Springer Series in Reliability Engineering

Hiromitsu Kumamoto

Satisfying Safety Goals by Probabilistic Risk Assessment

Springer Series in Reliability Engineering

Series Editor

Professor Hoang Pham
Department of Industrial 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

Hiromitsu Kumamoto

Satisfying Safety Goals by Probabilistic Risk Assessment

Springer

Hiromitsu Kumamoto, Dr. Eng
Graduate School of Informatics
Kyoto University
Kyoto 606-8501
Japan

British Library Cataloguing in Publication Data
Kumamoto, Hiromitsu
Satisfying safety goals by probabilistic risk assessment. -
(Springer series in reliability engineering)
1. System safety - Statistics 2. Risk assessment
3. Reliability (Engineering)
I. Title
620.8'6'015192
ISBN-13: 9781846286810

Library of Congress Control Number: 2007922342

Springer Series in Reliability Engineering series ISSN 1614-7839
ISBN 978-1-84628-681-0 e-ISBN 978-1-84628-682-7 Printed on acid-free paper

9 8 7 6 5 4 3 2 1

Springer Science+Business Media
springer.com

To my wife Michiko and to my mentor Dr. Ernest J. Henley

Preface

Fatal accidents are rare events, not commonly experienced in our daily lives. Automobiles run and aircrafts fly. The maximum-speed specification has been a typical design goal for these vehicles during everyday operation periods. People have established goals and designed, manufactured, operated and maintained engineering systems, accordingly. This is a goal-oriented approach that had not been used for fatal accidents because of our inexperience of such rare events.

Historically, however, we have accumulated a huge number of safety-related rare events since the Industrial Revolution 250 years ago. More people have now come to think that the goal-oriented approach to the rare events is necessary and possible for various engineering systems in a variety of industrial disciplines of nuclear, chemical, aerospace, machinery, railroad, automobile, and others. As is seen from recent international activities, this century is becoming a "safety-first" age. The goals are established, engineering systems are designed, and the achievements are checked and maintained throughout the life cycles. This is a new movement and some confusions and localisms exist among different disciplines. The author would like to set things in order for better safety.

This book is addressed toward graduate and undergraduate students and engineers and scientists working for safety-related industries, laboratories, business, and government. An undergraduate semester class can teach Chapters 6 to 9. These chapters treat rather elementary aspects of the probabilistic risk assessment (PRA). A graduate semester class can teach the first half of the book, *i.e.* Chapters 1 to 5. These chapters give rather conceptual and methodological treatments and clarify how to satisfy safety goals by the PRA to be complemented by deterministic approaches such as defense-in-depth and good engineering practices.

Chapter 1 first presents qualitative safety goals, and quantitative health objectives. Uncertainties inherent in the current PRA necessitate an introduction of subsidiary numerical objectives in place of the original goals. The satisfying process includes as an indispensable element a risk-informed integrated, probabilistic–deterministic decision making to account for the uncertainties. The tolerability aspects of risks are also presented to deal with risks exceeding broadly acceptable objectives. Societal risks are also discussed. This is, however, a more complicated and still a less feasible problem.

The risk-informed safety-goal satisfaction process involves categorizations of structures, systems, and components (SSC) and human actions (HA) from the point of view of safety significance. This categorization for prioritization is fully described in Chapter 2. Chapter 3, in turn, develops how the performance level assigned to each category can be materialized to ensure the eventual satisfaction of the safety goal. The integrated, probabilistic–deterministic decision making is required and developed. The emphasis is placed on uncertainties, dependent failures, defense-in-depth, early detection and treatment, good engineering practices, sufficient safety margins, and so on.

Chapter 4 presents general frameworks for hazard identification and risk reduction. Hazards should first be captured intuitively through guide words, abnormal-event vocabularies, and structured searches. The initiating-event prevention and mitigation are key elements of risk reduction.

Chapter 5 deals with the PRA. Event trees are combined with fault trees to model various scenarios and causes. This is the so-called level 1 PRA. Level 2 PRA investigates accident progressions and hazardous-material releases, and level 3 PRA estimates offsite consequences. The readers will recognize that the PRA is widely applicable to any industries with risks.

Basic-event quantifications are described in Chapter 6 to offer a starting point of risk quantification for the safety goal satisfaction. Parameters are defined precisely and their relations are clarified. Examples are given for exponential- and Weibull-parameter estimations. Up-to-date Bayes approaches are presented to deal with experience and plant-specific data. Chapter 7 gives system-level qualitative–quantitative analyses based on minimal cut sets, structure functions, inclusion-exclusion, and inactive and false alarms.

Two types of dependencies are quantified in Chapter 8. A common-cause analysis called an alpha-factor method is fully described. A graceful-degradation mechanism for an automobile steer-by-wire system is analyzed by a Markov transition diagram. The common causes are the most dangerous factors to defeat multiple barriers, while the graceful degradations allow early detection and treatment to maintain the system integrity. Human-error quantification is focused in the final Chapter 9. A methodology called THERP solely available for the quantification is described together with related topics.

The PRA-specific Chapters 5 – 9 (excluding Chapter 8) have been derived from relevant portions of our previous book, “H. Kumamoto, E.J. Henley: Probabilistic Risk Assessment and Management for Engineers and Scientists, Second Edition; IEEE Press (1996)”. These portions have been shortened and revised to include new material which reflects recent PRA developments. The dependent failure Chapter 8 is new. These five PRA chapters as a whole reinforce quantitative aspects of the safety-goal satisfaction process newly developed in the first half of the book, *i.e.* Chapters 1 to 4.

The author is grateful to senior editor Anthony Doyle who invited me to contribute to the “Springer Series in Reliability Engineering”, and to the genial staff at Springer: Kate Brown, Simon Rees, Sorina Moosdorf and others who remain anonymous. The author is also grateful to the pre-publication reviewers for many helpful comments.

January 2007

Hiromitsu Kumamoto
Kyoto University, Kyoto

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-aversive 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

1

Safety Goals and Risk-informed Decision Making

1.1 Introduction

The probabilistic risk assessment (PRA) is the most powerful approach to quantification of risk and safety. Risk is a combination of probability of harm and severity of that harm, while safety is freedom from unacceptable risk [1].

Basically, any plant should be designed and operated in such a way as to satisfy a given set of safety goals. This is a goal-oriented approach where goals are first specified, and then the plant is designed, created, operated and maintained accordingly. However, two problems must be answered for the goal-oriented approach to be materialized.

1) How safe is safe enough? This requires a set of safety goals to be satisfied.
2) How to deal with uncertainties? The current risk quantification involves significant uncertainties.

This chapter surveys how the two problems are being overcome by the risk-informed activities advocated by the US Nuclear Regulatory Commission (NRC) and the tolerability of risk framework by the UK Health and Safety Executive (HSE).

The target for the NRC is of course a nuclear power plant. However, the implications can certainly be translated into other fields including process, aerospace, railroad, medical, machinery, and automobile industries. It is easily seen that the prevention of core damage corresponds to prevention of vehicle collision (active safety), and accident mitigation by a containment structure corresponds to collision mitigation by an air bag (passive safety). Prevention coupled with mitigation is an indispensable element of the defense-in-depth philosophy to cope with the uncertainty of current risk quantification.

The NRC's risk-informed regulation is currently limited to changes or modifications to plant design and operation. However, the underlying philosophy can apply to current state of non-nuclear plant design and operation as well as their changes.

Section 1.2 describes the Safety Goal Policy Statement in 1986 that introduced qualitative safety goals as well as quantitative health objectives. This policy statement courageously challenged the question of "how safe is safe enough?". Unfortunately, the current PRA does not have sufficient capability to validate the plant against the quantitative health objectives because of the large number of uncertainties generated in the process of risk quantification.

Section 1.3 explains why the so-called subsidiary numerical objectives had to be introduced to resolve the weakness inherent in the current PRA. A core-damage frequency and large early-release frequency are designated as two subsidiary objectives.

Section 1.4 deals with how design and operation are evaluated in the framework of the subsidiary objectives for cases where risk increases are involved. The PRA thus retreating to the subsidiary objectives, however, is not yet free from uncertainty problems, although uncertainties have been decreased significantly as compared with the case of the original quantitative health objectives introduced by the Safety Goal Statement. Section 1.5 considers the uncertainty in more detail and Section 1.6 presents the risk-informed integrated decision making to manage the uncertainty.

The UK HSE has taken a different approach from that of the US NRC. The HSE's framework has been known as tolerability of risks (TOR). Section 1.7 describes the TOR together with a so-called ALARP principle. The framework provides us with tolerable risks, while the risk-informed regulation deals with acceptable risks. Both are important for the safety-significant categorization described in Chapter 2.

Most safety goals have dealt with individual risks where each individual wants to reduce the risk. Our society as a whole also wants to reduce the risk. Section 1.8 considers the individual and societal risks.

1.2 Safety Goals and Health Objectives

1.2.1 Safety Goal Policy Statement (1986)

The year 1986 will be remembered as an epoch-making year when the US NRC took a step toward defining "how safe is safe enough?". The Safety Goal Policy Statement was published in that year [2]. A distinguished feature of this statement was that it consisted of qualitative goals and quantitative objectives. This tradition of making use of the qualitative and quantitative aspects has evolved into today's *risk-informed* integrated decision making, very different from a *risk-based* decision making solely driven by numerical values.

It was four years after the publication of this Policy Statement when the NRC formally clarified in a Staff Requirements Memorandum (SRM) in 1990 that the safety goals were to be used to define "how safe is safe enough?" [3].

1.2.2 Qualitative Safety Goals

The Policy Statement describes qualitative safety goals as follows [2]:

1) Individual members of the public should be provided a level of protection from the consequence of nuclear power plant operation such that individuals bear no significant additional risk to life and health.
2) Societal risks to life and health from nuclear power plant operation should be comparable to or less than the risks of generating electricity by viable competing technologies and should not be a significant addition to other societal risks.

1.2.3 Quantitative Health Objectives (QHOs)

The following quantitative objectives are introduced to determine achievement of the safety goals.

1) The risk to an average individual in the vicinity of a nuclear power plant of prompt fatalities that might result from reactor accidents should not exceed one-tenth of one per cent (0.1 per cent) of the sum of prompt-fatality risks resulting from other accidents to which members of the US population are generally exposed.
2) The risk to the population in the area near a nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed one-tenth of one per cent (0.1 per cent) of the sum of cancer-fatality risks resulting from all other causes.

The vicinity of a nuclear power plant in the first objective is interpreted as the site boundary, and the average individual is a real or hypothetical person living there. The area near a nuclear power plant in the second objective is defined as a 10-mile radius zone.

The first is called a prompt-fatality objective because it deals with relatively acute fatalities due to violent radioactive energy released from the accident site. The second is called a cancer-fatality objective because it considers development of fatal cancers of radioactive origin after a latent period. The two objectives are named quantitative health (effects) objectives (QHOs).

1.2.4 Individual and Societal Risks

The first qualitative goal and the first objective consider an individual risk. The second qualitative goal deals with a societal risk where an evaluator of the risk is not an individual but a whole society. In other words, the denominator for calculating the risk is not the total number of individuals but a single society. The risk to life and health are considered as a threat to the society. The societal risk in a broader sense includes land-contaminations and environmental impacts as evidenced by the Chernobyl accident [3].

The second QHO is paired with the second qualitative goal. This QHO deals with the total number of cancer fatalities that the society suffers from in the 10-mile radius zone. In this context, a collective dose of radioactivity over the individuals in the zone might be a suitable measure because there is a strong correlation between the cancer fatalities and the collective dose. The collective dose is calculated by adding all the doses to all the exposed people in a 10-mile radius zone.

However, the existence of the 0.1 per cent requirement in the second objective suggests we should convert the total cancer fatalities into a cancer-fatality rate per individual or even into the dose to the most exposed individual.

The second QHO thus has two aspects; societal and individual. A summed risk or a collective dose may be used in place of individual cancer risk, and *vice versa.* A 50-mile radius is also used in place of the 10-mile radius [3]. Several interpretations are possible for the second QHO.

In this book, the second QHO is evaluated by the individual cancer-fatality risk. The 0.1 per cent requirement for the individual keeps the societal cancer risk at a sufficiently low level, except for a heavily populated 10-mile zone.

The land-contamination risk is not quantified because the NRC prioritized public health and safety. The Chernobyl accident (April, 1986) was fresh when the NRC published the Safety Goal Statement (August, 1986) that lacked a land-contamination-risk goal [3]. The land-contamination and other environmental effects would be kept sufficiently small when the second QHO is satisfied for the individual risk.

1.2.5 QHOs and Fatality Statistics

Figure 1.2.4 shows the QHOs as compared with various fatality rates in Japan. The vertical axis is the number of fatalities per 100 000 persons. Figure 1.2.4 for reference includes the average fatality rate due to all causes together with a variation over ages. The rate profile of England and Wales is also shown. It is surprising that two countries 10 thousand miles apart have age-dependent fatality rates very similar to each other. Note that the first QHO compares the plant risk with other accidents. Thus, the all-cause average including deaths from sickness is not the right target for comparison.

The accident average in Figure 1.2.4 indicates 30 fatalities per 100 000 persons. Therefore, the 0.1 per cent requirement yields 0.03 fatalities per 100 000 persons, *i.e.* 3×10^{-7}/(person year). This line is shown with the label of "prompt-fatality objective" in Figure 1.2.4.

The accident-fatality profile reaches its minimum during early teens. The prompt-fatality objective is about 1 per cent of this minimum accident-fatality rate. The objective is also less than 1 per cent of the workers accident rate 3.3×10^{-5} over all industries in Japan. Note that the workers accident rate is calculated from the 1628 fatalities divided by the total number of workers, 50 million.

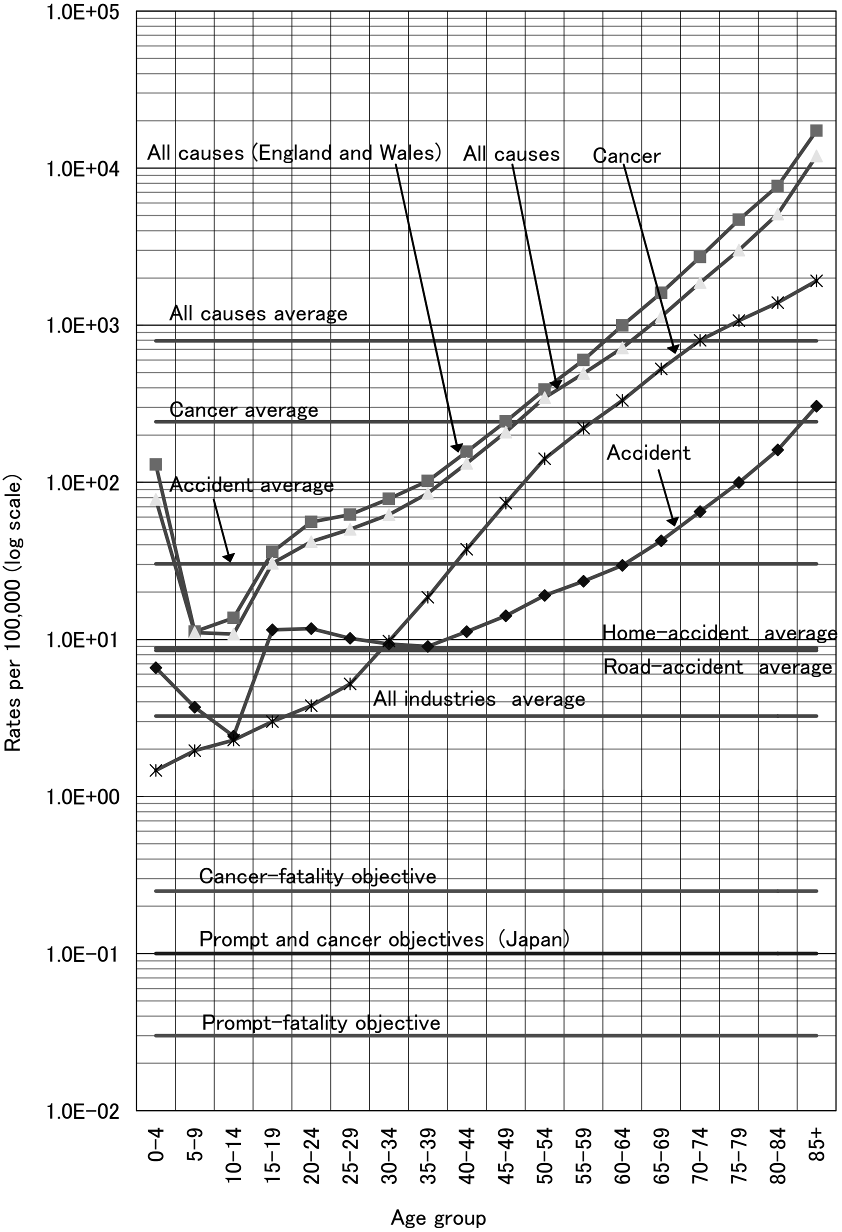


Fig. 1.1. QHOs and fatality statistics

The age average and age profile are also shown for the cancer-fatality rate. There were 309 thousand cancer fatalities in 2003 among the population of 128 million. The 0.1 per cent requirement yields the cancer-fatality objective of 0.25 per 100 000. The line is depicted as the “cancer-fatality objective”, which is less than 20 per cent of the cancer rate for infants when the rate reaches its minimum.

The Nuclear Safety Commission of Japan in December 2004 established a 1 in 1 million individual risk as an objective common to both a prompt- and a cancer-fatality rate. This is about 1/300 of the total accident rate, and 1/2000 of the cancer-fatality rate. The Japanese 10^{-6} per year per person objective is in between the US prompt- and cancer-fatality objectives, as shown in Figure 1.2.4.

1.2.6 Adequate Protection and QHOs

Consider a plant in the US that complies fully with the applicable rules and regulations. The license, rules, and regulations are regarded as a surrogate for an adequate protection ensuring sufficient safety. However, there is a difference of risk levels among the plants with adequate protection provision, and it is likely that some plants have risk levels above the Safety Goals and others have risk levels below the Goals [4]. Those plants with risk levels greater than the Safety Goals are supposed to reduce the risk below the Safety Goal by a so-called backfitting requirement.

The spectrum of the risk levels of the existing plants, on the other hand, provides a way of determining the objectives by a representative risk level among the plants.

1.2.7 Temporary Plant-configuration Goals

The QHOs address plant activities continuing over the year. Risk can be higher for a short period of time during temporary plant configurations such as when important pieces of equipment are taken out of service for preventive maintenance. It may be appropriate to allow a higher risk level if the activity lasts only a short while [3].

1.3 Subsidiary Numerical Objectives

1.3.1 Accident and Public Confidence

A severe core-damage accident will seriously erode public confidence on nuclear power plants. Here, the core damage is defined as exposure and heatup of the reactor core to the point at which prolonged oxidation and severe fuel damage are anticipated and enough of the core is involved to cause a significant release of radioactivity [5].

The Policy Statement published several months after the Chernobyl in 1986 noted that such an accident would not occur at a US nuclear power plant. This aspiration was only indirectly supported by the QHOs that do not directly refer to the core-damage accident.

Commissioner Bernthal, in his separate views attached to the Statement, already stated that:

1) Severe core-damage accidents should not be expected, on average, to occur in the US more than once in 100 years;
2) Containment performance at nuclear power plants should be such that severe accidents with substantial offsite damages are not expected, on average, to occur in the US more than once in 1000 years;
3) The goal for offsite consequences should be expected to be met after conservative consideration of the uncertainties associated with the estimated frequency of severe core-damage and the estimated mitigation thereof by containment.

Assume that 100 plants are operating in the US. The first point described above can be interpreted as 10^{-4}/(reactor-year) as the core-damage frequency (CDF) goal [6].

The Policy Statement also referred to a "general performance guideline" for further staff examination: "Consistent with the traditional defense-in-depth approach and the accident mitigation philosophy requiring reliable performance of containment systems, the overall mean frequency of a large release of radioactive materials to the environment from a reactor accident should be less than 1 in 1 000 000 per year of reactor operation."

This corresponds to a large early-release frequency (LERF) of 10^{-6}/(reactor-year). Here, large early-release is defined as the rapid, unmitigated release of airborne fission products from the containment to the environment occurring before the effective implementation of offsite emergency response and protective actions [5].

As discussed in SECY-93-138, the NRC staff attempted to define a guideline using this LERF of 10^{-6}/(reactor-year), but was unable to do this without making the guideline significantly more restrictive than the QHOs. Work on defining a large release of radioactive material with this associated frequency was terminated in 1993. The general performance guideline was removed from the Policy Statement [3].

Comparison with the QHOs was supposed to be made by using mean values. Uncertainties should have been taken into account by 90% confidence intervals, for instance. However, the QHOs turned out to be difficult to use for regulations because of the large uncertainties in calculating offsite consequences; the prompt- and cancer-fatality risks [7]. A so-called level 3 PRA (Section 5.6) or a consequence analysis were required for the quantification that considered meteorological conditions, geographical features, population density, evacuations, medical treatments, decontaminations, and other dubious factors.

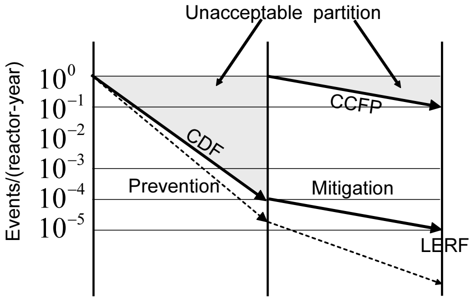


Fig. 1.2. Prevention (CDF) and mitigation (CCFP)

1.3.2 CDF and LERF Objectives

In the 1990 document titled "Implementation of the safety goals", the NRC endorsed objectives concerning the CDF and LERF [8]. These objectives are easier to be assessed because the level 3 PRA is not required. The document stated:

1) A CDF of less than 1 in 10 000 per year of reactor operation appears to be a very useful subsidiary benchmark in making judgments about that portion of our regulations that are directed toward accident prevention.
2) The Commission has no objection to the use of a 10^{-1} conditional containment failure probability (CCFP) objective for the evolutionary light-water reactor design.
3) These two constraints result in a LERF of one in one hundred thousand, since containment failure is necessary for a large release to occur.

These are called surrogate objectives because they are used as alternatives to QHOs. These are also called subsidiary numerical objectives because they support the QHOs. Note that the surrogate objectives are being claimed to be more conservative than the original QHOs. These are also called partitioned objectives because the LERF is divided into CDF (prevention) and CCFP (mitigation), as shown in Figure 1.2.

Release of radioactive materials from the reactor to the environment is prevented by a succession of passive barriers, including the fuel cladding, reactor-coolant pressure boundary, and containment structure. The containment, an imposed exclusion area and emergency preparedness are the essential elements for accident-consequence mitigation [9]. During the core-damage accident, the fuel cladding has been damaged, and the pressure boundary has been failed.

The Nuclear Safety Commission of Japan in March 2006 recommended the same CDF and LERF objectives as the US objectives. Japanese objectives are different in adding an adjective phrase "of the order of" to the US objectives.

