution	172
6.8.2	Case of Lognormal Distribution	173
6.9	Basic-event Parameters for PRA	174
6.9.1	Types of Parameters	174
6.9.2	Data for Parameter Quantification	174
6.9.3	Quantified Parameters	176
6.9.4	Bayesian Approach	176
6.9.5	Demand Failure and Standby Failure	177
6.9.6	Hierarchical Bayes Approach	178
6.10	Concluding Remarks	178
7	System Event Quantification	179
7.1	Introduction	179
7.2	Simple Systems	179
7.2.1	Reliability Block Diagram	179
7.2.2	Series System	180
7.2.3	Parallel System	181
7.2.4	Voting System	181
7.2.5	Nonseries-parallel System	183
7.3	Single Large Fault Tree	184
7.4	Minimal Cuts and Minimal Paths	184
7.4.1	Minimal Cut Sets	184
7.4.2	Minimal Path Sets	185
7.4.3	Minimal-cut Generation	186
7.5	Fault-tree Linking along Event Tree	188
7.6	Structure Functions	189
7.6.1	Definition	189
7.6.2	Simple Systems	189
7.6.3	Calculation of Unavailability	190
7.6.4	Minimal-cut and Minimal-path Representations	191
7.6.5	Inclusion-exclusion Formula	195
7.7	False and Inactive Alarms	197
7.7.1	Alarm-generating Function	197
7.7.2	False-alarm Function	198
7.7.3	Inactive-alarm Function	199
7.7.4	False-alarm and Inactive-alarm Probabilities	199
7.8	Concluding Remarks	201
8	Dependent Failure Quantification	203
8.1	Introduction	203
8.2	Common-cause Failures	203
8.2.1	Cause-level Analysis	204
8.2.2	Alpha-factor Model	206
8.2.3	Distribution of Alpha-factor Parameters	212

8.2.4	Alpha Factor with Staggered Testing.....	214
8.2.5	Beta-factor Model	215
8.3	Markov Analysis of Graceful Degradation.....	217
8.3.1	Steer-by-wire System Reliability.....	217
8.3.2	Fault-tolerant Design	218
8.3.3	Operation Procedure during Partial Failures	218
8.3.4	Markov Transition Diagram	220
8.3.5	Markov Differential Equation	222
8.3.6	Reliability Quantification	222
8.3.7	Design Alternative for Collision Safety	223
8.4	Concluding Remarks	224
9	Human-error Quantification	225
9.1	Introduction	225
9.2	Classification of Human Error for PRA.....	226
9.2.1	Preinitiator Error	226
9.2.2	Postinitiator Error.....	227
9.3	Slip, Lapse, Mistake, and No Detection.....	227
9.4	Stress and Performance-shaping Factors	229
9.5	Calculation of Nonresponse Probability.....	234
9.5.1	Median Response Time	234
9.5.2	Median of Operator-detection Time.....	235
9.5.3	Available Time and Nonresponse Probability.....	235
9.6	THERP	237
9.6.1	Task Analysis	238
9.6.2	HRA Event Tree	239
9.6.3	Stress and Skill Level	241
9.6.4	General THERP Procedure	242
9.7	Concluding Remarks	244
	References	245
	Index	249

Satisfying Safety Goals by Probabilistic Risk Assessment

Kumamoto, H.

2007, XVI, 253 p., Hardcover

ISBN: 978-1-84628-681-0