The Safety Assessment Principle in the UK is far more conservative: 10^{-7} events per reactor-year for LERF. The Principle assumes a hypothetical person at greatest risk. Furthermore, a dose of 1000 mSv (Section 1.7.1) or more to the hypothetical person should not occur in more than 1 million reactor-years.

1.3.3 Subsidiary Objectives

The endorsement of CDF has the following background [10]:

1) The CDF of 10^{-4} is by *de facto* already used as a fundamental Commission goal.
2) The derivation of a CDF from the QHOs may yield unacceptably large CDFs.
3) A CDF goal together with the CCFP would constitute a fundamental expression of the defense-in-depth philosophy.

The CDF remain subsidiary because [10]:

1) Several operating plants do not meet the CDF of 10^{-4} as measured by their IPEs (individual plant examinations).
2) The CDF goal is difficult to justify on a societal basis (*i.e.* the QHOs follow directly from societal considerations)

Chapter 19 of the USNRC SRP (standard review plan) states that the use of CDF and LERF as the basis for PRA guidelines is an acceptable way of approaching the principle of risk-informed regulations: “When proposed changes result in an increase in CDF, the increases should be small and consistent with the intent of the Commission’s Safety Goal Policy Statement” [9].

The SRP further states that the use of the QHOs *in lieu* of LERF is acceptable in principle and licensees may propose their use. However, in practice, implementing such an approach would require an extension to the level 3 PRA, in which case the methods and assumptions used in the PRA, and associated uncertainties, would require additional attention.

1.3.4 Prevention and Mitigation

The prevention, called active safety, and mitigation, called passive safety, are obviously indispensable functions for the automobile safety. Prevention is an action that reduces the frequency of occurrence of a hazardous event (Section 2.2.1), while mitigation is an action that reduces the consequences of a hazardous event [11].

A CDF goal of 10^{-4} per reactor-year is more conservative than the QHOs. As we already noted, some plants with adequate protection are not “safe enough” from a QHO perspective. Similarly, some plants with “enough safety” from a QHO perspective, are not “safe enough” from a CDF perspective [3]. As a consequence, plants meeting the CDF goal meet the QHOs but could have poor accident-mitigative capability.

Statement of a CDF goal without a LERF (or CCFP) could lead to the impression that the NRC is placing a higher importance on preventive features than on mitigative features, and thus is compromising on its traditional defense-in-depth policy. On the contrary, a LERF goal without the CDF yields the misunderstanding of the Commission's emphasizing mitigative features.

These subsidiary objectives are claimed to be more conservative than QHOs. However, these should be regarded as "minimum guidance" for prevention and mitigation to assure an appropriate defense-in-depth balance. The CCFP is determined in such a manner that additional emphasis on prevention is not discouraged. Some people though point out that the CCFP is too restrictive, especially for a plant during a shutdown (no power) phase because the containment is open for material handling.

These partitioned objectives are not to be imposed as compulsory requirements themselves but may be useful as a basis for regulatory guidance [8]. This is partly because some existing plants do not meet the CDF of 10^{-4}. It seems, however, that the subsidiary objectives will gradually change into mandatory requirements.

1.4 Acceptance Guidelines for Risk Increase

1.4.1 Permanent Change

These CDF, CCFP and LERF values are now used as "benchmark" values for use in risk-informed regulatory decision making [9, 12]. As described in Regulatory Guide 1.174 [12], the plant-specific change from the original design must satisfy the two conditions for CDF and LERF shown in Figures 1.3 and 1.4. These are conditions to ensure that the proposed increases in CDF and LERF are small enough to be consistent with the intent of the NRC's Safety Goal Policy Statement [2].

The following guidelines are cited from Regulatory Guide 1.174 with slight modifications:

1) Decrease: If the change clearly results in a decrease in CDF, the change will be considered to have satisfied the relevant principle of risk-informed regulation with respect to CDF. This region is not explicitly indicated in Figure 1.3 because of the log scale of the vertical axis. The baseline CDF calculation as an absolute value is not required.
2) Increase (Region III): When the calculated increase in CDF is very small (less than 1×10^{-6} per reactor-year, *i.e.* less than the 1% of the CDF benchmark), the change should be considered (*i.e.* reviewed by the NRC) regardless of whether there is an assessment of total CDF.
    2-1) While there is no requirement for the licensee to quantitatively assess the total CDF, information should be provided to show that there is no indication that the total CDF could significantly exceed 1×10^{-4} per reactor-year. If there is an indication that the CDF may be

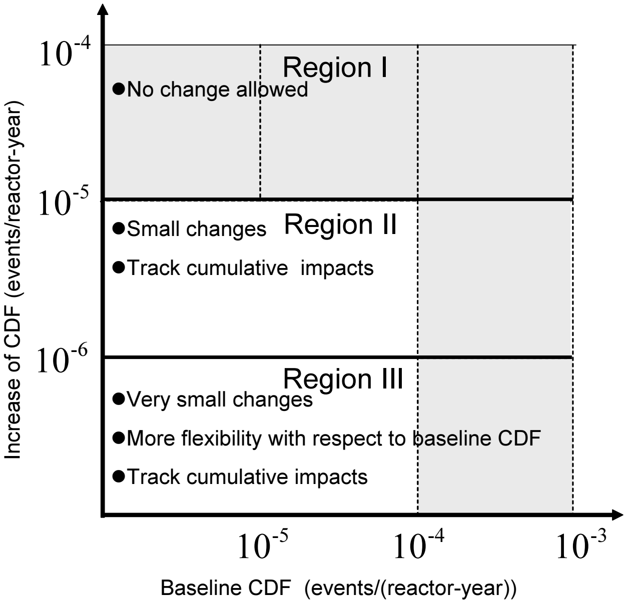

10^{-4}
10^{-5}
10^{-6}
Increase of CDF (events/reactor-year)
Region I
●No change allowed
Region II
●Small changes
●Track cumulative impacts
Region III
●Very small changes
●More flexibility with respect to baseline CDF
●Track cumulative impacts
10^{-5}
10^{-4}
10^{-3}
Baseline CDF (events/(reactor-year))

Fig. 1.3. Acceptance guidelines for CDF (only for indicative purposes)

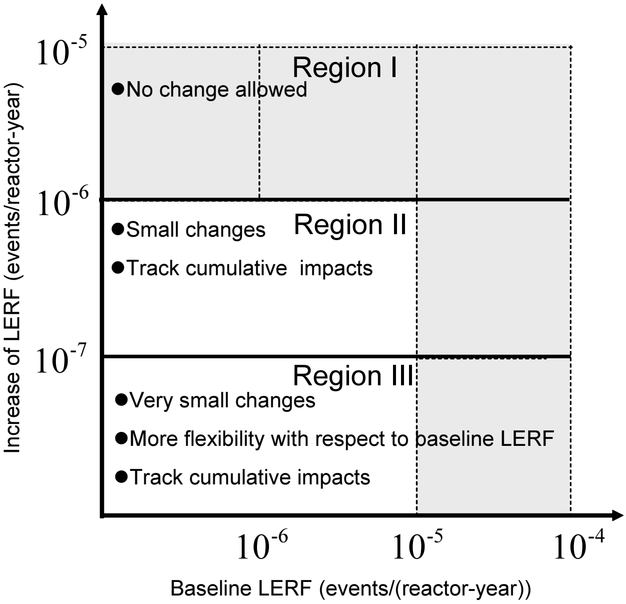

10^{-5}
10^{-6}
10^{-7}
Increase of LERF (events/reactor-year)
Region I
●No change allowed
Region II
●Small changes
●Track cumulative impacts
Region III
●Very small changes
●More flexibility with respect to baseline LERF
●Track cumulative impacts
10^{-6}
10^{-5}
10^{-4}
Baseline LERF (events/(reactor-year))

Fig. 1.4. Acceptance guidelines for LERF (only for indicative purposes)

considerably higher than 10^{-4} per reactor-year, the focus should be on finding ways to decrease rather than increase it.

2-2) Such an indication could result, for example, if the contribution to CDF calculated from a limited-scope analysis significantly exceeds 1×10^{-4} per reactor-year, if the licensee has identified a potential vulnerability from a margins-type analysis, or if plant operating experience has indicated a potential safety concern.

3) Increase (Region II): When the calculated increase in CDF is in the range of 10^{-6} per reactor-year to 10^{-5} per reactor-year, *i.e.* in the range of 1% to 10% of the benchmark CDF, the change should be considered only if it can be reasonably shown that the total CDF is less than 10^{-4} per reactor-year. This implies that a baseline CDF calculation is required.

4) Increase (Region I): When the calculated increase in CDF is larger than 10^{-5} per reactor-year, the change should not normally be considered

Similar guidelines exist for the increase of LERF.

The change may include a combination of two modifications. There may be modification 1 that causes a decrease in CDF and that may be masking the second modification. That is, though the overall change is not risk significant, each modification may be when considered by itself [13]. The overall impact on plant risk is important.

1.4.2 Temporary Change

When the proposed change is temporary, the time span of the change is considered. The integrated conditional core-damage probability (ICCDP) replaces the CDF. Here, the term "conditional" means that the change is in place in calculating ICCDP. The "integrated" indicates an integral over the temporary time span. The term "probability" replaces the "frequency" because CDF is multiplied by time, yielding a unitless quantity.

Temporary changes are often encountered when human actions (HAs) are introduced to compensate an increase in risk. For instance, the risk increases when automatic equipment becomes temporarily inoperable until its recovery. In such a case, manual operations are substituted for the automatic equipment.

ICCDP is defined by:

$$\text{ICCDP} = \mathit{\Delta}\text{CDF} \times T \tag{1.1}$$

where T is the time span that the change is in place.

ICCDP is also called the incremental conditional core-damage probability in Regulatory Guide 1.177. The word "incremental" refers to the incremental increase in risk over the temporary time period. ICLERP, a temporal version of LERF, is defined similarly to ICCDP.

Acceptance criteria similar to those in Regulatory Guide 1.174 (Figures 1.3 and 1.4) were developed because Regulatory Guide 1.174 only considered

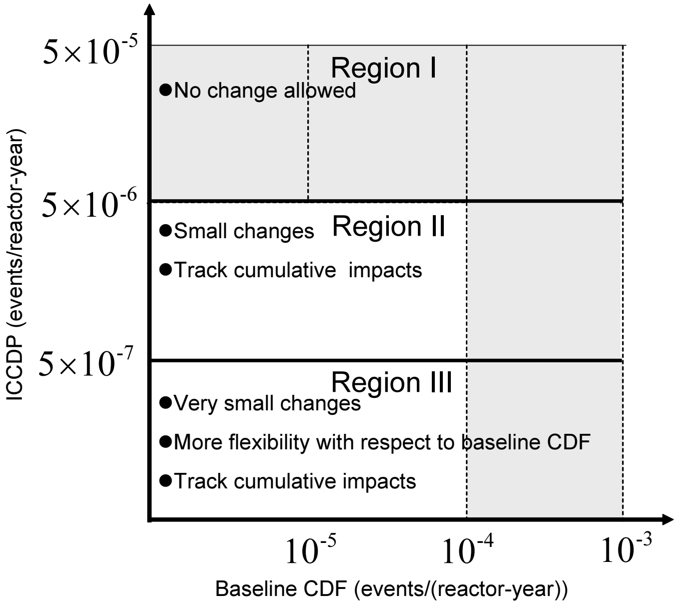

ICCDP (events/reactor-year)
5×10-5
5×10-6
5×10-7
Region I
●No change allowed
Region II
●Small changes
●Track cumulative impacts
Region III
●Very small changes
●More flexibility with respect to baseline CDF
●Track cumulative impacts
10-5
10-4
10-3
Baseline CDF (events/(reactor-year))

Fig. 1.5. Guidelines for integrated risk increase – ICCDP

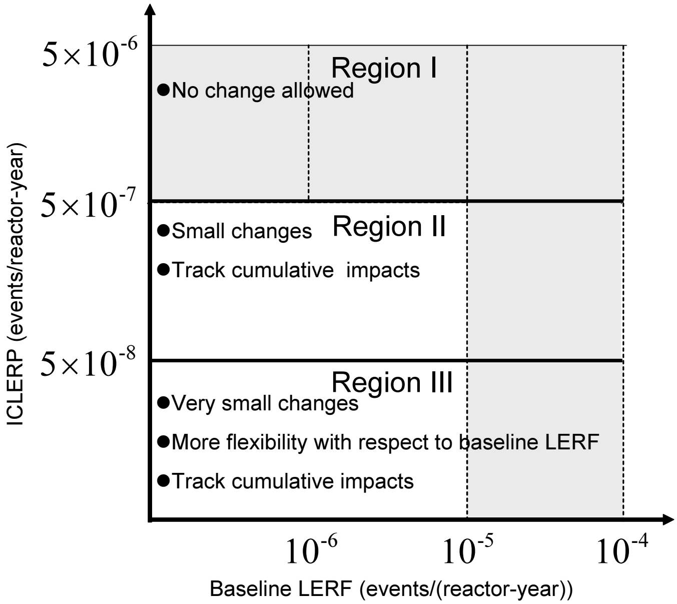

ICLERP (events/reactor-year)
5×10-6
5×10-7
5×10-8
Region I
●No change allowed
Region II
●Small changes
●Track cumulative impacts
Region III
●Very small changes
●More flexibility with respect to baseline LERF
●Track cumulative impacts
10-6
10-5
10-4
Baseline LERF (events/(reactor-year))

Fig. 1.6. Guidelines for integrated risk increase – ICLERP

permanent changes. The Regulatory Guide 1.177 [14] addresses the acceptability of integrated risk over periods when equipment is out-of-service for the allowed outage time (AOT). A preventive maintenance such as an emergency diesel-generator overhaul while the plant is at power should be completed and the equipment operability is restored within the AOT.

An acceptability limit of 5×10^{-7} per reactor-year for ICCDP is considered a small risk increase for a single AOT. This 5×10^{-7} value is chosen as the boundary between Regions II and III for ICCDP. The selected boundary between Regions I and II is 5×10^{-6} events per reactor-year, an increase of one order-of-magnitude. These boundary values result in Figure 1.5. Figure 1.6 is obtained in a similar manner to Figure 1.5 [13].

This approach would accept potentially large increases in risk if the modification is in place for a short period of time.

Related changes should be bundled as a package because the overall impact on plant risk is important. Risk tradeoffs can be performed by packaging, which is regarded as a significant benefit of risk-informed regulation [15]. However, the cumulative, synergetic effect of these changes should be considered, including possible dependencies and changes to the operating environment. For larger values of integrated risk (Region I), there may be a need to impose temporary restrictions on multiple changes during the same time period [13]. No clear statement is available for the maximum acceptable number of changes per year each of which is performed in a different time period.

1.5 Treatment of Uncertainties

The USNRC declares in the Policy Statement in August 1995 that the safety goals for nuclear power plants and subsidiary numerical objectives are to be used with appropriate consideration of uncertainties [16].

There are at least two types of uncertainty [8].

1) Aleatory uncertainty: This exists when an event occurs in a random manner. This uncertainty can be expressed in terms of probability or frequency. For instance, the aleatory uncertainty of a fair dice is expressed by the probability of each face to be 1/6. A quantitative risk assessment quantifies the aleatory uncertainties about the occurrences of harmful events.
2) Epistemic uncertainty: This has been referred to as state-of-knowledge uncertainty. There would be no epistemic uncertainty when the true value of aleatory uncertainty can be expressed by exact probabilistic numbers. Thus, the probability 1/6 for the die is free from any epistemic uncertainty. The existence of this epistemic uncertainty makes decision making under risk difficult and controversial. This uncertainty is classified into three types.
   2-1) Parameter uncertainty: The model for expressing the aleatory uncertainty is perfect but has one or more unknown parameters to be estimated with errors. Assume that a component lifetime is distributed

with an exponential distribution. This distribution has a single parameter called a failure rate. The error in the component-failure-rate estimation generates a parameter uncertainty.

The parameter uncertainty is caused by factors such as statistical uncertainty due to finite component test data, or data-evaluation uncertainty due to subjective interpretations of failure data. The data-evaluation uncertainty may be greater than the statistical uncertainty because the latter could be reduced by a variety of traditional, theoretical approaches.

2-2) Modeling uncertainty: The models for the aleatory uncertainties may not be realistic because of various approximations and assumptions that are made, for instance, for human performance and common-cause failures as well as for complicated physical processes such as reactor coolant-pump seal behavior upon loss of seal cooling. An introductory example is an exponential lifetime distribution when the component follows a wearout failure. This gives rise to a modeling uncertainty. A model describing not a frequency but a consequence may have modeling (or parameter) uncertainty. This leads to the uncertainty about severities of harm.

2-3) Completeness uncertainty: The calculated risk has errors from the true risk when there exist unanalyzed contributors such as earthquakes, fire and flood. Exceptional operations such as low-power and shutdown modes may be left unanalyzed. With respect to human actions, we can not analyze all the commission errors because there are, in theory, countless number of errors of the commission type. The incompleteness is a scope limitation, and causes deviations from realism.

The random hardware failure is a typical example of the aleatory uncertainty. This type of failure is defined as a failure occurring at a predictable rate but at an unpredictable (*i.e.* random) time, which results from one or more of the possible degradation mechanisms in the hardware [1, 11].

The so-called systematic failure, on the other hand, is defined as a failure originated in a deterministic way from a certain cause, which can only be eliminated by a modification of the design, the manufacturing process, the operational procedures, the documentation or the other relevant factors. Human error is a typical root cause of the systematic failure such as software bugs. A document describes the initial specification for the software of programmable logic controllers (PLC). Incorrect specifications in the document yield PLC failures. A superficial corrective maintenance without fundamental modification of root causes would not eliminate the cause of systematic failures [1, 11].

The failure rate of the random hardware failure can often be predicted with reasonable accuracy, while the rate of systematic failure cannot be accurately predicted. The systematic failure can be regarded as a major contributor to the modeling uncertainty.

Propagations of the parameter uncertainties yield distributions of the risk estimation, *i.e.* distributions of probability and consequence. Other epistemic uncertainties are dealt with by sensitivity studies rather than uncertainty propagations.

As discussed in Regulatory Guide 1.174, if the PRA is not full scope (completeness uncertainty), the impact of the change must be considered by supplementing the PRA evaluation by qualitative arguments or by bounding analyses [17].

The degree of uncertainty analysis depends on risk levels. In Regions II and III of Figure 1.3, the closer the CDF estimate to its corresponding acceptance guideline 10^{-4}, the more detail will be required in the assessment of the CDF value and the analysis of uncertainties. If the estimated CDF value is very small compared to the 10^{-4} value, a simple bounding analysis may suffice with no need for a detailed uncertainty analysis.

1.6 Risk-informed Integrated Decision Making

The risk-informed integrated decision making is a complementary utilization of deterministic and probabilistic approaches to satisfy the safety goals. This is completely different from a *risk-based* decision making that is solely based on numerical risk-value estimates.

1.6.1 Deterministic Approach

This approach proceeds in the following way:

1) Define a specific set of initiating events. These are called design basis events.
2) Assume a single active failure along each accident sequence initiated by the design basis event. The introduction of single failure is required to assure a so-called single-failure criterion.
3) Analyze whether the plant design and operation can successfully prevent and mitigate the accident sequence, given the initiating event and the single failure.

When the analysis shows a successful outcome, there is good reason (within the single-failure criterion) to believe that the plant withstands the specific set of design basis events [9]. This approach is called deterministic because there is little explicit consideration of the probability of occurrence of the design basis events and single-failure event, except for the rare-event exclusion for extreme cases such as a pressure-vessel rupture, *etc.* It is “determined” that the design basis events and the single-failure event could occur, and the plant is designed and operated to withstand such events.

This deterministic approach was developed when there was a scarcity of data from actual plant operation. It is based on the principle that the deterministic events would serve as a surrogate for the broad set of initiating events that could be realistically expected over the life of the plant [18]. This is also called a qualitative or traditional approach.

The TOR document of the UK HSE [19] also states that there were times when no methods were available for quantification of the risk. The main safety precaution was therefore to ensure that all items of plant were exceedingly robust and that several layers of safety were built in where there was thought to be some chance of failure.

The term "design basis accidents" implies that the plant design and operation based on the deterministic approach can successfully prevent and mitigate the accident sequence so that they do not produce unacceptable consequences. Thus, any release bigger than a design basis accident could only occur as the result of the sequential failure of several levels of safety protection, or as the result of some major and very unlikely event, such as the failure of the very strong vessel surrounding the reactor core. Such larger releases are called "beyond design basis" accidents [19].

1.6.2 Probabilistic Approach: PRA

Data about actual transients, accidents, and plant equipment failures have been accumulated and accident sequences became available to estimate the overall risk from plant operation. These sequences have far more variety than the deterministic sequences because the failures are not restricted to the single failure. At the present time each US plant has performed a PRA. The generic and plant-specific data are used for the PRAs to describe risk in terms of the frequency of reactor core-damage and significant offsite release, *etc.* [18].

1.6.3 Integrated Decision Making

The operating plant and its modifications should be consistent with the current philosophy of risk management: "The final or bottom line numbers obtained by the PRA should not be the only input to the decision making process, and other concepts such as defense-in-depth must be maintained" [15].

Decisions are expected to be made in an integrated fashion, considering traditional engineering and PRA risk information, and may be based on qualitative factors as well as quantitative analyses and information [12].

1.6.4 Decision Making Principles

Proposed changes of plant are expected to meet a set of key principles of Regulatory Guide 1.174. These principles are:

1) The proposed change meets the current regulations unless otherwise stated.
2) The proposed change is consistent with the defense-in-depth philosophy.
3) The proposed change maintains sufficient safety margins.
4) When proposed changes result in an increase in core-damage frequency or risk, the increases should be small and consistent with the intent of the Commission's Safety Goal Policy Statement [2].
5) The impact of the proposed change should be monitored using performance-measurement strategies.

Obviously, not only the proposed changes but also the existing designs and practices are expected to meet these key principles. The term "proposed change" can be replaced by "current status".

The first principle is related to the adequate-protection concept, the second principle to the famous defense-in-depth and the third principle to safety margins. The fourth principle is evaluated through the subsidiary numerical objectives described in Section 1.3. The last principle is the requirement after the implementation of the proposed change. The performance-measurement strategies correspond the last two phases (CA) of the plan, do, check, and action (PDCA) cycle. For instance, assumptions and equipment-reliability levels used in the PRA should be monitored and maintained. The second and the third principles are described below in more detail.

1.6.5 Defense-in-depth

Roles and Examples

A baseball game has essential aspects of defense-in-depth. There are four bases: first, second, third, and home. A run is scored only when a runner goes through the bases to the home. Only a homerun can break the four-base defense-in-depth at a swing. The game also has other protection layers; there are 9 innings in total, and the fielders are separated into infielders and outfielders.

The defense-in-depth provides us the time margin untill the hazardous events final occurrence. As a matter of fact it is rare that all the layers fail at the same time. A failure of a protection layer can be detected, and corrective measures can be established accordingly. A relief pitcher shows up. The defense-in-depth allows designs based on diversity, independence, early detection and treatment.

The IAEA document lists passive physical barriers and levels of protection arranged into a defense-in-depth format for a nuclear power plant [20]:

1) First barrier: fuel matrix.
2) Second barrier: fuel-rod cladding.
3) Third barrier: primary coolant boundary.
4) Fourth barrier: confinement.
5) First level: prevention of deviation from normal operation.

6) Second level: control of abnormal operation.
7) Third level: control of accidents in design basis.
8) Fourth level: accident management including confinement protection.
9) Fifth level: offsite emergency response.

Defense-in-depth for the nuclear power plant uses multiple means to accomplish safety functions and to prevent the release of radioactive materials. Defense-in-depth is important in accounting for uncertainties in equipment and human performance, and for ensuring some protection to remain even in the face of significant breakdowns in particular areas. Defense-in-depth may be changed but overall should be maintained [13].

Conditions for Defense-in-depth

Consistency with the defense-in-depth philosophy is maintained, for instance, for a nuclear power plant if:

1) A reasonable balance is preserved among prevention of core damage, prevention of containment failure, and consequence mitigation.
2) There is no overreliance on programmatic activities to compensate for weaknesses in plant design.
3) System redundancy, independence, and diversity are preserved commensurate with the expected frequency, consequences, and uncertainties.
4) Defenses against potential common-cause failures are preserved, and the potential for the introduction of new common-cause failure mechanisms is assessed. For instance [13], caution should be exercised to provide adequate assurance that the possibility of significant common-cause operator errors are not created.
5) Independence of barriers is not degraded.
6) Defenses against human errors are preserved. For instance [13], procedures are established for an independent check in a way that safety-significant actions have been properly executed.
7) The intent of the General Design Criteria in Appendix A to 10 CFR (Code of Federal Regulations) Part 50 is maintained.

Obviously, almost the same conditions should apply to the non-nuclear plants.

Prevention of core damage and prevention of containment failure in the first condition are quantified by CDF and CCFP, respectively. For non-nuclear plant for instance, an accident corresponds to the core damage, and a release of harmful substance to the containment failure. The consequence mitigation includes offsite emergency evacuations.

The programmatic activities in the second condition are typified by operator actions following a procedure [13].

According to IEC 61511-1 [11], the redundancy in the third condition is defined as the use of multiple elements or systems to perform the same function; redundancy can be implemented by identical elements (identical redundancy) or by diverse elements (diverse redundancy). Reference [19] and this book limit the redundancy only to the identical redundancy.

The diversity is defined as the existence of different means of performing a required function (IEC 61511-1). The backup via dissimilar components is called design diversity (TOR). The diversity is also defined as a replication of an activity or structure, system, train or component requirement using a different design or method [18]. More descriptions of diversity are found in Section 3.4.3

The dissimilar components are expected to fail independently. A typical example is two emergency feedwater systems, one using electrical drives and the other steam turbines. Different engineers designing diverse computer software, independently tackling the same problem, sometimes make similar mistakes due to a common specification error, thus creating a chance that these will fail simultaneously [19].

Dependent failures are defined as events whose probability cannot be expressed as the simple product of the unconditional probabilities of the individual events (IEC 61511-1). More precisely, two failure events A and B are dependent if $\Pr\{A \text{ and } B\} > \Pr\{A\}\Pr\{B\}$. In other words, failure event B is more likely to happen, given the occurrence of event A. A common-cause failure is representative of dependent failures.

There are a total of 55 General Design Criteria referred to in the seventh condition. These are minimum requirements and are divided into 6 classes: 1) overall requirements (5), 2) protection by multiple fission-product barriers (10), 3) protection and reactivity control systems (10), 4) fluid systems (17), 5) reactor containment (8), and 6) fuel and radioactivity control (5). Each class has the total number of criteria shown in the parentheses. Two examples of criteria are shown below:

1) Criterion 1 – Quality standards and records. Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified as necessary to assure a quality product in keeping with the required safety function. A quality-assurance program shall be established and implemented in order to provide adequate assurance that these structures, systems, and components will satisfactorily perform their safety functions. Appropriate records of the design, fabrication, erection, and testing of structures, systems, and components important to safety shall be maintained by or under the control of the nuclear power unit licensee throughout the life of the unit.
2) Criterion 14 – Reactor coolant pressure boundary. The reactor coolant pressure boundary shall be designed, fabricated, erected, and tested so as to have an extremely low probability of abnormal leakage, of rapidly propagating failure, and of gross rupture.

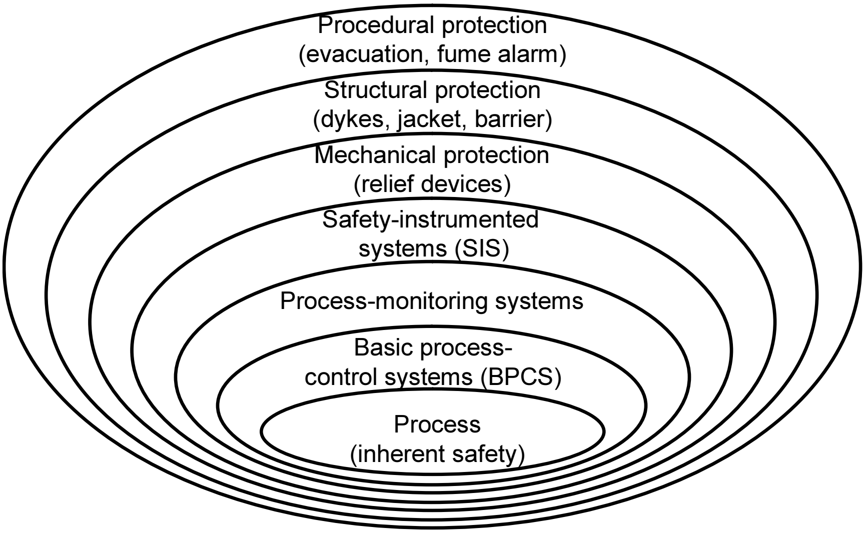


Fig. 1.7. Protection layers of the process industries (IEC 61511)

Protection Layer

The term "protection layers (PLs)" is used in process industries to represent the defense-in-depth concept [11]. A protection layer consists of a grouping of equipment and/or administrative controls that function in concert with other protection layers to prevent or mitigate process risk. Dependability and auditability are demanded, in addition to independence.

1) Dependability: The PL can be counted on to do what it was designed to do by addressing both random hardware failures and systematic failures.
2) Auditability: A PL is designed to facilitate regular validation of the protective functions. Here, the validation is defined as an activity of demonstrating that the function meets in all respects the requirements specification.

A condition for the protection layer is that it reduces the risk by at least a factor of 10. However, this requirement does not always apply to the terminology of protection layers.

Figure 1.7 displays the concept of protection layers:

1) Basic process-control systems (BPCS): These are used for the correct operation of the plant within its normal operating range. This includes measuring, controlling and/or recording of all the relevant process variables. Basic process-control systems are in continuous operation or frequently requested to act and intervene before the action of a safety-instrumented system is necessary. This type of system does not need to be implemented according to the IEC 61511 standard that deals only with the safety-instrumented systems. A typical example in continuous operation is a

temperature-control system. An example of the intermittently operating BPCS is a timer mechanism to initiate power supply and shutdown.

2) Process-monitoring systems: These act whenever one or more process variables leave the normal operating range. The systems alert the operators or induce manual interventions. This type of system does not need to be implemented according to the IEC 61511 standard. An example is a pressure sensor to initiate a high-pressure alarm and alert the operator to take appropriate action to stop feeding material.
3) Safety-instrumented systems (SIS): A SIS consists of sensors, logic solvers, and final elements implementing the physical action. The SIS either prevent a hazardous event or mitigates the consequences of a hazardous event. The SIS needs to be implemented according to the IEC 61511. BPCS and monitoring systems reduce the demand rate to the SIS. The failure of BPCS thus increases the demand.
4) Mechanical protection: Relief valves and rupture discs are typical examples.
5) Structural protection: This is physical barriers such as pressure vessel, containment, dyke, *etc.*
6) Procedural protection: There are the plant emergency response and the community emergency response based on procedures and broadcasting.

1.6.6 Sufficient Safety Margins

Safety margins often used in deterministic analyses to account for uncertainty and provide an added margin to give adequate assurance that the various limits or criteria important to safety are not violated [13].

Sufficient safety margins are maintained if codes and standards or their alternatives approved for use by the regulatory agency are met or sufficient margin is provided to account for uncertainty of analysis and data (see Section 3.5 for more detail).

1.7 Tolerability of Risk and ALARP

The tolerability of risk concept [19] partly originated from radiation risk.

1.7.1 Radiation Fatality Risk

An “effective dose” or simply a “dose” is a total amount of radiation that our body receives from external plus internal sources. The unit of the effective dose is the milisievert (mSv).

The average annual dose from natural radiation excluding those of radon is 1 mSv in the UK. The average radon dose is slightly more than 1 mSv. The International Commission on Radiological Protection (ICRP) recommended in 1990 that 1 mSv per year is the tolerable limit for members of the public. This is a manmade dose and does not include medical nor natural radiations.

The ICRP also recommended for employees the limit of 20 mSv a year on average over a five-year period with no more than 50 mSv in any one year. This was based on the annual fatality rate of 10^{-3} per employee, which is intolerable. Employers are expected to ensure that the actual doses are lower, down to the level justifiable by “as low as reasonably practicable” (ALARP) principle. As a consequence, the average dose for workers at nuclear installations is roughly 1 mSv per year with some maintenance workers receiving doses from 5 to 15 mSv.

If a person received 5000 mSv over a few hours, severe depletion of the white blood cells leads to a high probability of death in the following few weeks. A dose of 50 000 mSv would cause a quick death. These are called early effects.

As a rule of thumb the 1 mSv per year received uniformly over a lifetime causes 5 additional fatal cancers per year in the population of 100 000. These cancers increase proportionally with the annual dose. The increment of cancers are called late effects because the cancer outbreaks 10 to 20 years after the exposure. The statement of “5 additional fatal cancers per year” should be interpreted as the rate of having “damaged cells” that will eventually develop into a cancer one or two decades later. The additional risk does not refer to a particular time of death.

The average period of life lost by the early effect is estimated as 35 years, while the lost period by the late effect is 15 years [19]. The US prompt-fatality objective in Figure 1.2.4 is smaller than the cancer-fatality objective, and this is conceptually consistent with the lost year ratio of 15/35, although the actual ratio of objectives is far smaller, 3/25 from Figure 1.2.4.

The ICRP recommendation for public members, 1 mSv/year, thus causes 5 cancers per year out of 100 000. About 240 people per 100 000 die annually from cancer in Japan, as shown in Figure 1.2.4. Therefore, roughly 5 additional cancers to 240 result from the ICRP recommendation. This corresponds to 1) a 2% increase of cancers, and to 2) the annual mortality-rate increment of 5×10^{-5}/year.

The ICRP recommendation for workers, 20 mSv/year, corresponds to 1) a 40% increase of cancers, and to 2) the annual mortality-rate increment of 10^{-3}/year, which is intolerably high without the ALARP effort.

Suppose that the annual dose continues throughout a lifetime. Applying the rule of thumb, the average risk of death per year associated with an annual dose is summarized in Table 1.1. The average risk of death at nuclear installations would be between 5 in 100 000 (1 mSv) and 25 in 100 000 (5 mSv) per year with a risk of 10 in 100 000 (2 mSv) or better at power stations.

Table 1.1. Annual dose and annual fatality risk

Remarks	Dose/year increment	Fatality risk/year increment
Nuclear min	1 mSv	5 in 100 000
Nuclear power	$\leq$ 2 mSv	10 in 100 000
Nuclear max	5 mSv	25 in 100 000
Nuclear exceptional	15 mSv	75 in 100 000

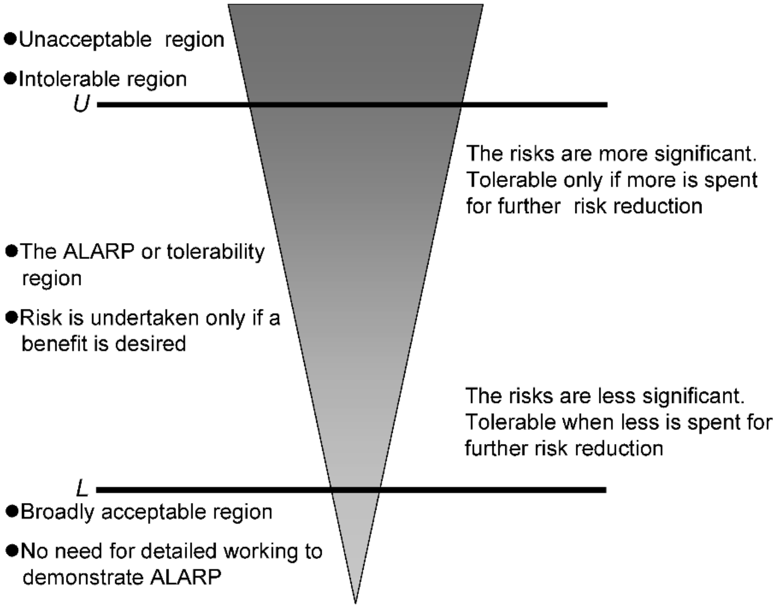

●Unacceptable region
●Intolerable region
U
The risks are more significant. Tolerable only if more is spent for further risk reduction
●The ALARP or tolerability region
●Risk is undertaken only if a benefit is desired
The risks are less significant. Tolerable when less is spent for further risk reduction
L
●Broadly acceptable region
●No need for detailed working to demonstrate ALARP

Fig. 1.8. Unacceptable, ALARP and broadly acceptable regions

1.7.2 TOR Requirements

The TOR requirements of the UK HSE originally came from regulations of cancer-producing materials such as radioactive materials and asbestos, and toxic substances such as lead. The three regions of TOR are illustrated in Figure 1.8. The TOR concept plays a role when the risk level in question exceeds the broadly acceptable level. The US Safety Goal Statement, on the other hand, defines the broadly acceptable risk level that a nuclear power plant must not exceed.

The IEC 61511-3 and Safety Assessment Principles for Nuclear Power Plants by HSE state the TOR concept as:

1) Unacceptable region: An upper level *U* beyond which the risk is so large that it is refused altogether in any ordinary circumstances. If such a risk exists it should be reduced by preventive measures so that it falls in either

the "tolerable" or "broadly acceptable" regions, or the risk should be abandoned.

2) Broadly acceptable region: A lower level L below which the risk is so small and insignificant in the sense that the risk does not worry us or cause us to alter our ordinary behavior.
    2-1) The regulator need not ask employers to seek further improvement.
    2-2) Nevertheless employers might decide to spend even more to reduce the risk, and some do.
    2-3) It is necessary to remain vigilant to ensure that the risk remains at this level by the precautions maintained.
3) The risk falls between U and L.
    3-1) The risk is considered to be "tolerable" provided that it has been reduced until the cost of risk reduction, whether in money, time, or trouble, is grossly disproportionate to the risk averted, and provided that regulations and generally accepted standards have been kept towards the control of the risk.
    3-2) The higher the risk, the more would be expected to be spent to reduce it.
    3-3) In short, risk must be reduced to a level that is ALARP including the conformity with the regulations and standards; this is the ALARP principle.
    3-4) The risk thus reduced is called tolerable risk.

The TOR report suggested that the maximum tolerable risk U for any worker was set at around 1 in 1000 per year, which is compatible with the ICRP 1990 recommendation of 20 mSv per year.

Note that the employers are legally required to reduce the risk by following the best industrial practice, not just to stick at the level U that is regarded as marginally intolerable. Thus, ALARP (strengthened by the gross proportionality) allow the UK HSC (Health and Safety Commission) to demand much lower risks to the employers. Fatality rates for most workers in any industry in the UK are well below this upper limit. As a result, most industries have been subjected to ALARP constraints.

The HSC gives 10^{-4} per year as the maximum level U of individual risk for the general public who have a risk imposed on them "in the wider interest of society". The risk of 10^{-4} per year to any member of the public is the maximum that should be tolerated from any large industrial plant in any industry. Of course, the ALARP principle ensures that the risk from most plant is in fact lower or much lower.

However, HSC adopted a risk of 10^{-5} per year, 10% value of the ordinary U, as the benchmark for new nuclear power stations in the UK, recognizing that this is, in the case of a new station, broadly achievable and measurable.

The lower bound L is one in a million per year because it is extremely small when compared to the background level of risk. This happens to be the same order as the US and Japanese objectives shown in Figure 1.2.4.

1.7.3 Applying TOR Framework

Important components for applying the TOR framework are authoritative good practice precautions (AGPP). The sources of AGPPs include:

1) Prescriptive legislation, approved codes of practice and guidance produced by Government.
2) Standards produced by standards-making organizations (*e.g.* BS, CEN, CENELEC, ISO, IEC, ICRP)
3) Guidance agreed by a body representing an industrial or occupational sector (*e.g.* trade federation, professional institution, sports governing body).

The TOR framework is worked out according to steps described in r2p2 literature [21]. A condensed version of these steps is:

1) Duty holders must have in place suitable controls to address all significant hazards arising from their undertakings. Those controls should, as a minimum, implement AGPPs, irrespective of specific risk estimates.
2) Regard a hazard as significant unless otherwise shown.
3) In most cases an option is available for reducing the risks to a tolerable level. When no option is available for the reduction, we are dealing with activities located in the upper, “intolerable” region of the framework. We shall give consideration of banning or remedying these activities or processes.

1.8 Explicit Consideration of Societal Risk

There are statistics that show the worldwide frequency of chemical accidents causing 100 or more deaths is about 0.25 per year [19]. HSE proposes that the risk of an accident causing the death of 50 people or more in a single event should be regarded as intolerable if the frequency is estimated to be more than one in five thousand per year (per facility).

1.8.1 Individual and Societal Risk

Terms “individual risk”, “societal risk” and “probable loss” are defined in the following way for the fatality. Refer to [22] for more general definitions including harms other than fatality.

Individual risk of fatality is the frequency per year at which the most exposed individual may be expected to die from the realization of specified hazards [11].

The individual risk can be calculated independently of how many other people die simultaneously by a single event. This risk is not affected by the population size exposed to the accident. The individual risk from the airplane accident is independent of how many other passengers are aboard simultaneously.

The society, however, would not accept a large number of fatalities even if the risk per individual is small. The societal objection would be stronger when a sizable number of people die simultaneously by a single accident. The societal risk is an extreme version of common-cause failures where simultaneity is a concern.

As is seen from the recent US NRC activities, however, the trend is that explicit treatment of societal risk is almost being discarded as an “academic indulgence” at least for a while, and that the surrogate objectives are introduced to replace both individual and societal risks. This book describes the societal risk in some detail because not a few people still expect societal goals to be quantified by PRA.

We tend to show a great deal of concern about a single event killing a large number of people. This is partly because such an event may frequently cause other consequences such as serious local disruption, land contamination, loss of plant, loss of electricity, and the fear and anger. The number of fatalities obviously has a strong correlation with the population exposed. When the individual risk is sufficiently small, then the societal risk can often be kept small.

1.8.2 Graphical Representation of Societal Risk

Societal risk of fatality can be visualized as the relationship between the frequency and the number of fatalities in a given population from the realization of specified hazards.

A widely used criterion of societal risk is based on an N–f plot, where the horizontal axis N is the number of fatalities, and the vertical axis f is the annual frequency [11] (Figure 1.9). This curve visualizes the societal risk by a frequency distribution of simultaneous fatalities by an accident of the single facility. The risk-neutral line is the line on which the expected number of fatalities remains a constant. The risk-aversive line is steeper than the neutral line. The expected number of fatalities on the aversive line decreases with the size N of fatalities of the horizontal axis. An example of a risk-aversive societal goal is given in Section 2.2.5.

The only feasible procedure is to select an accident of a considerable size, treat it as a point of reference, and compare it with other major events to find a feasible anchor point on an N–f plot. We then have to make allowance for the possibility of much larger and exceedingly improbable events and much smaller ones that are more likely [19].

Figure 1.10 is a conceptually simpler version of the N–f plot. The horizontal axis is money loss, while the vertical axis is a frequency per six months. The line is a constant expected loss line of \$300. There are 5 scenarios from an accident, almost satisfying the expected loss criterion.

A well-known Farmer curve consists of points (N, F) where symbol F indicates the annual frequency of N or *more* fatalities caused by the same facility. This is also called an N–F curve. The N–f and N–F curves are

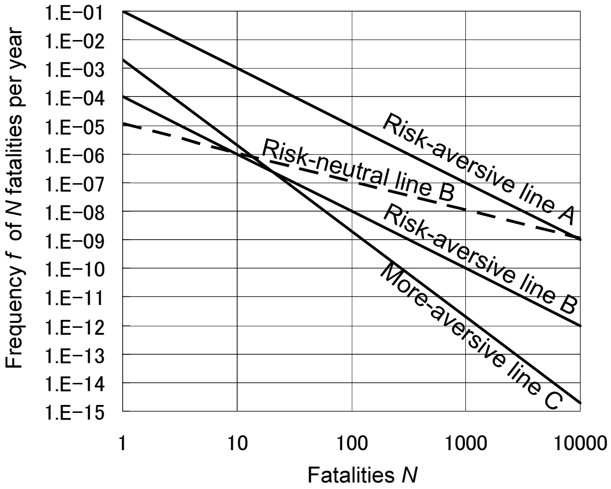


Fig. 1.9. Risk criteria represented by N–f curves

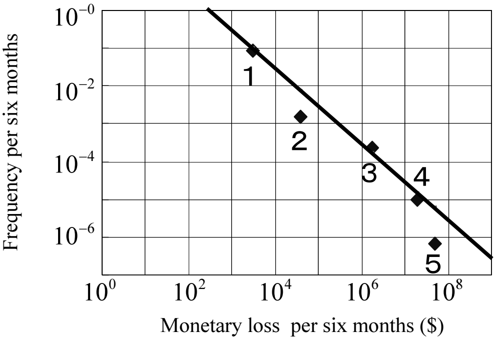


Fig. 1.10. An example of a risk-neutral criterion

frequently expressed on a log-log scale. These two curves can often be used to visualize societal risk goals of fatality. An example is shown in Figure 1.11 [22]. Note that the risk-neutral line in the N–f plot becomes a curved line for the N–F plot. Both lines A and B are risk aversive in Figure 1.11.

The societal risk is a subset of societal concerns that are defined as risks that, if realized, could have adverse repercussions for the institutions responsible for protecting people [21].

A so-called collective risk of fatality also has a population-size effect. This is defined as a diffuse risk associated with exposure to hazardous materials. Fatalities increase monotonically with respect to the population exposed.

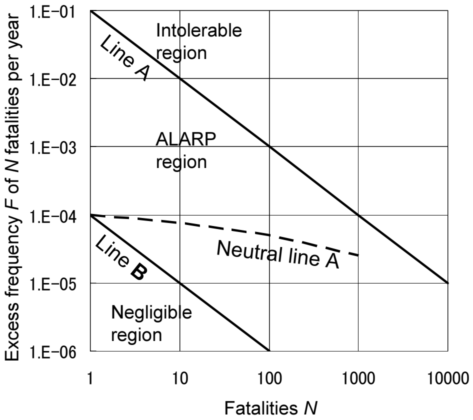


Fig. 1.11. Risk criteria on N–F curve by UK Advisory Committee on Dangerous Substances (ACDS) (1991)

The probable loss of mortality is the expected number of fatalities calculated as a sum of products of frequency and fatalities.

1.8.3 Example: Individual and Societal Risks

Example Description

Consider a hypothetical installation located at the center of Figure 1.12. The circular area around the installation is divided into four ranges. The first one is within 1 km from the installation, the second one is from 1 km to 5 km, the third one is from 5 km to 10 km, and the forth one is from 10 km to 15 km. Each range is further divided into four directions, resulting in 16 areas: NE1 to NE4, NW1 to NW4, SW1 to SW4, and SE1 to SE4.

Population size is denoted for each area in Figure 1.12. For instance, the north-east area NE1 in the first range has 10 persons, while the south-east area SE4 in the fourth range 10 000 persons.

Suppose that a large release of poison gas occurs with a frequency of once per 10 000 years. Persons living in each range are killed by the release accident with the percentage denoted in Figure 1.12, provided that the wind is directed toward the corresponding areas. Thus, all the 10 people die in NE1 by the release accident during a north-east wind. The percentage decreases with the radius from the plant.

Assume that meteorological data yield probabilities of the wind directions listed as fractional numbers in the figure. For instance, a NE wind occurs with probability 1/2, a NW wind with 1/8, a SW with 1/4, and a SE with 1/16. The remaining 1/16 is the probability of calm when no fatality is assumed to occur because the released gas would not disperse.

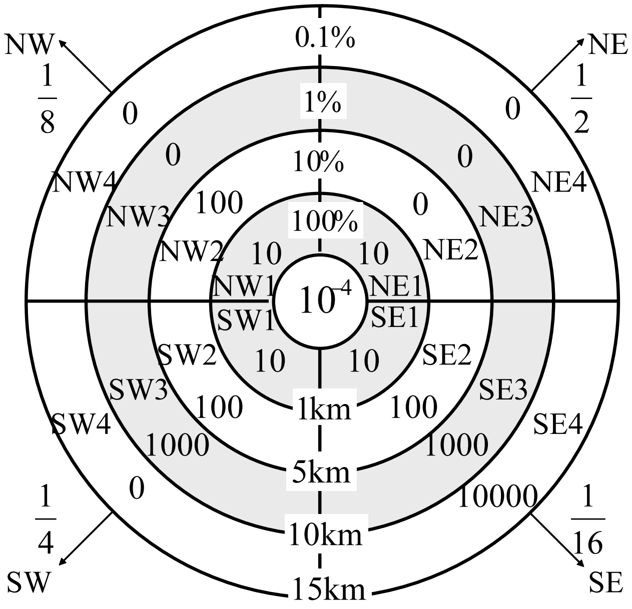


Fig. 1.12. Poison-gas release event to define individual and societal risks

Individual Risk

Consider the individual risk in area NE1. A person will be killed in the area when 1) the release event occurs, 2) the wind direction is north-east, and 3) the gas has a fatal effect on the person. The event frequency is 10^{-4} per year, the wind direction probability is 1/2, and the fatal-effect probability is unity. Thus, the fatal frequency per year for the person is $10^{-4} \times 0.5 \times 1 = 5 \times 10^{-5}$.

Individual risks in the 16 areas are listed in Table 1.2. Figure 1.13 shows the individual risks as a function of distance from the plant. We see that the north-east areas have the highest individual risks, while the south-east areas have the lowest. This is due to the wind-direction probabilities. Note that the individual risks have been calculated without recourse to the population size in each area.

Societal Risk

Row [A] of Table 1.2 shows that the release accident with the north-east wind occurs with annual frequency 5×10^{-5}. The fatal probability of the NE1 area is unity, and thus 10 people are killed by the accident with the wind. The other NE areas produce no fatalities because these areas are uninhabited.

Row [B] indicates that the accident with the north-west wind occurs with frequency of 1.25×10^{-5}. Area NW1 produces 10 fatalities from the accident because the fatality probability is unity. Area NW2 yields the same number of fatalities because of the population of 100 and the fatality probability of 0.1.

Table 1.2. Individual and societal risks of the 16 areas

[A] Event under NE wind: frequency of 5×10^{-5} and fatalities of 10

Area	Population	Event frequency	Wind probability	Fatality probability	Individual risk	Fatalities under wind
NE1	10	10^{-4}	0.5	1	5×10^{-5}	10
NE2	0			0.1	5×10^{-6}	0
NE3	0			0.01	5×10^{-7}	0
NE4	0			0.001	5×10^{-8}	0

[B] Event under NW wind: frequency of 1.25×10^{-5} and fatalities of 20

Area	Population	Event frequency	Wind probability	Fatality probability	Individual risk	Fatalities under wind
NW1	10	10^{-4}	0.125	1	1.25×10^{-5}	10
NW2	100			0.1	1.25×10^{-6}	10
NW3	0			0.01	1.25×10^{-7}	0
NW4	0			0.001	1.25×10^{-8}	0

[C] Event under SW wind: frequency of 2.5×10^{-5} and fatalities of 30

Area	Population	Event frequency	Wind probability	Fatality probability	Individual risk	Fatalities under wind
SW1	10	10^{-4}	0.25	1	2.5×10^{-5}	10
SW2	100			0.1	2.5×10^{-6}	10
SW3	1000			0.01	2.5×10^{-7}	10
SW4	0			0.001	2.5×10^{-8}	0

[D] Event under SE wind: frequency of 6.25×10^{-6} and fatalities of 40

Area	Population	Event frequency	Wind probability	Fatality probability	Individual risk	Fatalities under wind
SE1	10	10^{-4}	0.0625	1	6.25×10^{-6}	10
SE2	100			0.1	6.25×10^{-7}	10
SE3	1000			0.01	6.25×10^{-8}	10
SE4	10000			0.001	6.25×10^{-9}	10

We conclude that 20 people will die from the accident with the probability of 1.25×10^{-5}.

The remaining two cases of wind direction can be processed in a similar way. The second and the third columns of Table 1.3 list 4 pairs of frequency and fatalities. Each of these pairs denotes (N, f). This shows that N fatalities occur with frequency f.

The four rows from (A) to (D) of Table 1.3 happen to be arranged in an ascending order of fatalities. Thus, the frequency FNE of 10 or more fatalities can be calculated as a sum of the four frequencies fNE, fNW, fSW and fSE. The frequency is called an excess frequency. The remaining three excess frequencies can be calculated similarly. The last FSE is the frequency of 40 or more fatalities and equals the frequency of 40 fatalities because this is the maximum number. The (N, f) curve and the (N, F) curve are depicted in Figure 1.14.

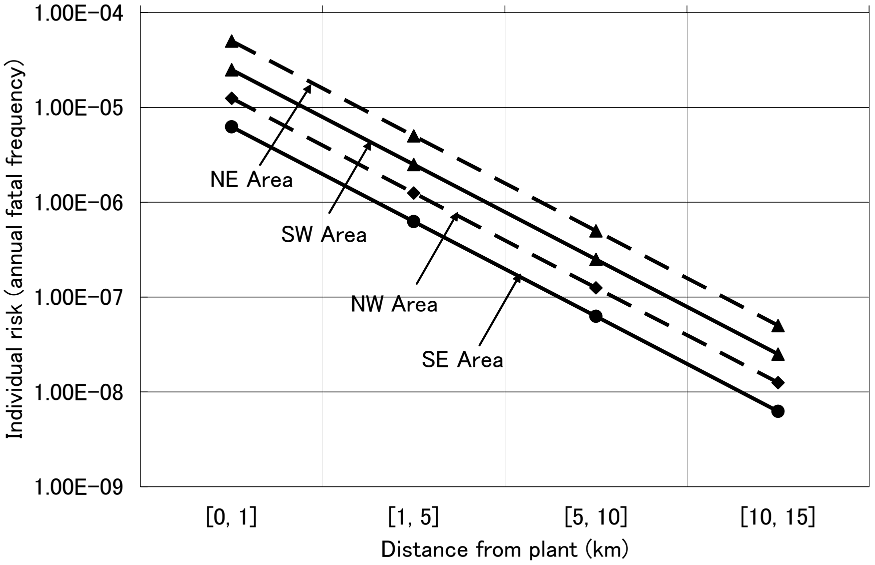


Fig. 1.13. Individual risks as a function of plant distance

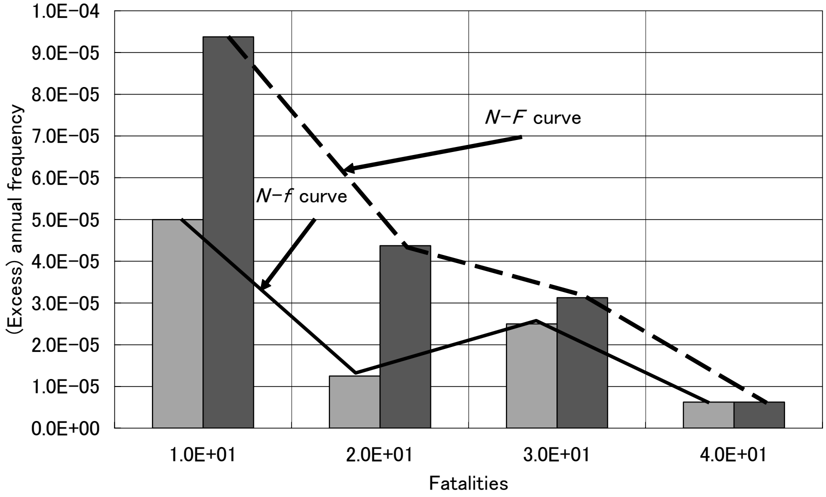


Fig. 1.14. *N–f* curve and *N–F* curve

1.9 Concluding Remarks

Qualitative safety goals, quantitative health objectives, and subsidiary numerical objectives are presented. The risk-informed integrated decision making

Table 1.3. Societal risks of the release accident

Wind direction	Accident and wind	Fatalities	Excess frequency
(A) NE	[fNE] 5.00×10^{-5}	10	[FNE] 9.38×10^{-5}
(B) NW	[fNW] 1.25×10^{-5}	20	[FNW] 4.38×10^{-5}
(C) SW	[fSW] 2.50×10^{-5}	30	[FSW] 3.18×10^{-5}
(D) SE	[fSE] 6.25×10^{-6}	40	[FSE] 6.25×10^{-5}

accounts for uncertainties inherent in the current PRA. The tolerability of risks and societal risks are also presented.

The risk-informed decision making contains as an indispensable element a categorization of structures, systems, and components (SSC) as well as human actions (HA)in terms of their safety significance. This point will be described in the next chapter.

2

Categorization by Safety Significance

2.1 Introduction

A plant consists of a variety of systems, structures, and components (SSCs) operated and maintained directly or indirectly by humans. Some SSCs and human activities (HAs) are more important than others from the point of view of risk. A risk-informed safety assurance utilizes risk information to 1) satisfy safety goals, 2) gain public trust, 3) increase safety assurance effectiveness, and 4) to remove unnecessary burden. The first step of the risk-informed safety assurance is the categorization of SSCs and HAs. The second step is the realization of requirements demanded for each category (Chapter 3)

This chapter first describes the categorization process advocated by IEC 61508, IEC 61511, and BS EN 951. These categorizations are based on the amount of risk reduction by the SSC. More complicated cases of risk-informed safety assurance are seen in the US NRC's risk-informed regulations. Categorizations of SSCs and HAs are described. The same "pressure-tank" example is used to illustrate common principles of these unrelated methodologies at a first glance.

2.2 Safety Integrity Level: IEC 61508 and IEC 61511

2.2.1 Hazardous Situation and Event

Hazard is defined as a potential ability to cause harm. Hazard has a source. For example, movement is a hazard. The source is a vehicle and the harm is a fatal injury by a collision. Hazard does not necessarily mean actual occurrence of harm or high probability of harm.

A hazardous situation is defined as a circumstance immediately before the harm is produced by the hazard. This is simply an occurrence of an initiating event. The hazardous situation would eventually yield harm if nothing stops it.

The hazardous situation, or the initiating event, occurs when a hazard comes into a play through some mechanism. A typical activation is through a failure of a control system that has suppressed the hazard. An intersection with a traffic signal is a hazard (source) of collision. The failure of the traffic signal yields a hazardous situation where extreme care is required for any drivers going through it.

The hazardous situation becomes a hazardous event when the harm becomes existent.

2.2.2 Definition of Function

A function is an action that is required to achieve a desired goal. Safety functions are those functions that serve to ensure safety. A typical safety function in a nuclear power plant is a “reactivity control”. A high-level objective, such as preventing the release of radioactive materials to the environment, is one that designers strive to achieve through the design of the plant and that plant operators strive to achieve through proper operation of the plant.

The function is often described without reference to specific plant systems and components or humans that are required to carry out this action. Functions are often accomplished through some combination of lower-level functions such as detection of an abnormal event. The process of manipulating lower-level functions to satisfy a higher-level function is sometimes called a *control function*. During function allocation the control function is assigned to human and machine elements [13].

2.2.3 Functional Safety System

A functional safety system prevents the occurrence of a hazardous event, given a hazardous situation. Some functional safety systems mitigate the hazardous event, such as an automobile collision, that has occurred. The mitigation reduces the fatal effect on people. IEC 61508 contains detailed descriptions about the functional safety systems [1].

The functional safety system consists of 1) monitor, 2) judge, 3) actuator, 4) power source, 5) piping and wiring, *etc.* This is similar to a human. In the process industries, the functional safety system is called a safety-instrumented systems (SIS) [11]. The present day machine industries take these systems for granted.

Operations of functional safety system include: 1) potentially hazardous movements of a machine are shut down or reversed when an emergency button is actuated, 2) potentially hazardous movements are prevented when the safety guard covering a machine is opened or when an approach of a worker is detected [23], 3) overspeed is detected and the machine is made to stop, 4) prestart warning device alarms a worker that the machine is about to start when the waiting time has elapsed [24]. An extreme is an emergency cooling system that is activated upon detection of loss of coolant at a nuclear power plant.

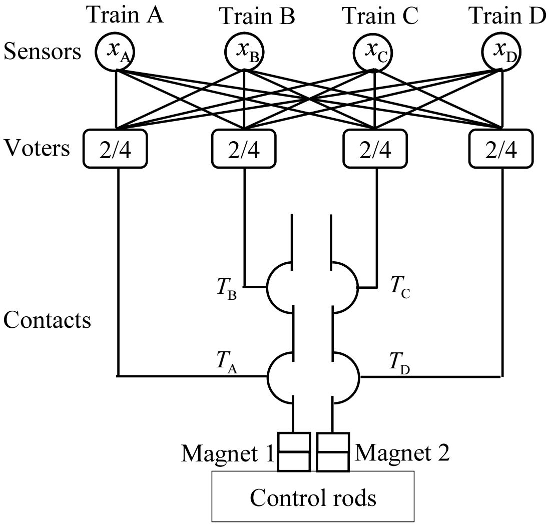


Fig. 2.1. An example of a functional safety system

2.2.4 Example: Reactor Scram System

Consider a reactor scram system shown in Figure 2.1. When a hazardous situation at a nuclear power plant is detected, the system drops enough control rods into the reactor to halt a so-called chain reaction. This insertion is a reactor scram or a reactor trip.

Five features of the scram system are listed.

1) Inadvertent events are monitored by four identical channels, A, B, C, and D.
2) Each channel is physically independent of the others. For example, every channel has a dedicated sensor and a voting unit.
3) Each channel has its own two-out-of-four:G voting logic. Capital G, standing for "good" means that the logic can generate the scram signal if two or more sensors successfully detect an inadvertent event. The logic unit in channel A has four inputs, x_{A}, x_{B}, x_{C}, x_{D}, and one output, T_{A}. Input x_{A} is a signal from a channel A sensor. This input is zero when the sensor detects no inadvertent events, and unity when it senses one or more events. Inputs x_{B}, x_{C}, and x_{D} are defined similarly. Note that a channel receives sensor signals from other channels. Output T_{A} represents a decision by the voting logic in channel A; zero values of T_{A} indicate that the reactor should not be tripped; a value of 1 implies a reactor trip. The voting logic in channel B has the same inputs, x_{A}, x_{B}, x_{C}, and x_{D}, but it has output T_{B} specific to the channel. Similarly, channels C and D have output T_{C} and T_{D}, respectively.

4) A one-out-of two:G twice logic with input T_{A}, T_{B}, T_{C}, and T_{D} is used to initiate control-rod insertion. The rods are suspended by magnets energized by two circuits. The two circuits must be cut off to de-energize the magnets; $(T_{\mathrm{A}}, T_{\mathrm{C}}) = (1, 1)$, or $(T_{\mathrm{A}}, T_{\mathrm{D}}) = (1, 1)$, or $(T_{\mathrm{B}}, T_{\mathrm{C}}) = (1, 1)$, or $(T_{\mathrm{B}}, T_{\mathrm{D}}) = (1, 1)$. The two 1-out-of-2:G logic units are ANDed. The rods are then released from the magnets and dropped into the reactor core by gravity. This is a “de-energize to drop” principle.

2.2.5 Example: Risk-aversive Safety Goal

Section 1.7 describes upper bound U and lower bound L of a tolerable risk region. Consider a case where these bounds are functions of the severities listed in Table 2.1. Frequency ratings are shown in Table 2.2.

Introduce a risk matrix where each column represents a severity rating, and each row denotes a frequency rating. Each cell in this hypothetical matrix is labeled as ◯ for unconditional acceptance, as $\diamond$ for conditional tolerability, and as $\times$ for unconditional rejection. A result is shown in Table 2.3. The term ALARP means that the risk level becomes tolerable in the conditional tolerability region if the risk can be justified (Section 1.7.2). Cost and availability of technology are major bases for this justification. We see from Table 2.3 that the conditional tolerability region for 1 fatality is the interval of annual frequencies $(10^{-4}, 10^{-2}]$.

Consider the expected number of fatalities for each lower bound L. The expected number is $1 \times 10^{-4} = 10^{-4}$ for the 1-fatality case, and $10 \times 10^{-6} = 10^{-5}$ for the 10-fatality case. Thus, the 10-fatality goal is more demanding than the 1-fatality case. The annual frequency decreases more rapidly than the one that yields a constant number of fatalities over different fatality consequences. This tendency of disliking a severe accident more severely than the expected value level is called a risk aversion (Section 1.8.2). The upper bound of Table 2.3 follows a constant, expected number of fatalities. This is called the risk-neutral preference.

2.2.6 Safety Integrity Level

Suppose that failure rate of 10^{-6}/year or approximately 10^{-10}/h is specified as a performance objective for a functional safety system. This is a strict requirement, and its manufacturer should reflect this objective in design and production.

Design, production and other activities should be varied according to the requirement level. This practice is symbolically expressed in terms of a safety integrity level (SIL) in standards IEC 61508 [1], IEC 61511 [11], EN 50126 [26], 50128 [27], and 50129 [28]. The SIL is determined from the failure rate or demand-failure probability required for a functional safety system.

Two types of failures are considered: random failure and systematic failure. The random failure can be quantified, while the systematic failure is difficult

Table 2.1. Example of severity rating of accident [25]

No	Rating	Consequence
IV	Insignificant	Minor injuries
III	Marginal	Major injuries
II	Critical	1 fatality
I	Catastrophic	10 fatalities
0	Disastrous	100 or more fatalities

Table 2.2. Example of frequency rating of accident [25]

Label	Rating	Annual frequency
A	Frequent	10^{-1}
B	Probable	10^{-2}
C	Occasional	10^{-3}
D	Remote	10^{-4}
E	Improbable	10^{-5}
F	Incredible	10^{-6}

Table 2.3. ALARP region designated as ◇ [25]

Annual frequency	Minor injuries	Major injuries	1 fatality	10 fatalities	100 fatalities
$10^{-1} < f \leq 10^{-0}$	◇	×	×	×	×
$10^{-2} < f \leq 10^{-1}$	◇	◇	×	×	×
$10^{-3} < f \leq 10^{-2}$	◇	◇	◇	×	×
$10^{-4} < f \leq 10^{-3}$	○	◇	◇	◇	×
$10^{-5} < f \leq 10^{-4}$	○	○	○	◇	◇
$10^{-6} < f \leq 10^{-5}$	○	○	○	◇	◇
$10^{-7} < f \leq 10^{-6}$	○	○	○	○	○

to quantify. Design and production are typical sources of systematic failures. Furthermore, the common-cause failures are frequently brought about by the systematic failures. Thus, special treatment in quality assurance is required to decrease the systematic failures for the functional safety system. IEC 61511 considers the SIL from the point of view of the process-industry users.

The SIL resembles the hotel star ranking. The manufacturer can provide functional safety systems graded by SIL. Users can use the safety system having a suitable grade. Functional safety systems are categorized according to the SIL, and the safety significance becomes apparent.

For a given SIL, the safety system is quantitatively evaluated for the random failures whether the system satisfies the SIL or not. To cope with systematic failures and unknown random failures, safety principles such as redundancy, diversity, failure detection, and others are applied to design, production, operation and maintenance. This is analogous to the probabilistic approach coupled with a deterministic one, as described in Regulatory Guide

1.174 for the nuclear power plant, *i.e.* risk-informed integrated decision making. This point will be described in more detail in this chapter and in Chapter 3.

Table 2.4 of EN 50126 defines the SIL for the railroad. IEC 61508 and IEC 61511 define the SIL as in Table 2.5. There are differences between these two table definitions.

Demand-failure probability is the probability of failure per demand when the safety system is demanded to operate. A safety belt should have a small demand-failure probability. The dangerous-failure rate is applicable to a high-demand case such as an automobile brake where its failure immediately leads to an accident.

IEC 61508 defines the "low-demand mode" as the case when the frequency of demands for operation is not greater than one per year and not greater than the proof-test frequency. The "high-demand or continuous mode" is the case where the frequency of demands is greater than one per year or greater than the proof-test frequency. These criteria come from a convention to calculate a demand-failure probability averaged over the proof-test interval for the low-demand mode (Section 3.9.2). The phrase "twice the proof-test frequency" in IEC 61508 is modified here.

The highest SIL of 4 indicates that the system is markedly dangerous and tremendous risk reduction is necessary. It is desirable to avoid the use of SIL 4 safety system. To implement the SIL 3 system, it is recommended to use a redundant system consisting of two or more SIL 2 systems. This redundancy can cope with the uncertainty except for dependencies such as common-cause failures. When a quantitative approach is used, Tables 2.4 and 2.5 are used to derive the SIL from the target demand-failure probability or the failure rate. On the other hand, when a qualitative approach is used, the SIL is first determined, and the quantitative numbers are obtained for demand probability or failure rate from the tables. These two types of approaches will be described more fully in this section.

2.2.7 Example: High-demand Mode

Consider an automatic train-protection (ATP) system of a hypothetical railroad [25]. The ATP operates in a high-demand mode in a similar way to a traffic signal. Assume, for simplicity, that the ATP failure yields 10% of the fatal accidents on this railroad. This assumption is used to allocate performance objectives to a variety of accidents of different origins.

The number of fatalities due to the ATP failure is relatively small as compared with railroad fire accidents; it is sufficient to consider two types of accidents with 1 and 10 fatalities, respectively. The demand always exists for the ATP. An ATP failure yields a 1 fatality accident with a percentage of 5%, a 10-fatality accident with the same 5%, and no accident with the remaining 90%. The ATP failure is temporal, and is repaired quickly.

Table 2.6 simply extracts upper and lower bound frequencies for the two accidents from Table 2.3.

Note that the bounds include contributions other than the ATP-oriented accidents. Thus, the annual frequencies for the ATP-oriented accidents must be one tenth of the values in Table 2.6. On the other hand, the ATP failure yields 1 and 10 fatality accidents with the same 5% probability. As a result, the frequencies in Table 2.6 should be multiplied by $0.1 \times 20 = 2$. The result is shown in Table 2.7. The ATP failure frequency is constrained by the lower bound for the 10-fatality accident. The unconditionally acceptable frequency value is 2×10^{-6}/year. The acceptable bound 2×10^{-6}/year becomes 2×10^{-10}/h when the unit changes from "year" to "hour". The dangerous-failure rate of the ATP is 2×10^{-10}. Thus, the SIL is determined as 3 from Table 2.4.

Table 2.4. Definition of SIL by EN 50126 (railroad)

SIL	Per hour failed-dangerous rate λ	Per demand failed-dangerous probability P
4	$(0, 10^{-10})$	$(0, 10^{-7})$
3	$[10^{-10}, 0.3 \times 10^{-8})$	$[10^{-7}, 10^{-6})$
2	$[0.3 \times 10^{-8}, 10^{-7})$	$[10^{-6}, 10^{-5})$
1	$[10^{-7}, 0.3 \times 10^{-5})$	$[10^{-5}, 10^{-4})$

Table 2.5. Definition of SIL by IEC 61508 and IEC 61511

SIL	Per hour failed-dangerous rate λ	Per demand failed-dangerous probability P	Risk-reduction factor
4	$[10^{-9}, 10^{-8})$	$[10^{-5}, 10^{-4})$	(10 000, 100 000]
3	$[10^{-8}, 10^{-7})$	$[10^{-4}, 10^{-3})$	(1000, 10 000]
2	$[10^{-7}, 10^{-6})$	$[10^{-3}, 10^{-2})$	(100, 1000]
1	$[10^{-6}, 10^{-5})$	$[10^{-2}, 10^{-1})$	(10, 100]

Table 2.6. Upper and lower bounds of ALARP region

Fatalities/ upper and lower	1 fatality	10 fatalities
U	10^{-2}	10^{-3}
L	10^{-4}	10^{-6}

Table 2.7. Upper and lower bounds of ATP failure frequency

Fatalities/ upper and lower	1 fatality	10 fatalities
ATP upper bound	2×10^{-2}	2×10^{-3}
ATP lower bound	2×10^{-4}	2×10^{-6}

Suppose that the railroad uses 20 identical ATP units. Thus, the failure rate of each unit must be 10^{-11}/h because the unit can cause the ATP failure. The SIL 3 indicates the safety-significance level of the ATP system. The unit supports the safety function of the ATP. Thus, each unit is categorized into the same safety-significance level as the parent system. This is similar to the approach for the nuclear power plant. Of course, the quality assurance would be more intensive if the ATP contains more units.

When the upper bound in Table 2.7 is used, the target failure-rate value of ATP becomes 2×10^{-7}/h. This is a maximum value of the conditional-tolerability region. The failure rate should be decreased until the ALARP principle can justify the cessation of risk reduction. Assume a criterion that 3 million dollars should be spent to save life. Then, the risk reduction continues until the failure rate reaches the broadly acceptable lower bound of 2×10^{-10}/h or the further reduction requires cost exceeding the criterion.

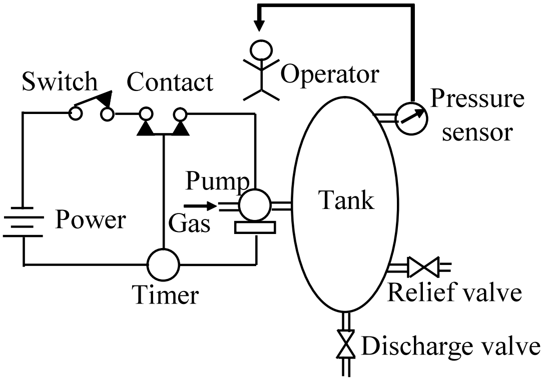


Fig. 2.2. Schematic of pressure-tank system

2.2.8 Semiquantitative Method using Subsidiary Objective

In the semiquantitative method the plant performance is evaluated quantitatively, while the consequence of an accident is assessed only qualitatively. The method is illustrated by the following example that is used throughout this chapter.

Pressure-tank Example

The system shown in Figure 2.2 pumps flammable gas from a reservoir into a pressure tank [29]. The switch is normally closed and the pumping cycle is initiated every month by an operator who manually resets the timer. The timer contact closes and pumping starts. Well before any overpressure condition exists the timer times out and the timer contact opens. Current to the pump

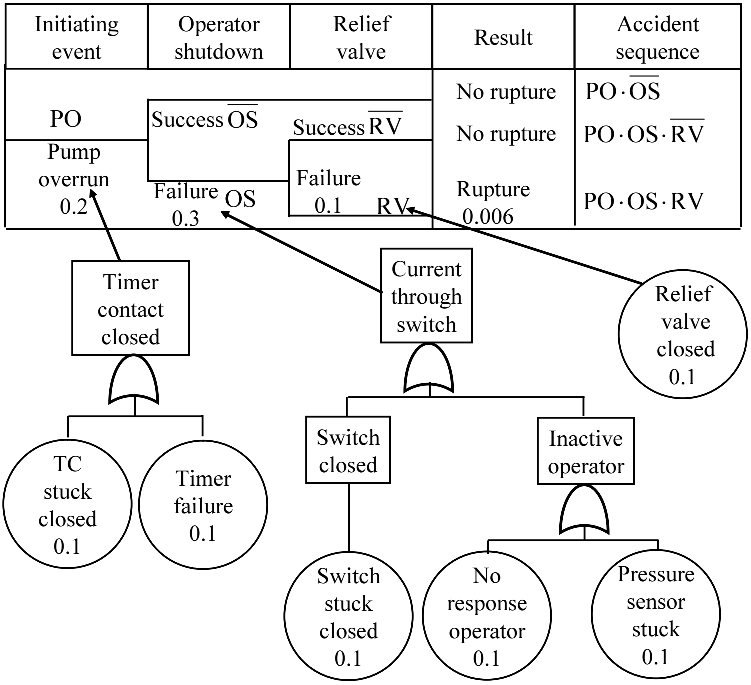


Fig. 2.3. Event tree coupled with fault trees

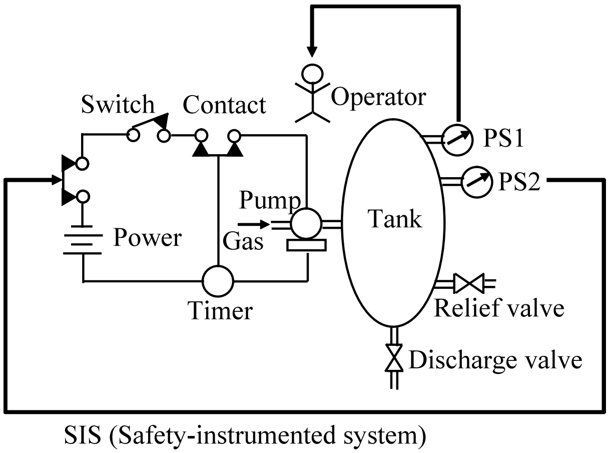


Fig. 2.4. Pressure-tank system with additional SIS

cuts off and pumping ceases (to prevent a tank rupture due to overpressure). This timer system can be regarded as a basic process-control system (BPCS) shown in Figure 1.7. This terminology of BPCS originates from IEC 61511.

The failure of the BPCS causes an initiating event labeled as "pump overrun" that has a potential leading to a flammable gas release to the environment via the tank rupture. The BPCS does not perform any safety functions. Its failure contributes to the occurrence of the initiating event. As shown in Figure 2.3, the initiating event is assumed to occur with a frequency of 0.2/year according to a rare-event approximation (Section 7.6.5) because the two basic events "Timer contact stuck closed" and "Timer failure" occurs with frequencies 0.1/year, respectively. Other initiating-event candidates are leaks from process equipment, pipe ruptures, and external events such as earthquakes.

If the timer contact does not open due to the BPCS failure, the operator is instructed to respond to the pressure-sensor alarm and to open the manual switch, thus causing the pump to stop. This is a process-monitoring system, a type of protection layer shown in Figure 1.7. The process-monitoring system fails with probability 0.3 as shown in Figure 2.3.

Even if the timer and operator both fail, overpressure can be relieved by the relief valve, a type of noninstrumented, mechanical protection shown in Figure 1.7. Releases from the relief valve are piped to a flare system whose failures are not considered for simplicity of description. As shown in Figure 2.3 this noninstrumented protection fails with probability of 0.1.

Other types of noninstrumented protection are the structural protection shown in Figure 1.7. A dyke is an example of the structural protection. For the flammable gas released by the tank-rupture event, the dyke is not a good measure for risk reduction.

Before the start of each cycle, the tank is emptied by opening the discharge valve to dump the residual gas. This valve is then closed. The operator is instructed to observe the pressure sensor to confirm the depressurized tank. Note that the pressure sensor may fail before the new cycle. An undesired event, from a risk viewpoint, is a pressure-tank rupture by overpressure.

Figure 2.3 shows the event tree and fault tree for the pressure-tank rupture due to overpressure. The event tree starts with an initiating event that initiates the accident sequence. The tree describes combinations of success or failure of the system's mitigative features that lead to desired or undesired plant states.

In Figure 2.3, PO denotes the event "pump overrun," the first type of initiating event that starts the potential accident scenarios. The second type is the tank discharge failure before the start of the cycle. This initiating event will be described later.

Symbol OS denotes the failure of the operator shutdown system, PP denotes failure of the pressure-protection system by relief-valve failure. The overbar indicates a logic complement of the inadvertent event, that is, successful activation of the mitigative feature. There are three sequences or scenarios displayed in Figure 2.3. The scenario labeled PO·OS·PP causes overpressure and tank rupture, where symbol "·" denotes the logic intersection, (AND).

Therefore the tank rupture requires three simultaneous failures. The other two scenarios lead to safe results.

The event tree defines top events, each of which can be analyzed by a fault tree that develops more basic causes such as hardware or human faults. We see, for instance, that the pump overrun is caused by timer-contact failure stuck closed, or timer failure. By linking the three fault trees (or their logic complements) along a scenario on the event tree, possible causes for each scenario can be enumerated.

For instance, tank rupture, the most dangerous scenario, occurs when the following three basic causes occur simultaneously: 1) timer contact stuck closed, 2) switch stuck closed, and 3) pressure relief closed. Probabilities for these three causes can be estimated from generic or plant-specific statistical data, and eventually the probability of the tank rupture due to the initiating event of pump overrun can be quantified.

SIL for Demand Mode SIS

A tolerable frequency of the tank-rupture event may be specified by reflecting

1) national and international standards and regulations,
2) corporate policies, and
3) community, local jurisdiction and insurance companies.

The rupture frequency in the current example is 0.006/year for the first initiating event, as shown in Figure 2.3. The tank rupture is a hazardous event, the term being defined in Section 2.2.1. Assume a tolerable frequency of 10^{-4}/year, considering the large release of flammable gas into the environment following the rupture. This frequency has a similar role to the subsidiary CDF objectives for the nuclear power plant. The approach is called semiquantitative because the frequency of the tank rupture is evaluated quantitatively, while its consequence is assessed only qualitatively. Moreover, the subsidiary LERF objective is not considered for the tank-rupture problem without a containment.

Assume that inherently safe designs such as replacing the flammable gas by a nonflammable one have already been reviewed. The process-monitoring system and relief valves are implemented. The structural protection such as containment is not feasible for the current case.

The last measure is the SIS shown in Figure 2.4. This consists of a new pressure sensor, a logic solver, and a new relay contact. The SIS opens the contact when high pressure is detected. This is an automated version of the process-monitoring system relying on the operator.

Note that the sharing of the same pressure sensor between the process-monitoring system and the SIS would introduce dependency. When the pressure sensor fails to alarm the high pressure, the sensor also fails to detect the high pressure for the SIS. A similar dependency would be introduced when the same switch is shared between the process-monitoring system and the SIS, or the same contact between the BPCS and the SIS.

If the operator fails to depressurize the tank before the cycle begins, then the timer BPCS fails because the initial tank pressure is sufficiently high. The depressurization failure thus becomes another initiating event that has the two causes: 1) operator depressurization error (omission), and 2) pressure-sensor failure (stuck low). The operator incorrectly thinks that the tank has been emptied when the pressure sensor fails in stuck-low mode. Even if the pressure sensor indicates the correct high pressure, the operator may forget the depressurization (omission). The minimal cut sets of the initiating event coupled with the failure of the process-monitoring system are:

1) {operator discharge failure, operator no response}
2) {pressure sensor stuck low}
3) {operator discharge failure, switch stuck closed}

Table 2.8 summarizes the components of the pressure-tank system. The above minimal cut sets can be expressed as: 1) {OP0, OP1}, 2) {PS1}, and 3) {OP0, SW}. Note that the pressure-sensor failure is a single-event cut set (*i.e.* system-failure mode, Section 7.4) for the initiating event along with the BPCS failure. The initiating-event frequency is approximated by the sum of cut set frequencies: $0.01 + 0.1 + 0.01 = 0.12$/year.

Table 2.8. Component list of pressure-tank system

Label	Description	Failure mode	Prob.	Frequency
OP0	Operator	Discharge failure		0.1/year
C1	Contact 1	Stuck closed		0.1/year
TM	Timer	Failure		0.1/year
SW	Switch	Stuck closed	0.1	
OP1	Operator	No response	0.1	
PS1	Pressure sensor 1	Stuck low	0.1	0.1/year
RV	Relief valve	Stuck closed	0.1	
SIS	SIS	Failure	0.005	

The demand rate to the relief valve is thus 0.12/year. The relief valve fails with probability 0.1. The demand to SIS becomes 0.012/year. The total demand to SIS from the two types of initiating events becomes $0.006 + 0.012 = 0.018$, and the SIS must have a risk-reduction factor of $1.8 \times 10^{-2}/10^{-4} = 180 \simeq 200$ in order to satisfy a tolerable frequency of 10^{-4}, resulting in SIL 2 SIS from Table 2.5.

2.2.9 Layer of Protection Analysis

An example of layer of protection analysis (LOPA) is shown in Table 2.9. This portion of LOPA is similar to the semiquantitative method described in the last section, except for the tabular format. LOPA, however, considers consequences, as described shortly.

Table 2.9. Layer of protection analysis table

1	2	3	4	5	6	7	8	9	10	11
	Hazardous event		Initiating event		BPCS	Protection layers without SIS			PLs with SIS	
	Consequence	Severity	Initiator	Initiator likelihood	BPCS	Monitoring system	Relief valve	Likelihood without SIS	SIS risk reduction	Likelihood with SIS
1	Fire from tank rupture	S	BPCS failure	0.2		0.3	0.1	0.006	0.005	0.00003
2	Fire from tank rupture	S	Discharge failure	0.12			0.1	0.012	0.005	0.00006

Table 2.10. Severity ratings of safety-layer matrix, LOPA, and risk graph

Safety-layer matrix	LOPA	Risk graph
Hazardous event severity	Impact event severity levels	Consequence on person and environment
Minor: Minor damage to equipment. No shutdown of the process. Temporary injury to personnel and damage to the environment.	**Minor:** Impact initially limited to local area of event with potential to broader consequence, if corrective action not taken.	**C$_1$**: Light injury to persons. A release with minor damage that is not very severe but is large enough to be reported to plant management.
Serious: Damage to equipment. Short shutdown of the process. Serious injury to personnel and the environment.	**Serious:** Impact event could cause serious injury or fatality on site or offsite.	**C$_2$**: Serious permanent injury to one or more persons; death of one person. Release within the fence with significant damage.
Extensive: Large-scale damage of equipment. Shutdown of a process for a long time. Catastrophic consequence to personnel and the environment.	**Extensive:** Impact event that is five or more times severe than a serious event.	**C$_3$**: Death of several persons. Release outside the fence with major damage that can be cleaned up quickly without significant lasting consequences.
		C$_4$: Catastrophic effect, many people killed. Release outside the fence with major damage that cannot be cleaned up quickly or with lasting consequences.

Each row of Table 2.9 starts with a hazardous event yielding a consequence with a severity level. By the LOPA terminology, the consequence is called an impact event. The severity-level classification is shown in the "LOPA" column of Table 2.10. For the current case, the severity is labeled as "Serious (S)".

There are two initiating events leading to the consequence. Both of the initiating-event likelihoods are "High". As a matter of fact, the BPCS failure has the initiator likelihood of 0.2/year, while the depressurization failure has the likelihood of 0.12/year.

Note that the BPCS-failure initiating-event can not be dealt with by the BPCS. This initiator can be dealt with the process-monitoring system and the relief valve. Thus, the likelihood of the hazardous event without an SIS is 0.006/year for the first initiating event.

The BPCS cannot deal with the second initiator, depressurization failure, because the time-out mechanism is too late for the pressurized tank at the startup time. There is a shared-component dependency via the pressure sensor between the initiator and the process-monitoring system. Thus, the demand frequency to the relief valve must be evaluated by a combined system of initiator and the process-monitoring system. The minimal cut sets were already shown. It was determined that the demand frequency to the relief valve was 0.12/year. This frequency is shown in Table 2.9. The hazardous event likelihood without SIS is 0.012/year.

The SIS risk-reduction factor is specified as 200, *i.e.* the SIS demand-failure probability is 0.005. This is SIL 2. This reflects the event likelihoods without the SIS, and the consequence severity. The resulting likelihoods for the two initiating events are 0.00003 and 0.00006, respectively. The total likelihood of the consequence is 0.00009, which is judged tolerable by the analyst of the pressure-tank example system. Recall that the tank-rupture likelihood has a similar role to the CDF.

Now let us consider a consequence analysis. The fatality frequency due to fire is calculated by:

$$\mathrm{FF} = \mathrm{RF} \times \mathrm{PI} \times \mathrm{PE} \times \mathrm{PF} \tag{2.1}$$

where

1) FF: Fatal frequency due to the fire.
2) RF: Frequency of flammable material release. This frequency is the tank-rupture frequency, 0.00009/year for the current example.
3) PI: Probability of ignition. The tank area has explosion-proof equipment, and the electrical equipment maintenance follows the guidance for ignition reduction. No transfer of ignition from other areas. The ignition probability is determined as 0.1.
4) PE: Probability of a person in the tank area. This is estimated as 0.1.
5) PF: Probability of fatality by fire. This is estimated as 50%.

The fatality frequency due to fire becomes:

$$\mathrm{FF} = 0.00009 \times 0.1 \times 0.1 \times 0.5 = 4.5 \times 10^{-7}/\mathrm{year} \tag{2.2}$$

This frequency is judged to satisfy the company's quantitative health objective for a single fatality by the flammable material. When the tank contains toxic gas the fatality frequency due to the toxic release must be evaluated too.

The subsidiary CDF objective avoids this type of consequence analysis because considerable uncertainties may exist, for instance, in estimating the probability of ignition, the probability of a person in the area, and the probability of fatality by fire.

Table 2.11. Frequency ratings of safety-layer matrix, LOPA, and risk graph

Safety-layer matrix	LOPA	Risk graph
Hazardous event likelihood	Initiation likelihood	Demand frequency
Low: Events such as multiple failures of diverse instruments or valves, multiple human errors in a stress free environment, or spontaneous failures of process vessels.	**Low:** A failure or series of failures with a very low probability of occurrence within the expected lifetime of the plant. $f < 10^{-4}$/year. Examples: 1) Three or more simultaneous instrument, or human failures. 2) Spontaneous failure of single tanks or process vessels.	$\mathbf{W_1}$: A very slight probability that the unwanted occurrences occur and only a few unwanted occurrences are likely. $f < 0.1$/year
Medium: Events such as dual instrument, valve failures, or major releases in loading/unloading areas.	**Medium:** A failure or series of failures with a low probability of occurrence within the expected lifetime of the plant. $10^{-4} \leq f < 10^{-2}$/year. Examples: 1) Dual instrument or valve failures. 2) Combination of instrument failures and operator errors. 3) Single failures of small process lines or fittings.	$\mathbf{W_2}$: A slight probability that the unwanted occurrences occur and a few unwanted occurrences are likely. $0.1 \leq f < 1$/year
High: Events such as process leaks, single instrument, valve failures or human errors that result in small releases of hazardous materials.	**High:** A failure can reasonably be expected to occur within the expected lifetime of the plant. $10^{-2} \leq f$/year. Examples: 1) Process leaks. 2) Single instrument or valve failures. 3) Human errors that could result in material releases.	$\mathbf{W_3}$: A relatively high probability that the unwanted occurrences occur and frequent unwanted occurrences are likely. $1 \leq f < 10$/year

2.2.10 Safety-layer Matrix

The safety-layer matrix is shown in Figure 2.5. The labels a, b, and c in this figure indicate the following remarks.

1) a: One SIL 3 safety-instrumented function does not provide sufficient risk reduction. Additional modifications are required in order to reduce risk.
2) b: One SIL 3 safety-instrumented function may not provide sufficient risk reduction. An additional review is required.
3) c: SIS independent layer is probably not needed.

The PLs in the third axis are defined as all the PLs protecting the process including the SIS being classified. This matrix does not consider SIL 4 SIS.

The severities of a hazardous event without considering PLs are defined in the "safety-layer matrix" column of Table 2.10. The tank rupture and the resulting release of flammable material and the potential fire can be regarded as large-scale damage of equipment, shutdown of a process for a long time,

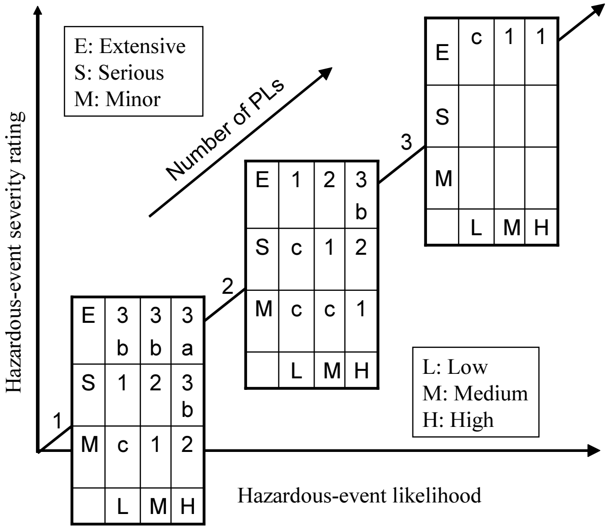


Fig. 2.5. Safety-layer matrix consisting of dimensions of likelihood, severity, and protection layers

and catastrophic consequence to personnel and the environment. Thus the severity rating is classified as "Extensive".

The original design of the pressure-tank system has two PLs: 1) process-monitoring system, and 2) relief valve. The frequency of hazardous-event likelihood without considering PLs is defined in the "safety-layer matrix" column of Table 2.11. The frequency of a hazardous event becomes the initiating-event frequency, *i.e.* failure frequency 0.2/year for the BPCS initiating event and 0.12/year for the discharge-failure initiating-event. The hazardous-event likelihood is labeled as "High". This labeling, of course, should be performed without the quantitative information about the initiating-event frequency. We cite the number only to illustrate the approach.

The pressure-tank system has 3 PLs including the SIS for the first initiating event. IEC 61511 requires that each PL should reduce at least the hazardous event by a factor of 10. In this sense, the process-monitoring system is not a PL because its risk-reduction factor is $1/0.2 = 5$. Thus, the number of PLs decreased to 2.

The system has only 2 PLs for the second initiating event because the monitoring system has a strong dependency on the discharge failure via the shared pressure sensor. The number of PLs is conservatively estimated again as 2 in Figure 2.5.

The cell at "E" row and "H" column shows that the SIS should be a SIL 3 safety-instrumented system. This is higher than the SIL 2 result of the LOPA.

Table 2.12. Risk graph consisting of consequence, exposure, avoidance, and demand frequency

Case number		1	2	3	4	5	6	7	8	9	10	11	12	13
Consequence severity		C_1	C_2				C_3				C_4			
Personnel exposure			F_1		F_2		F_1		F_2		F_1		F_2	
Possibility of avoidance			P_1	P_2	P_1	P_2	P_1	P_2	P_1	P_2	P_1	P_2	P_1	P_2
Demand frequency	W_1	–	–	a	a	1	a	1	1	2	1	2	2	3
	W_2	–	a	1	1	2	1	2	2	3	2	3	3	4
	W_3	a	1	2	2	3	2	3	3	4	3	4	4	b

2.2.11 Risk Graph

A risk graph is shown in Table 2.12. The labels "–", "a", "b" and numbers 1 to 4 in this table indicate the following remarks.

1) –: No safety requirements.
2) a: No special safety requirements.
3) b: A single SIS is not sufficient.
4) 1, 2, 3, and 4: Safety integrity levels.

The numbers associated with labels C, F, and P can be regarded as scores. It turns out that the total score determines the 3-dimensional column vector, where W_1, W_2, and W_3 correspond to the first, second, and third dimension, respectively. For instance, (C_2, F_2, P_2), (C_3, F_1, P_2), and (C_4, F_1, P_1) result in the same vector $(1, 2, 3)$.

The risk graph assumes first that no SIS is in place except for BPCS, monitoring systems and relief valves for the pressure-tank example.

There are two types of initiating events: 1) timer BPCS failure, and 2) operator discharge error. The frequency of tank rupture without the SIS was 0.018/year, as was shown in Table 2.9. The frequency is less than 0.1, and is labeled as W_1 from the "risk graph" column of Table 2.11. The consequence is evaluated as C_3 from the column of Table 2.10.

The frequency of human presence in the hazardous zone multiplied by the exposure time is rated as follows.

1) F_1: Rare to frequent exposure in the hazardous zone.
2) F_2: Frequent to permanent exposure in the hazardous zone.

For the pressure-tank system, access to the tank area is restricted for workers and public. Online maintenance is not performed. Thus, the frequency of human presence is labeled as F_1.

The possibility of avoiding the consequences of the hazardous event is rated as follows:

1) P_1: Possible under certain conditions.
2) P_2: Almost impossible.

The factors to be considered for determining the avoidance possibility rating are [11]:

1) Operation of a process is supervised or unsupervised. The supervision means operation by both skilled and unskilled persons.
2) Speed of development of hazardous event. For example, suddenness, quickness, or slowness.
3) Ease of recognition of danger such as (1) being recognized immediately, (2) being detected by technical measures, or (3) being detected without technical measures.
4) Ease of avoidance from hazardous event. For example, (1) escape routes possible, (2) not possible, or (3) possible under certain conditions.
5) Actual safety experience. Such experience may exist for an identical process or for a similar process or they may not exist.

For the pressure-tank system, the rupture occurs so rapidly, the avoidance possibility is labeled as P_2, *i.e.* almost impossible. The combination of C_3, F_1, P_2, and W_1 yields SIL 1 SIS. If the frequency is F_2 in Table 2.10, then the SIL would increase to 2.

2.2.12 Category for Machinery Safety: EN 954

Consider, for instance, a driverless vehicle that moves at low speeds (3.5 km/h) along a specified route in a factory [23]. A categorization by a risk graph from BS EN 954-1 [30] is shown in Figure 2.6.

A pedestrian may be seriously and irreversibly injured (S2) when a collision occurs because the vehicle carries a heavy load. The pedestrian is continuously exposed (F2) to the hazard because they have free access to the vehicle's route. The hazard avoidance is possible (P1) because of the low speed of the vehicle. The collision-prevention safety system turns out to have category 3, as shown by the thick lines in Figure 2.6.

Definitions of categories B, 1, 2, 3 and 4 are given in Table 2.13. Categories B and 1 are mainly characterized by the selection of components, while categories 2 to 4 are by the structure.

The BS EN 954-1 is qualitative and much easier to use than the IEC 61508 that tends to be quantitative to deal with statistical data such as mean time to dangerous failure and a so-called diagnostic coverage (Section 3.7). A revised version of BS EN 954-1 is ISO 13849-1. The EN 954 does not address the software used for PLCs.

A correspondence between SIL and the EN 954 category is shown in Table 2.14 [23, 24].

2.3 SSC Categorization Guideline: NEI 00-04

This section describes a categorization process NEI 00-04 proposed by the US Nuclear Energy Institute in 2004 [18]. We will see, for instance, that the risk-reduction factor is simply an importance measure called a ”risk-achievement worth (RAW)” used for the SSC categorization.

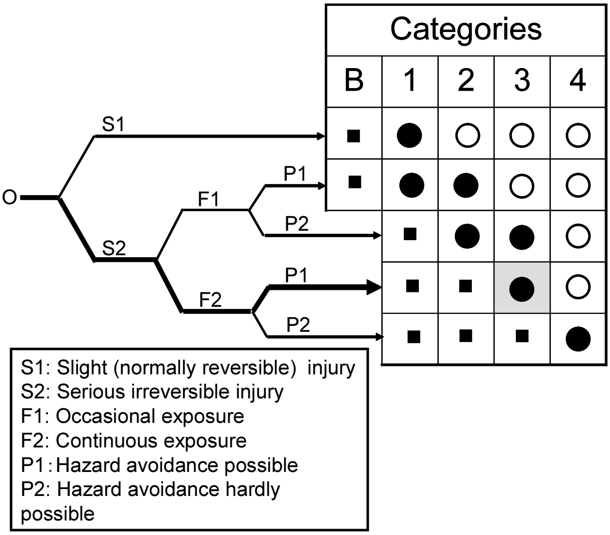

Categories
B
1
2
3
4
S1
S2
F1
F2
P1
P2
P1
P2
O
S1: Slight (normally reversible) injury
S2: Serious irreversible injury
F1: Occasional exposure
F2: Continuous exposure
P1: Hazard avoidance possible
P2: Hazard avoidance hardly possible

Fig. 2.6. Risk graph for categorizing safety function for machinery

2.3.1 Safety-related SSCs

The design of nuclear power plant ensures that 1) the reactor can be shut down quickly to stop the reaction, 2) the core can be cooled reliably, *and* 3) all radioactive material remains contained within the passive barriers such as reactor-coolant pressure boundary or containment structure [19].

Safety-related SSCs mean those that are relied upon to remain functional during and following design basis events to assure [31]:

1) The capability to shut down the reactor and maintain it in a safe shutdown condition,
2) The integrity of the reactor-coolant pressure boundary, *or*
3) The capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures.

Consider as an illustrative example the improved version of the pressure-tank system of Figure 2.4 where a SIS is introduced. The components were listed in Table 2.8. All the components other than the timer and the timer contact are safety related because they are relied upon to remain functional to deal with the initiating event. This is obvious from the deterministic behavior of the pressure-tank system. It is intuitively seen that pressure sensor (PS1) is more safety significant than switch (SW) because the sensor not only protects the tank by sensing the overpressure but also its failure causes an initiating event, *i.e.* operator discharge failure.

Table 2.13. Definition of categories

Cat.	Requirements in brief	System behavior
B	Components of safety-related control systems must be designed, constructed, selected, assembled and combined in accordance with the relevant standards such that they can withstand the expected influence.	The occurrence of a fault can lead to the loss of the safety function.
1	The requirements of B shall apply. Well-tried components and well-tried safety principles shall be used.	The occurrence of a fault can lead to the loss of the safety function, but the probability of occurrence is lower than in category B.
2	1) The requirements of B and the use of well-tried safety principles shall apply. 2) The safety function shall be checked at suitable intervals by the machinery control system.	The loss of the safety function is detected by the check. The occurrence of a fault can lead to the loss of the safety function between the checks.
3	1) The requirements of B and the use of well-tried safety principles shall apply. 2) Safety-related components shall be designed such that: 2-1) a single fault in any of these components does not lead to the loss of the safety function, and 2-2) the single fault is detected whenever reasonably practicable.	1) If the single fault occurs, the safety function is still maintained. 2) Some but not all faults are detected. 3) Accumulation of undetected faults can lead to the loss of the safety function.
4	1) The requirements of B and the use of well-tried safety principles shall apply. 2) Safety-related components shall be designed such that: 2-1) a single fault in any of these components does not lead to the loss of the safety function, and 2-2) the single fault is detected during or prior to the next demand on the safety function, or, if this is not possible, an accumulation of faults should not as a result lead to the loss of the safety function.	If faults occur, the safety function is still maintained. Faults are detected in good time to prevent the loss of safety function.

2.3.2 Quality-assurance Program

Because of the importance of the safety-related equipment to protecting public health and safety, the quality-assurance (QA) program (described in Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," to 10 CFR Part 50) is applied to all activities affecting the safety-related functions of that equipment. These activities range over

Table 2.14. Correspondence between SIL of IEC 61508 and category of EN 954-1

Category	SIL	Remarks
B	-	State-of-the-art safety-related control systems
1 or 2	1	Discrete time periodic testing
3	2	Single-failure criteria with partial fault detection
4	3	Continuous self-monitoring
-	4	Not typical in machinery protection

designing, purchasing, fabricating, handling, shipping, storing, cleaning, erecting, installing, inspecting, testing, operating, maintaining, repairing, refueling, and modifying.

Here, the quality assurance is defined to comprise all those planned and systematic actions necessary to provide adequate confidence that a SSC will perform satisfactorily in service.

The Appendix B, for instance, states the following actions for instructions, procedures, and drawings: "Activities affecting quality shall be prescribed by documented instructions, procedures, or drawings, of a type appropriate to the circumstances and shall be accomplished in accordance with these instructions, procedures, or drawings. Instructions, procedures, or drawings shall include appropriate quantitative or qualitative acceptance criteria for determining that important activities have been satisfactorily accomplished."

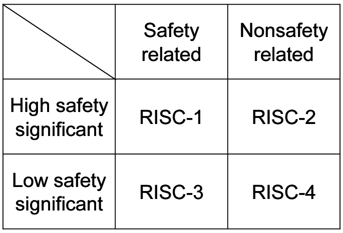
The QA program follows a PDCA cycle: 1) assuring that an appropriate quality-assurance program is established and effectively executed and 2) verifying, such as by checking, auditing, and inspection, that activities affecting the safety-related functions have been correctly performed.

2.3.3 Safety-significance Categorization

The 10 CFR Part 50 recognizes that the QA program should be applied in a manner consistent with the importance to safety of the associated plant equipment. In the past, engineering judgment provided the general mechanism to determine the relative importance to safety of plant equipment [32].

Insights from PRAs have revealed that certain plant equipment important from a deterministic point of view is of little significance to safety. Conversely,

Table 2.15. Risk-informed safety classifications by NEI 00-04 categorization process



	Safety related	Nonsafety related
High safety significant	RISC-1	RISC-2
Low safety significant	RISC-3	RISC-4

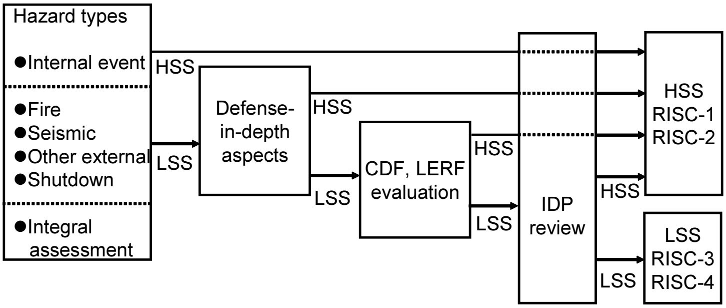


Fig. 2.7. NEI 00-04 categorization process into HSS and LSS

certain plant equipment turns out to be significant to safety but is not classified as a safety-related SSC.

As a consequence, Section 50.69 of 10 CFR Part 50 titled as "Risk-informed categorization and treatment of structures, systems and components for nuclear power reactors" has come to give the following definitions where RISC is the abbreviation of risk-informed safety class:

1) RISC-1 SSCs means safety-related SSCs that perform (high) safety-significant (HSS) functions.
2) RISC-2 SSCs means nonsafety-related SSCs that perform (high) safety-significant functions.
3) RISC-3 SSCs means safety-related SSCs that perform low safety-significant (LSS) functions.
4) RISC-4 SSCs means nonsafety-related SSCs that perform low safety-significant functions.

These four classes are shown in Table 2.15 [18]. A low safety-significant SSC, for instance, may have availability 2 or 5 times larger than a high safety-significant SSC in evaluating CDF or LERF.

Qualitative Criteria for High Safety-significance

The concept of high safety significance can be best illustrated by qualitative criteria used by NEI 00-04 to make a categorization not by PRAs but by screening tools. The qualitative criteria result in more conservative categorization. In other words, more SSCs are identified as high safety significant.

1) All SSCs that are involved in the mitigation of any unscreened scenario are identified as safety significant. Containment challenges include bypass events such as interfacing systems loss of coolant accident (ISLOCA) and steam generator tube rupture (SGTR). Operator action to isolate the ISLOCA is considered safety significant. A strategy during an SGTR event is the depressurization of primary and secondary systems and the equalization of pressures between primary and secondary. These all help to limit the leakage and are safety significant [13].

2) All screened scenarios are reviewed to identify any SSCs that would result in a scenario being unscreened, if that SSC was not credited. This review assures that the SSCs that were required to maintain low risk are retained as safety significant. For instance, a tank rupture due to tank defects may be screened out due to an inherently high reliability of the pressure tank. For potentially high-consequence events, even if the event frequency is below a screening criterion, the features that lead to the frequency being low (for example, surveillance test practices, startup procedures) are safety significant [9].
3) When multiple SSCs are available to satisfy the safety function, only SSCs that support (1) the primary method and (2) the first alternative method to satisfy the function are considered to be safety significant. Assume that the SIS of the pressure-tank system consists of three independent trains. Then, trains 1 and 2 are considered to be safety significant.
4) When a SSC failure would initiate a shutdown event, then it is safety significant. The stuck-closed timer contact initiates the pump shutdown, and this contact is safety significant.
5) Failure of the SSC may compromise the reactor-coolant pressure boundary or containment integrity. These SSCs are safety significant.
6) Failure of the SSC will directly fail another safety-significant SSC, including SSCs that are assumed to be inherently reliable (*e.g.*, piping and tanks) and SSCs that may not be explicitly modeled (*e.g.*, room-cooling systems). These SSCs are safety significant.
7) The SSC is necessary for safety-significant operator actions credited. An example is instrumentation equipment. The pressure-sensor failure directly leads to the operator-discharge failure. Thus, the pressure sensor is safety significant for the pressure-tank system.
8) The SSC is necessary for safety-significant operator actions to assure long-term containment integrity or offsite emergency planning activities.

If none of the above conditions is true, low safety significance can be assigned, if the following condition is met:

1) Historical data show that these failure modes are unlikely to occur and such failure modes can be detected and mitigated in a timely fashion, or
2) A condition-monitoring program would identify the degradation of the SSC prior to its failure.

Risk-informed Categorization

PRA provides insights that may be utilized to support the determination of the relative safety significance of plant SSCs. The probabilistic insights help identify low safety-significant SSCs that are candidates for reductions in QA treatment. The QA is graded commensurately with these categorizations [32].

The principles for categorizing SSCs are [18]:

1) Use applicable risk-assessment information. The categorization is thus risk informed.

2) The categorization process should employ a blended approach considering both quantitative PRA information and qualitative information. The process is called an integrated decision making panel (IDP). There should be at least five experts as members of the IDP in the fields of: (1) plant operations, (2) design engineering (including safety analyses), (3) systems engineering, (4) licensing, and (5) PRA.
3) The Regulatory Guide 1.174 principles of the risk-informed approach to regulations should be maintained.
4) A safety-related SSC will, as a default, be categorized as RISC-1 unless a basis can be developed for recategorizing it as RISC-3.
5) Attribute(s) that make a SSC safety significant should be documented.

Table 2.16. Example importance summary

Component-failure mode	FV	RAW	CCF RAW
1) Valve “A” fails to open	0.002	1.7	n/a
2) Valve “A” fails remain closed	0.00002	1.1	n/a
3) Valve “A” in maintenance (closed)	0.0035	1.7	n/a
4) Common-cause failure of valves “A”, “B” and “C” to open	0.004	n/a	54
5) Common-cause failure of valves “A” and “B” to open	0.0007	n/a	5.6
5) Common-cause failure of valves “A” and “C” to open	0.0006	n/a	4.9
Component importance	0.01082 (sum)	1.7 (max)	54 (max)
Criteria	> 0.005	> 2	> 20
Candidate safety significant?	Yes	No	Yes

2.3.4 Internal Event Assessment Example

Redundant-valve Example
Consider an example in reference [18]. The importance-measure criteria used to identify candidate safety significance are:

C1) Sum of FV (Fussell–Vesely) importance values for all basic events modeling the SSC of interest, including common-cause events > 0.005.
C2) Maximum of component basic event RAW (risk-achievement worth) values > 2.
C3) Maximum of applicable common-cause basic events RAW values > 20.

The importance measures are defined and discussed in NUREG/CR-3385 [33] and [29]. See Equations 2.3 and 2.4.

Three failure modes are considered for valve “A”: 1) failure to open, 2) failure to close, 3) closed by maintenance. Common-cause failure (CCF) events (failures to open) are considered for the three sets of valves including valve "A": 1) "A", "B" and "C", 2) "A" and "B", and 3) "A" and "C". These sets are called common-cause component groups (Section 8.2.2).

The FV condition C1 is met because 0.01082 > 0.005. The CCF RAW condition C3 is also satisfied for common-cause group "A", "B" and "C": 54 > 20. The three valves would be identified as candidate HSS.

Attribute(s) that make a SSC safety significant should be documented. The component-failure mode dominating the screening criteria is failure to open. This mode is used as a safety-significant attribute.

Table 2.17. Minimal cut sets of pressure-tank system

1	2	3	4	5	6	7
No.	Minimal cut	Freq./year	FV PS1	RAW PS1	FV C1	RAW C1
1	{C1,SW,RV,SIS}	0.000005		col 3	col 3	0.00005
2	{C1,OP1,RV,SIS}	0.000005		col 3	col 3	0.00005
3	{C1,PS1,RV,SIS}	0.000005	col 3	0.00005	col 3	0.00005
4	{TM,SW,RV,SIS}	0.000005		col 3		col 3
5	{TM,OP1,RV,SIS}	0.000005		col 3		col 3
6	{TM,PS1,RV,SIS}	0.000005	col 3	0.00005		col 3
7	{OP0,SW,RV,SIS}	0.000005		col 3		col 3
8	{OP0,OP1,RV,SIS}	0.000005		col 3		col 3
9	{PS1,RV,SIS}	0.00005	col 3	0.0005		col 3
	Total	0.00009	0.00006	0.00063	0.000015	0.000225

Table 2.18. Summary of FV and RAW importance for pressure sensor, relay contact and switch

Description	FV	RAW
PS1 (Stuck low)	$\frac{0.00006}{0.00009} = 0.66$	$\frac{0.00063}{0.00009} = 7$
C1 (Stuck closed)	$\frac{0.000015}{0.00009} = 0.16$	$\frac{0.000225}{0.00009} = 2.5$
SW (Stuck closed)	0.16	2.5

Pressure-tank Example

A calculation process of FV importance and RAW is shown in Table 2.17 for the pressure-tank problem. Column 2 enumerates minimal cut sets. Column 3 gives the annual frequencies of the cut sets. Each cut set frequency is calculated by a product of a cut set component frequency multiplied by probabilities. The bottom row is the total to give the frequency of the tank rupture.

Column 4 indicates the minimal cut sets containing component PS1, the first pressure sensor. The bottom row shows the total frequency when the summation is restricted to these 3 minimal cuts. It turns out that the FV importance of PS1 is 0.00006/0.00009 = 0.66, as shown in Table 2.18.

Column 5 shows the cut set frequencies when PS1 fails, *i.e.* its failure probability or frequency is set to unity. Only cut sets 3, 6 and 9 are affected. The total is the tank-rupture frequency when PS1 is being failed (or *not used*). The RAW thus becomes 0.00063/0.00009 = 7. This means that the risk-reduction factor of PS1 is 7. The RAW value turns out to be a risk-reduction factor used in IEC 61508 and 61511.

FV and RAW measures for contact C1 can be calculated in a similar way. It is easily examined from Table 2.17 that switch SW would have the same FV and RAW as contact C1. These results are summarized in Table 2.18.

The three components PS1, C1, and SW are high safety significant (HSS) according to the criteria just mentioned: FV larger than 0.005 or RAW larger than 2 for independent failures. Note that contact C1 of the timer system is not safety related but HSS because the contact failure may cause the first initiating event, *i.e.* pump overrun.

A SSC is not automatically low safety significant even if the risk importance measure criteria are not met, It must go through checks by other types of PRAs, defense-in-depth assessment, CDF and LERF impact evaluation and IDP review, as shown in Figure 2.7. The CDF and LERF evaluation is called "Sensitivity studies" by the NEI 00-04 document, which may be confused with the ordinary sensitivity studies described next.

Sensitivity Studies

The NEI 00-04 recommends sensitivity studies for internal events PRA:

1) Increase all human-error basic events to their 95th percentile values.
2) Decrease all human-error basic events to their 5th percentile values.
3) Increase all component common-cause events to their 95th percentile values.
4) Decrease all component common-cause events to their 5th percentile values.
5) Set all maintenance unavailability terms to 0.0.
6) Any applicable sensitivity studies to ensure PRA adequacy.

If, following the sensitivity studies, the component is still found to be low safety significant and if it is safety related, it is still a *candidate* for RISC-3. In this case the analyst is to define why the SSC is of low risk significance. For instance, the SSC does not perform an important function, the SSC is in excess redundancy, the SSC is rarely used, [18]. The risk-importance process, including sensitivity studies, is performed for both CDF and LERF.

The SSC can cause initiating events for the internal events PRA. This should be reflected in calculating the importance values. As a matter of fact, the pressure sensor PS1 causes the second initiating event, discharge failure. This has been reflected as the failure of the monitoring system sharing the same pressure sensor.

External Event and Shutdown PRAs

Similar categorization using the importance measures are carried out for external event PRAs including the fire PRA (Section 5.9). This is shown in the hazard-type column of Figure 2.7. A weighted sum of these importance measures is used in the NEI document to integrate internal PRA with external PRAs. Similar criteria as the internal event PRA are used for the weighted importance.

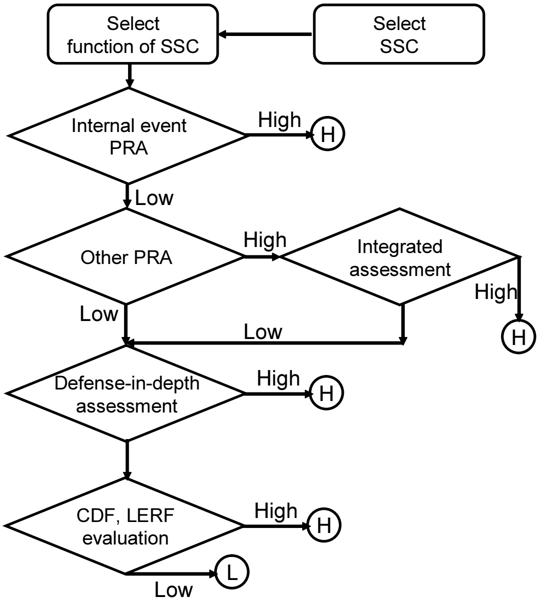


Fig. 2.8. Determination of low safety-significance candidate to be fed into IDP

Figure 2.8 shows two paths ending in LSS in the categorization process using risk information prior to a defense-in-depth assessment described in Section 3.8.

1) LSS by internal event PRA and LSS by other PRAs, or
2) LSS by internal event PRA but HSS by other PRAs and yet LSS by integral assessment.

Categorization of Function and SSC
A safety function supported by a HSS SSC is regarded as HSS. Otherwise, the safety function is a LSS candidate.

Once a function is labeled as HSS, all SSCs that support this function are, as default, assigned as HSS. Some SSCs support multiple functions. The SSC should be assigned the highest risk significance of the functions that the SSC supports. These conditions may override individual SSC evaluations by importance measures. Final decisions are made by the IDP.

The criterion for nondefault assignment of low safety significance for an SSC supporting a safety-significant function is that its failure would not preclude the fulfillment of the safety-significant function.

For each RISC-1 (or RISC-2) SSC, attributes are clarified. Examples include high-level features such as “provide flow”, “isolate flow”, *etc.* These attributes are monitored and maintained by the special treatment activities.

2.4 Safety Significance of Human Actions: NUREG-1764

2.4.1 Human-factors Engineering Review

Consider the pressure-tank system, The process-monitoring system includes the human action of opening the electric switch to shutdown the pump upon detection of overpressure. The tank system also contains a human action causing an initiating event, *i.e.* discharge failure.

Using a manual action in place of an automatic action and reducing the time available are typical changes to human actions (HAs). Plant modifications, procedure changes and others yield changes in HAs. A plant change may include changes to equipment, as well as to HAs. Changes to HAs involve new actions, modified actions, or modified task demands.

NUREG-1764 [13] provides guidance to determine the appropriate level of human-factors engineering review of human actions based upon their safety significance. The guidance can be applied to categorization of the existing human actions even if these are not the changes. This section describes the safety-significance categorizations of existing human actions from the point of view of the NUREG-1764 approach.

The guidance now has three steps for the existing HAs. The first step is quantitative, while the second is qualitative. The third step is an integrated assessment [13]:

Step 1) A quantification of the risk importance of the HA to be categorized,
Step 2) A qualitative evaluation of the safety significance of the HA, and,
Step 3) An integrated assessment of HA safety significance to determine the appropriate level of human-factors (HF) engineering review.

The human actions are assigned to one of three safety-significance levels (high, medium, low). After the categorization of human actions, these are reviewed using standard criteria in human-factors engineering to verify that the actions can be reliably performed when required. A risk-informed approach is used to determine the safety significance for graded human-factors engineering review.

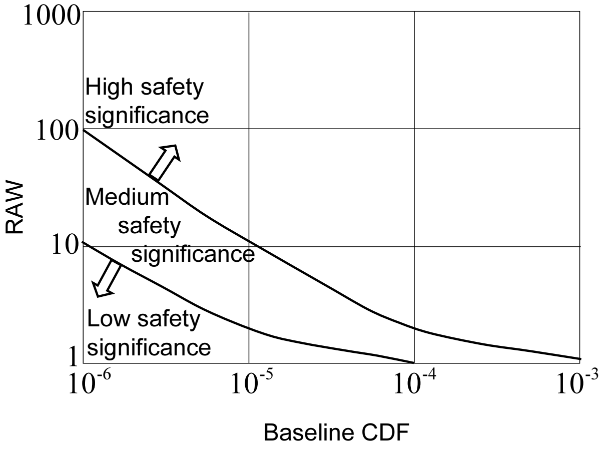


Fig. 2.9. RAW and baseline CDF

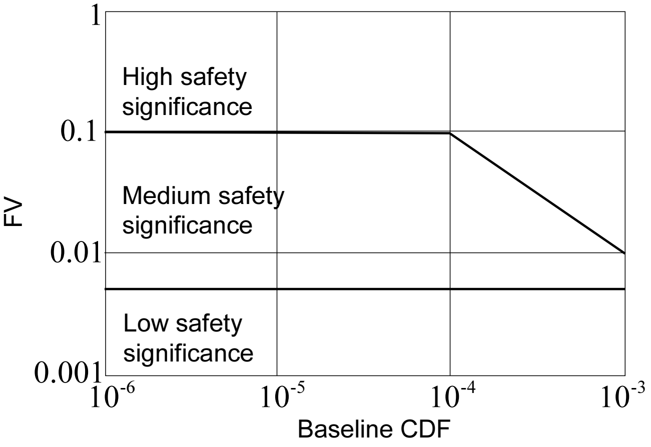


Fig. 2.10. FV and baseline CDF

2.4.2 Step 1: Quantitative Assessment

High safety-significant HAs should be identified from the PRA and human-reliability analysis (HRA). The PRA is level 1 (core damage) and/or level

2 (release from containment) including both internal events and/or external events (if available). Refer to Chapter 5 for the PRA levels.

HAs should be categorized using more than one importance measure and HRA sensitivity analyses to provide adequate assurance that an important human action is not overlooked because of the selection of the measure or the use of a particular assumption in the analysis.

The RAW and FV importance measures are typically used as in the case of SSCs. They are evaluated relative to the plant baseline CDF. The RAW is the increase in CDF when the HA fails. That is, the HEP (human-error probability) of the HA is increased from its base-case value to 1.0 and the overall CDF is recomputed. The equation for RAW for HA is:

$$\text{RAW(HA)} = \frac{\text{CDF with HA being failed}}{\text{Baseline CDF}} \tag{2.3}$$

A high RAW value means that failure of the HA results in a risk-significant situation. In other words, the HA with the base-case reliability reduces the risk by the factor of RAW. The HA reliability should be verified by a thorough human-factors engineering review for high RAW values.

FV is defined as the CDF of core-damage cut sets (or accident sequences or scenarios) that contain the HA in question, divided by the total CDF:

$$\text{FV(HA)} = \frac{\sum \Pr\{\text{CDF cut sets containing HA}\}}{\text{Baseline CDF}} \tag{2.4}$$

If FV is high, the HA with the base-case reliability contributes to a relatively large portion of risk. Thus, for defense-in-depth purposes, the HA reliability should not be degraded further to result in a large increase of CDF. A thorough human-factors engineering review is required to prevent and detect the degradation.

The FV is included to obtain a more robust evaluation of safety significance because if the HEP is too high or too low due to uncertainty or poor modeling, this will affect both the RAW and FV measures, but in opposite directions. The FV importance measure addresses HAs that may not have a high RAW value (*e.g.*, due to a relatively low HEP), but that contribute notably to the CDF.

Figures 2.9 and 2.10 show the safety-significance assignments for RAW and FV. The terms “Level I, II, III” were used in NUREG-1764 to represent the safety significance of the HA. However, this terminology is confusing when we say “increase level by one”. In NUREG-1764 the increase from Level II means a move to Level I. The level numbering is in the reverse order compared to SIL.

This section rewrites the levels in the following way: 1) Level I: high safety significance (HSS), 2) Level II: medium safety significance (MSS), 3) Level III: low safety significance (LSS).

After both RAW and FV are determined, the HAs should be placed in the most conservative or highest safety significance of the two figures. Similar assignments can be made for LERF evaluations.

Human actions of HSS receive a detailed human-factors engineering review and those of MSS undergo a less-detailed one, commensurate with their safety significance. For human actions placed in LSS, there is a minimal human-factors review or none except for verification that the action is in fact in this safety significance.

The curve between the HSS and MSS areas of Figure 2.9 is roughly based on a CDF of 10^{-4} core-damage events per reactor-year, given the failed HA. This CDF is the subsidiary objective. Similarly, the curve between the MSS and LSS areas are roughly based on a CDF of 10^{-5} core-damage events per reactor-year, one order of magnitude less than the subsidiary objective.

The evaluation should consider all of the relevant HAs. Any dependent HAs should be aggregated together. Any HAs that are not dependent can be treated separately.

Consider the pressure-tank system as an illustrative example. The human action OP1 has the same importance measures as timer contact C1: RAW of 2.5 and FV of 0.16. The baseline value is 0.9×10^{-4}. A conservative classification yields HSS from Figure 2.9. The same HSS is obtained from Figure 2.10.

The assessment of the safety significance of an HA may be checked by performing appropriate sensitivity studies, varying the HEP through its range of uncertainty, as, for example, characterized by the 90% confidence interval. The final assessment should be conservative.

Furthermore, if there are judged to be dependent HAs that were not properly modeled in the HRA and if the reviewer is unable to adequately address them, then increasing the human-factors review of the set of dependent HAs should be considered. For the pressure-tank system, human actions OP0 and OP1 are dependent HAs because both are performed by the same operator.

There also may be cases when a lessening of the defense-in-depth or safety margin is only relied on a HA. Then, an increase of the human-factors review would be appropriate.

2.4.3 Step 2: Qualitative Assessment

Step 2 modifies the safety-significance assignment of Step 1 by qualitative criteria. These results can be either: 1) no change, 2) elevate one level, or 3) reduce one level.

Elevate Level of HF Review by One

If "yes" responses are obtained for many qualitative criteria described below, the level of review of the HA should probably be increased. If a "yes" response is received for only one or two criteria, then the analyst should consider whether the "yes" response is sufficient to warrant elevating the level of review.

1) Operating experience: Experience/events at that plant or plants of similar design show poor performances of the HAs under consideration.

2) New responsibility: The human actions require new responsibilities for the success of safety functions. An example may be the reallocation of responsibility from an automatic system to personnel for the initiation, ongoing control, or termination of a function. The operator of the pressure-tank example has two responsibilities: prevention of initiating event and mitigation of pump-overrun event.
3) Difficult tasks: The HA is significantly different from the way in which personnel usually perform their tasks (*e.g.*, making them more complex, significantly reducing the time available to perform the action, increasing the operator workload, changing the operator role from primarily "verifier" to primarily "actor").
4) Difficult context: Here, context is defined as the overall performance environment, including plant conditions and behavior that, for example, affect the time available for the operator response and the effectiveness of job aids. A manual action for a safety-related function is now required under new circumstances. The operator of the pressure-tank example may be asked to initiate the pumping cycle urgently, forgetting to discharge the gas.
5) Degraded HSIs (human–system interfaces): The HA changes the HSIs significantly that are used by personnel to perform the task. For example, the pressure-tank operator now performs tasks from a control room, whereas previously the tasks were performed onsite where the operator could hear the gas discharged.
6) Degraded procedures: The HA significantly changes the procedures that personnel used to perform the task, or the task is not supported by procedures.
7) Problem of training: The HA significantly modifies the training, or the task is not addressed in training.
8) Less teamwork: For example, (1) one operator is now performing the tasks accomplished by two or more operators in the past, (2) it is now more difficult to coordinate the actions of individual crew members, or, (3) task performance is more difficult to supervise.
9) Less skill: It is necessary for an individual who is less trained and has lower qualifications to take the action.
10) More communication demands: The HA significantly increases the level of communication needed to perform the task. For example, an operator must now communicate with other personnel to perform actions as compared with a task at a local panel containing all necessary HSIs.
11) Degraded environment: The HA significantly increases the environmental challenges (such as radiation, or noise) that could negatively affect task performance.

Reduce Level of HF Review by One

The analyst should consider reducing the level of HF review if the HA has the following characteristics.

1) The answers are "no" to most of the qualitative criteria. One "yes" answer should not necessarily preclude a reduction in the level of the review, unless it is a "yes" to a significant criterion.
2) The action is well defined and the analyst is confident that it can be easily performed. For example, (1) it is clear when to perform the action, (2) there are clear procedures, (3) there is sufficient time and staff available, and (4) the action is similar to those routinely taken.

When the review is reduced to LSS, the following criteria taken from Chapter 19 of the Standard Review Plan (SRP), Appendix C.2 should be used to verify that the SSCs or human actions are of LSS [9]:

1) The HA does not relate to the performance of a safety function or a support function to a safety function, or does not complement a safety function. The HA does not support other operator actions that are credited in PRAs for either procedural or recovery actions.
2) The failure of the HA will not result in the eventual occurrence of a PRA initiating event.
3) The HA is not required in maintaining barriers to the release of fission products during severe accidents.
4) The failure of the HA will not unintentionally release radioactive material, even in the absence of severe accident conditions.

If any of the above criteria are not satisfied, then re-elevation to a MSS human-factors review is recommended.

2.4.4 Step 3: Integrated Assessment

This step integrates the results from Steps 1 and 2. For example, assume that Step 1 gives LSS, and Step 2 results in "elevate". Then, Step 3 may yield MSS.

2.5 Concluding Remarks

Three types of categorization are described to determine the safety significance of safety-instrument systems, SSCs, and human actions, respectively. The next chapter develops how the performance required for each category can be materialized.

3

Realization of Category Requirements

3.1 Introduction

Safety goals, quantitative health objectives, subsidiary numerical objectives, and tolerable risks are dealt with in Chapter 1. Risk-informed categorizations of safety systems, SSCs and human actions are described in Chapter 2 from the point of view of safety significance in satisfying tolerable or acceptable risk levels. This chapter considers how the requirements demanded for each category can actually be satisfied by uncertainty management, compliance with standards and regulations, dependent failure management, safety margins, human-factors review, early detection and treatment, defense-in-depth, and performance evaluation.

3.2 Uncertainty

We must first decrease uncertainties. Guiding principles for uncertainty reduction are 1) simplicity, 2) clarity, 3) understandability, 4) transparency, 5) consistency, and 6) completeness.

These principles are typically used in generating specifications and designs. Structured and modular specification and design reduce complexity. Checklists, inspection, simulation, and formal methods during specification and design increase completeness [1]. SISs should be listed for each plant-operation mode such as startup and each operational procedures such as equipment maintenance, sensor calibration, *etc.* Operation and maintenance instructions must be clear and understandable. If only a small number of uncertainties were left, actual applications would satisfy the safety goals in almost the same way as predicted by the PRA.

The parametric, modeling, and completeness uncertainties make this optimism a daydream. To cope with the residual uncertainties, we must adhere to principles such as compliance with standards and regulations, quality assurance, well-tried components, redundancy, independence, diversity, defense-in-depth, safety margin, early detection and treatment, and so on.

3.3 Guidelines, Standards, and Regulations

The compliance is important in reducing and treating uncertainties. This point is also emphasized as a Regulatory Guide 1.174 principle in Chapter 1. Typical standards are those of quality-assurance programs such as Appendix B to 10 CFR Part 50 and ISO 9000. Good engineering practices or AGPP (Section 1.7.3) must also be observed. Safety life-cycle viewpoints are advocated by many standards. Figure 3.1 shows phases after determination of SILs of functional safety systems or safety-instrumented systems [1, 11] The safety requirement phase clarifies specifications of SIS including success criteria. The design phase determines architecture such as 1-out-of-2 structures. The SIS installation is validated, for instance, by walk through. Operation includes manual interventions during failures in the SIS. The SIS modification is managed by a change control.

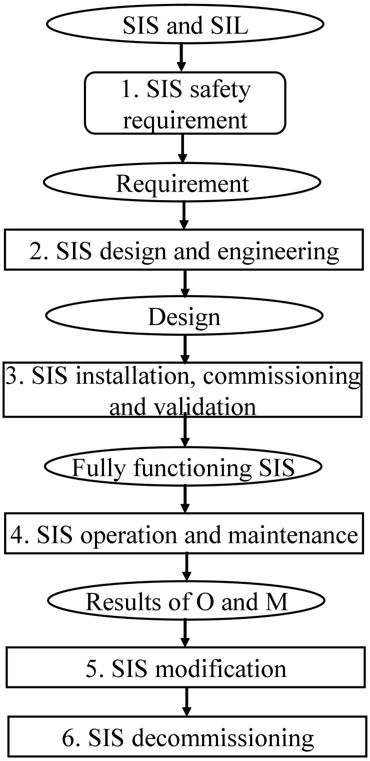

SIS and SIL
1. SIS safety requirement
Requirement
2. SIS design and engineering
Design
3. SIS installation, commissioning and validation
Fully functioning SIS
4. SIS operation and maintenance
Results of O and M
5. SIS modification
6. SIS decommissioning

Fig. 3.1. SIS safety life cycle after determination of SIL

3.4 Management of Dependent Failures

Various dependencies among failures are frequently overlooked to result in significantly underestimated risks.

3.4.1 Types of Dependencies

Chapter 19 of the Standard Review Plan [9] describes four types of dependencies: 1) functional dependencies, 2) human-interaction dependencies, 3) component hardware failure dependencies, and 4) spatial dependencies.

Functional Dependencies
These dependencies occur because the function of one system or component depends on that of another system or component. Functional dependencies include interactions that can occur when the change in the function of a system or component causes a physical change in the environment that results in the failure of another system or component.

Functional dependencies are further classified into [9, 11, 34]:

1) Shared-component dependencies. For example, systems or system trains that depend on a common intake or discharge valve have this dependency. These are also called shared-equipment dependencies.
2) Actuation-requirement dependencies. Systems that depend on the following items for initiation or actuation:
   2-1) common signals, common circuitry;
   2-2) common support systems like AC or DC power for instruments;
   2-3) conditions such as low reactor pressure vessel water level;
   2-4) permissive and lockout signals that are required to complete actuation logic.
3) Isolation-requirement dependencies. These originate from conditions that could cause more than one system to isolate, trip, or fail. These conditions include:
   3-1) environmental conditions such as temperature, pressure, or humidity;
   3-2) temperature and pressure of fluids being processed;
   3-3) water-level and radiation-level status.
4) Power-requirement dependencies. For example, systems that depend on the same power sources for motive power have this dependency. This is an example of functional input dependency defined in [34]. In other words, component B is not functionally unavailable as long as A is not working. Once electric power becomes available, the pump will be operable because the pump is not damaged by the power failure.
5) Cooling-requirement dependencies. Systems that depend on the following items for cooling:
   5-1) the same room-cooling subsystem;
   5-2) the same lube-oil cooling subsystem;
   5-3) the same service-water train;

   5-4) the same cooling-water train.

6) Purity-requirement dependencies. These yield, for example, plugging of relief valves and sensors [11].
7) Indication-requirement dependencies. For example, systems that depend on the same pressure, temperature, or level instrumentation for operation have this dependency.
8) Cascade failure. Failure of A leads to hardware failure of B [34]. For example, failure of a valve on a pump suction line to open, may damage the pump if it is started. Even if the valve is made open later, the pump would still be inoperable because of damage.
9) Phenomenological-effect dependencies. These are caused by conditions generated, for example, during an accident sequence that influence the operability of more than one system. These are also called "physical–environmental" dependencies [34]. These are similar to the cascade failure. These conditions include:
   9-1) harsh environments that result in protective trips of systems;
   9-2) loss of pump net positive suction head when containment heat removal is lost;
   9-3) clogging of pump strainers from debris (from active as well as passive components) generated during a loss of coolant accident (LOCA);
   9-4) failure of components outside the containment following containment failure attributable to harsh environment inside the containment;
   9-5) coolant pipe breaks or equipment failures resulting from containment failure;
   9-6) high vibration induced by component A causes failure of component B.
10) Operational dependencies.
   10-1) mode 1 is unavailable when the system is in mode 2;
   10-2) individually safe process states can create a separate hazard such as overload of emergency storage when occurring concurrently [11].

NUREG/CR-5485 defines functional *requirement* dependency as the case where the functional requirements of component B is determined by the functional status of component A [34]. For instance,

1) B is needed when A fails.
2) B is needed when A works.
3) B is not needed when A fails.
4) B is not needed when A works.
5) Load on B is increased upon failure of A.

Human-interaction Dependencies

These dependencies could become important contributors to risk if operator error can result in multiple component failures. Past PRAs show that the following plant conditions could lead to human-interaction dependencies:

1) Tests or maintenance that require multiple components to be reconfigured.

2) Multiple calibrations performed by the same personnel.
3) Postaccident manual initiation (or backup initiation) of components that require the operator to interact with multiple components.

Spatial Dependencies
Multiple failures could be caused by events that fail all equipment in a defined space or area. These spatially dependent failures include those caused by internal flooding, fires, seismic events, turbine missiles, or any of the other external event initiators.

In cases where these events are not modeled in the PRA, the dependencies resulting from the unmodeled initiators should be evaluated qualitatively as part of the integrated decision making process. Inadequate space, inadvertent or spurious sprinkler operation, or routine equipment travel near major components are causes of the spatial dependencies.

Component Hardware Failure Dependencies
These dependencies, usually referred to as common-cause failures (CCFs), typically cover the failures of identical components that may be caused by systematic failures including design, manufacturing, installation, calibration, operational deficiencies. CCFs are treated quantitatively by common-cause failure analysis (Chapter 8) such as alpha- and beta-factor methods [36].

3.4.2 Common-cause Failures

Explicit Dependency and Implicit Dependency
Where appropriate, these dependencies such as shared component, actuation requirement, isolation requirement, power requirement, cooling requirement, purity requirement, indication requirement, phenomenological effect, operation, human interaction, and spatial dependencies have been included explicitly in the accident-sequence models (event trees, ETs) and the mitigation-system analysis models (fault trees, FTs). The dependencies represented in ETs or FTs are called explicit dependencies. Common-cause failure analysis deals with residual, implicit dependencies typified by “component hardware failure dependencies” other than the explicit ones.

Coupling Mechanisms and Common-cause Failures
The common-cause failures occur because of similarities that are common to a group of components. The similarities are called coupling mechanisms [34]. For example:

1) Hardware-based.
    1-1) Same physical appearance.
    1-2) Same layout or configuration.
    1-3) Same subcomponents.
    1-4) Same manufacturing attributes. The attributes include manufacturing staff, quality-control procedure, manufacturing method, and material.

1-5) Same construction or installation attributes. These include the same staff, procedure, and schedule.

2) Operational-based.
   2-1) Same operating staff.
   2-2) Same operating procedure.
   2-3) Same maintenance or test or calibration schedule.
   2-4) Same maintenance or test or calibration staff.
   2-5) Same maintenance or test or calibration procedures. Unfortunately, it is impractical to implement diverse procedures for nondiverse equipment.

3 Environmental-based.
   3-1) Same plant location.
   3-2) Same component locatioin.
   3-3) Common environment or working medium.

3.4.3 Safety Principles for Dependency

The dependency between the SIS and BPCS, and the SIS and other protection layers shall be taken into consideration. The following provisions as stated in IEC 61511, 61508, EN 954, NUREG/CR-5485 and others should be provided for each type of dependence.

Shared-component Dependencies

1) A device used to perform part of a SIS shall not be used for BPCS. This is because, if the shared component fails, a demand will be created to which the SIS may not be capable of responding.
2) Suppose on the other hand that a shared component is used between SIS and BPCS. It should be ensured that the component dangerous-failure rate is sufficiently low or that a failure of BPCS does not compromise SIS. Sensors and valves are examples where the sharing of components with the BPCS is often committed.
3) Suppose that a SIS implements safety- and nonsafety-instrumented functions. All the hardware and software shall be treated as part of the SIS with the highest SIL if they can negatively affect any safety-instrumented functions. A programming access to the nonsafety software may cause a dangerous failure of SIS.
4) Suppose that hardware and software are shared by SISs with different SILs. These hardware and software shall conform to the highest SIL unless otherwise justified.

Power-requirement Dependencies

1) Manual means to achieve the safe state are provided during the power failure.
2) Overvoltage or undervoltage are detected and coped with by safety shutoff or switchover to second power unit [1].

3) The voltage of a supplemental power supply, such as a battery backup or an uninterruptible power supply, is monitored and a powerdown, for instance, is initiated when the voltage becomes out of range.
4) The switching position required to execute the safety function is realized by removing the control signal, such as electrical voltage and pressure, *i.e.* by switching off the energy supply. This fail-safe design is called a "closed-circuit principle" or "idle-current principle" or "de-energized to trip" [23].
5) The SIS should not initiate any unexpected reactions including spurious operations when the power supply (voltage or pressure) fluctuates [23].
6) Disconnection from the energy supply and discharge of the residual energy should be available to make things safer when the safety function does not depend on the supply [23]. All safety-critical information should be stored prior to the disconnection and discharge.
7) Surge-immunity testing is performed to check the capacity of the safety-related system to handle peak surges [1].

Cooling-requirement Dependencies

1) Temperature increase is measured by sensors to detect overtemperature. For higher SIL, actuation of safety shutoff via a thermal fuse should be available [1].
2) The fans are monitored [1].
3) A forced-air cooling is activated for temperatures beyond specification. An alarm is issued [1].

Human-interaction Dependencies

1) The human–machine interfaces shall follow good human-factors practice described typically in references [37, 38].
2) Inspection of the safety-requirement specification is performed by an independent person to correct the specification error [1].
3) Inspection of the hardware is performed by a person independent of the design to correct the design error [1].
4) Walk-through of the hardware is performed by a person independent of the design to correct implementation error, *etc.* [1].
5) Modification protection: The safety-related system is protected against hardware modifications [1].

Purity-requirement Dependencies

1) The necessary purity class of the pressure medium is achieved by a suitable device (usually a filter) [23].
2) Prevention of dirt intake is considered by "negative pressure" or a vent filter [23].
3) Increase of interference immunity is provided by a noise filter at the power supply and by a filter against electromagnetic injection [1].

Phenomenological-effect Dependencies

1) One or more pressure-control valves are provided to prevent the pressure from rising beyond a specified level [23].
2) Any SIS necessary to service a major accident remains operational. For example, a valve remains operational for certain periods during a fire (IEC 61511).

Component Hardware Failure Dependencies

1) Decrease of total failure rates is important because this leads to a reduction of common-cause sources such as maintenance activities.
2) Systematic failures are typical common causes, and their reduction leads to a decrease of common-cause failures [1].
3) Online diagnostic test is important to detect the first failure before propagating to a common-cause failure [1].
4) Diversity means the use of a totally different approach to achieve roughly the same results (functional diversity) or the use of different types of equipment in design to perform the same function (equipment diversity). Staff diversity uses different teams to install, maintain, and/or test redundant trains [34].

   IEC 61508 considers the equipment diversity. It also considers another type of diversity related to defense-in-depth; two or more items carrying out different functions [1]. Diversity between protection layers are important [11]. Diverse programming is also important for PLCs.
5) Physical protection and spatial separation to avoid common-cause failures [11, 34]. The protection is based on a passive barrier to act as a shield or an environment separator. For example, protection and separation are used
   5-1) between different protection layers;
   5-2) between safety-related systems and nonsafety-related systems;
   5-3) between multiple lines;
   5-4) between electrical energy lines and information lines to minimize crosstalk [1].
6) Prohibition of write access from nonsafety-related systems to safety-related systems.
7) When processing redundant signals, one channel uses a logic 1 while the other uses a logic 0 [23]. Common-cause failures by electromagnetic emission can be detected [1].
8) Transmission redundancy where the same information is transferred several times in sequence [1].
9) Information redundancy where data is transmitted in blocks, together with a calculated checksum for each block.
10) Interlocks between redundant components or channels so that only one at a time can be taken out of service of testing or maintenance. This reduces errors such as mistakenly performing a test on one component while the standby component is undergoing preventive maintenance [34]. See Section 5.2.2 for a related topic about railroad accidents.

11) Removal of crossties between redundant trains will eliminate common-cause failures. Strong administrative controls are required when crossties are used to cope with some other causes of failures [34].
12) Staggered testing and maintenance offers some advantages over simultaneous ones [34]. The probability that an operator repeats an incorrect action is lower when test or maintenance are performed, for instance, months apart. The staggered test and maintenance also reduces a time span where components are exposed to common-cause failures (see Section 8.2.4).
13) Increasing the degree of redundancy may decrease common-cause failures because more operational diversity in a staggered test becomes available [34].

Cause-defense Matrix

NUREG/CR-5485 introduces a cause-defense matrix [34]. For diesel generators, the following causes of common-cause failures are considered as rows of a matrix: 1) corrosion products in an air-start system, 2) dust on relay controls, 3) governor out of adjustment, 4) water or sediment in fuel, 5) corrosion in jacket-cooling system, 6) improper lineup of cooling-water valves, 7) aquatic organisms in service water, 8) high room temperature, 9) improper lube-oil pressure-trip point, 10) air-start system with closed valve, 11) fuel-supply valves left closed, 12) fuel-line blockage, 13) air-start receiver leakage, and 14) corrective maintenance on wrong diesel generator.

The selected defense against root causes and coupling mechanisms are placed as columns:

1) General administrative or procedural controls.
   - 1-1) configuration control (*e.g.,* valve status);
   - 1-2) maintenance procedures;
   - 1-3) operating procedures;
   - 1-4) test procedures.
2) Specific maintenance or operation practices.
   - 2-1) governor overhaul;
   - 2-2) drain water and sediment from fuel tanks;
   - 2-3) corrosion inhibitor in coolant;
   - 2-4) service-water chemistry control.
3) Design features.
   - 3-1) air dryers or air-start compressors;
   - 3-2) dust covers with seals on relay cabinets;
   - 3-3) fuel-tank drains;
   - 3-4) room coolers.
4) Diversity.
   - 4-1) functional;
   - 4-2) equipment;
   - 4-3) staff.
5) Barrier.
   - 5-1) spatial separation;

   5-2) removal of crossties or implementation of administrative controls, otherwise.

6) Testing and maintenance.
   6-1) staggered testing;
   6-2) staggered maintenance;

For instance, defense “1) configuration control” has a strong impact on “6) improper lineup of cooling water valves”. Note that some defenses affect the root causes, while others affect the coupling mechanisms. A root cause of a component failure is a cause of which removal may lead to successful component operation.

3.5 Safety Margins

Safety margins often introduced in deterministic analyses to account for uncertainty and provide an added margin to provide adequate assurance that the various limits or criteria important to safety are not violated [13].

Some of the safety principles concerning the safety margins are extracted from IEC 61511, IEC 61508, EN 954 and others.

1) An adequate overlap between contacts in a closing state for slide valves.
2) The actuating forces should withstand the frictional forces.
3) Safety-related components are designed in such a way that they can fulfill their function under influences that are usual for the application. This is called “resistance to relevant external influences” [23]. The safety margin is called “sufficient overdimensioning” in IEC-61508.
4) All components are selected such that they can withstand the anticipated stresses such as force, vibration, voltage, pressure, flow, temperature, viscosity [23].
5) Derating is considered where hardware components are operated at stress levels well below the maximum specification ratings [1].
6) The capacity of the safety-related system to handle peak surges [1].
7) Worst-case testing and failure-insertion testing are performed [1].
8) Safety margin is increased for human action by making a longer time available to perform the action.
9) Proven-in-use components are used. For instance, 10 000 h operation time, at least one year’s experience with at least 10 devices in different applications, and no safety-critical failures [1]. Stricter conditions for higher SIL. Well-tried computer memories and programs.
10) Observance of guidelines and standards is made. This is not restricted to the safety margins, but the observance is important to ensure reasonable margins.
11) Maximum allowable spurious trip rate is specified.
12) Realistic mean time to repair estimate is used.
13) A definition of process safe-state is given for each SIS. Successful operation of SIS output such as tight shutoff valves is defined.

3.6 Human-factors Review for HSS Human Actions

One of the deterministic aspects of design, as discussed in Regulatory Guide 1.174, is to ensure that the HA meets current regulations, and does not compromise defense-in-depth.

Human-factors reviews include those of 1) operating-experience review, 2) functional-requirements analysis and function allocation, 3) task analysis, 4) staffing, 5) probabilistic risk and human-reliability analysis, 6) human-system interface design, 7) procedure design, 8) training-program design, 9) human-factors verification and validation, and 10) human-performance monitoring strategy [13].

Some points to note are listed below [1, 13]:

1) Human-system interface (HSI) technologies: Human-performance issues associated with HSI technologies are identified for the HAs.
2) The HSI design seeks to minimize the probability that errors will occur, and maximize the probability that errors will be detected and personnel will be able to recover them.
3) The HSI design contains all necessary alarms, displays, and controls to support plant-personnel tasks.
4) The function-allocation analysis considers not only the personnel role of initiating manual actions but also responsibilities concerning automatic functions, including monitoring the status of automatic functions to detect system failures. The demands upon the personnel are considered in terms of all other concurrent demands upon the same personnel. The overall level of workload is considered when allocating functions to the personnel.
5) For each specific scenario, the tasks that personnel are required to perform are identified and assessed. Such tasks can include necessary primary (*e.g.*, start a pump) as well as secondary (*e.g.*, access the pump-status display) tasks. This analysis is used for the identification of errors of omission. The proper completion of required tasks is verified.
6) The task analysis identifies the information required to inform personnel that each HA is necessary, that the HA has been correctly performed, and that the HA can be terminated.
7) The task analysis addresses the full range of plant conditions and situational factors, and performance-shaping factors anticipated to influence human performance. A range of plant-operating modes relevant to the HAs (*e.g.*, abnormal and emergency operations, transient conditions, and low-power and shutdown conditions) is included in the task analysis.
8) Addition of additional manual actions to periods of high workload is checked whether it increases staffing needs.
9) HSS HAs are used as input to the design of procedures, HSI components, and training.
10) Where appropriate, procedures identify how the operating crew independently verify that the HAs have been successfully performed.

11) The training program addresses the knowledge and skill requirements for all HAs for the licensed and nonlicensed personnel.
12) Sufficient evidence is given to provide reasonable confidence that operators have maintained the skills necessary to accomplish the assumed actions.
13) Operation possibilities are limited. Password is required to allow change of operation mode [1].
14) Operation is performed only by skilled operators. Basic training plus two years on-the-job experience to avoid misuse [1].
15) Protection is provided against operator mistakes: Confirmation and consistency checks on each input command [1]. Echoing of input actions back to the operator is called input acknowledgement. Incorrect input actions are rejected by the consistency check.
16) User friendliness is realized to reduce complexity during operation of the safety-related system [1].
17) Maintenance friendliness is realized to simplify maintenance procedures and to provide necessary means for effective diagnosis and repair [1].
18) Overrides and their cancellations are provided when justified.

3.7 Early Detection and Treatment

3.7.1 Detection Examples

Detection methods found in IEC 61508-7 include:

1) Relay contacts and comparators are monitored.
2) Hardware redundancy is used to detect failures.
3) Transmission redundancy (repetition) and information redundancy (checksum for each block) are used to detect failures of data paths.
4) Majority voters are used to detect and mask failures in a 1-out-of-3 architecture.
5) Two processing units are checked by reciprocal comparison by software.
6) Crossmonitoring of multiple actuators.
7) Static failures (stuck-at failure) are detected by a forced change (dynamic principle).
8) Self-tests by a set of patterns, and by additional special hardware.
9) Detection of odd-bit failures, one-bit failures, and multibit failures by signature, checksum, *etc.*
10) Detection of failures during addressing, writing, storing and reading (RAM test).
11) Watch-dog timer to monitor a defective program sequence.
12) Positive-activated switch to open a switch by a direct cam mechanism to ensure that the switch must have been opened.
13) Functional, black-box, or statistical testing.

14) Online diagnostic test and proof test are repeated periodically to detect failures as described in the next section.

3.7.2 Diagnostic Coverage

A dangerous failure is a failure that has the potential to put the safety-related system in a hazardous or fail-to-function state [1]. In a multiple-channel system, a dangerous hardware failure is less likely to lead to the overall dangerous or fail-to-function state.

A safe failure is a failure that does not have the potential to put the safety-related system in a hazardous or fail-to-function state. A safe failure typically leads to a safe shutdown.

A failure mode and effect analysis (Section 4.4) would be helpful to identify the dangerous failure and the safe failure.

Let λ_{D} denote the total dangerous-failure rate, and λ_{S} the total safe-failure rate. The word "total" means that a summation is taken over relevant failure modes. The failure rates are thus divided into dangerous-failure rate and safe-failure rate. For a complex component, a fifty-fifty division is generally accepted because detailed analysis is not feasible [1].

Online diagnostic tests are performed to detect failures in a safety-related system. The tests are repeated at a diagnostic-test interval such as 1 h.

A diagnostic coverage (DC) is defined as a fractional decrease in the probability of dangerous failures resulting from the online diagnostic tests [1].

The total dangerous-failure rate λ_{D} is thus divided into total undetected dangerous-failure rate λ_{DU} and total detected dangerous-failure rate λ_{DD}:

$$\lambda_{\mathrm{D}} = \lambda_{\mathrm{DU}} + \lambda_{\mathrm{DD}} \tag{3.1}$$

The diagnostic coverage DC for dangerous failures is given by:

$$\mathrm{DC} = \frac{\lambda_{\mathrm{DD}}}{\lambda_{\mathrm{D}}} = \frac{\lambda_{\mathrm{DD}}}{\lambda_{\mathrm{DD}} + \lambda_{\mathrm{DU}}} \tag{3.2}$$

This is simply termed "diagnostic coverage".

Some of the diagnostic coverage listed in Table C.2 of IEC 61508-6 are:

1) CPU: Less than 70% for low DC, and less than 90% for medium DC.
2) Communication and mass storage: 90% for low DC, 99.9% for medium DC, and 99.99% for high DC.
3) Sensors: 50% to 70% for low DC, 70% to 85% for medium DC, and 99% for high DC.

Denote by λ_{SU} the total undetected safe-failure rate, and λ_{SD} the total detected safe-failure rate. Diagnostic coverage for safe failures is defined as follows:

$$\frac{\lambda_{\mathrm{SD}}}{\lambda_{\mathrm{S}}} = \frac{\lambda_{\mathrm{SD}}}{\lambda_{\mathrm{SD}} + \lambda_{\mathrm{SU}}} \tag{3.3}$$

The detected dangerous failure and the detected safe failure are restored during the diagnostic test period. The time to restoration (TTR) consists of the following times.

1) Time to the diagnostic test. The failures cannot be detected by the next test.
2) Time to repair. This includes the time spent to detect the failure by the test and any time required for repair.

The TTR average is denoted by MTTR (mean time to restoration). A typical value is 8 h [1]. The MTTR is also called mean time to repair (Section 6.3.2).

A proof test detects failures undetectable by the diagnostic test, and renews the safety-related system. The proof test is repeated at a proof-test interval such as six months and one year. Note that the diagnostic-test interval is usually far shorter than the proof-test interval.

3.7.3 Safe-failure Fraction

The dangerous failure is not dangerous when it can be detected. A detected dangerous failure can frequently be reduced to a safe failure. The safe-failure fraction (SSF) is defined by:

$$\mathrm{SSF} = \frac{\lambda_{\mathrm{S}} + \lambda_{\mathrm{DD}}}{\lambda_{\mathrm{S}} + \lambda_{\mathrm{D}}} = \frac{\lambda_{\mathrm{S}} + \lambda_{\mathrm{DD}}}{\lambda_{\mathrm{SD}} + \lambda_{\mathrm{SU}} + \lambda_{\mathrm{DD}} + \lambda_{\mathrm{DU}}} \tag{3.4}$$

3.7.4 System Behavior on Detection of Failure

The detection of a dangerous failure of the SIS by diagnostic-test or proof-test results in actions [11]:

1) A manual special action to achieve or maintain a safe state. This may, for example, include the safe shutdown of the process. If an operator takes the manual action such as opening a valve in response to an alarm, then the alarm shall be considered part of the SIS that is independent of the BPCS.
2) Suppose that the SIS can tolerate the single hardware failure. Operation of the process may be continued while the failed part is being repaired. If the repair is not completed within the mean time to restoration (MTTR) assumed in the probability quantification, then the manual action described in term "1" shall take place. If an operator notifies maintenance staff to repair a failed system in response to an alarm, then the alarm may be a part of the BPCS but is subject to appropriate proof testing and change management along with the rest of the SIS.
3) Suppose that the SIS in a demand mode cannot tolerate the single hardware failure. Operation of the process may be continued while the failed part is being repaired within the MTTR. During this time, the continuing

safety of the process is ensured by additional measures and constraints to provide a risk reduction at least equal to the one provided by the SIS before the failure. If the repair is not completed within the MTTR assumed in the probability quantification, then the manual action described in “1” takes place.

4) Suppose that the SIS in a continuous mode cannot tolerate the single hardware failure. Then, the manual action described in “1” may take place. The total time to detect the failure and to perform the action is less than the time for the hazardous event to occur.
5) Desired response (*e.g.*, alarms or automatic shutdown) under failures is clarified.
6) Manual means such as an emergency stop button are provided to actuate the SIS final elements unless otherwise directed by the safety-requirement specifications.
7) Bypass facilities with an alarming device are provided to allow online testing if required for operability, maintainability and testability.
8) A reset command, if justified, is provided to nullify the SIS that has been activated.

3.7.5 Hardware Fault Tolerance by SFF and SIL

A SIS is made up from a number of subsystems to implement the safety function. Typical subsystems are sensors, logic solvers, and final elements.

A type A subsystem is defined by [1]:

1) the failure modes of all components constituting the subsystem are well defined;
2) the behavior of the subsystem under failed conditions can be completely determined;
3) there is sufficient dependable field-failure data to support the failure rates for detected and undetected dangerous failures.

A subsystem becomes type B when either one of the three conditions above is not satisfied.

A hardware fault tolerance N means that $N + 1$ or more failures could cause a loss of safety function.

A hardware fault tolerance of 1 thus means that there are two redundant channels, and the failure of one channel does not lead to the SIS failure. The minimum hardware fault tolerance is introduced to cope with uncertainties of assumptions made in the design of SIS, and the uncertainty of failure rates.

Table 3.1 lists minimum hardware tolerance as a function of SFF and SIL for subsystems of type A, while Table 3.2 considers subsystems of type B.

Suppose that SFF is between 60% and 90% for a type-B subsystem of SIL2 SIS. The subsystem must have hardware fault tolerance equal to or larger than 1.

Table 3.3 shows the minimum hardware fault tolerance requirement of IEC 61511 for PE (programmable electronics) logic solvers in a different format from Tables 3.1 and 3.2 of IEC 61508. Table 3.4 is an equivalent representation in the IEC 61508 format. Note that IEC 61511 does not consider SIL 4. Moreover, IEC 61511 does not partition SFF at the 99% level. The hardware fault tolerance 3 is introduced into IEC 61511 to cope with SIL3 for SFF less than 60%. A higher fault tolerance is required for smaller SFF and higher SIL. This is closely related to the defense-in-depth level described next.

Table 3.1. Type-A subsystems: minimum hardware fault tolerance (IEC 61508)

SFF	Minimum hardware fault tolerance		
	0	1	2
SFF $<$ 60%	SIL1	SIL2	SIL3
60% $\leq$ SFF $<$ 90%	SIL2	SIL3	SIL4
90% $\leq$ SFF $<$ 99%	SIL3	SIL4	SIL4
99% $\leq$ SFF	SIL3	SIL4	SIL4

Table 3.2. Type-B subsystems: minimum hardware fault tolerance (IEC 61508)

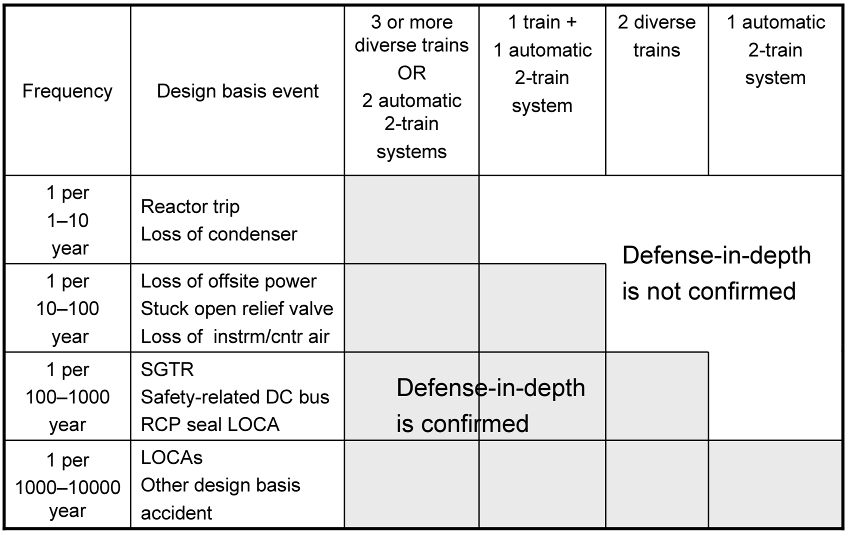
SFF	Minimum hardware fault tolerance		
	0	1	2
SFF $<$ 60%	N.A.	SIL1	SIL2
60% $\leq$ SFF $<$ 90%	SIL1	SIL2	SIL3
90% $\leq$ SFF $<$ 99%	SIL2	SIL3	SIL4
99% $\leq$ SFF	SIL3	SIL4	SIL4

Table 3.3. Minimum hardware fault tolerance requirement in IEC 61511

SIL	Minimum hardware fault tolerance		
	SFF $<$ 60%	60% $\leq$ SFF $<$ 90%	90% $\leq$ SFF
1	1	0	0
2	2	1	0
3	3	2	1
4	Special requirements apply (see IEC 61508)		

Table 3.4. Rearrangement of IEC 61511 fault tolerance to IEC 61508

SFF	Minimum hardware fault tolerance			
	0	1	2	3
SFF $<$ 60%	N.A.	SIL1	SIL2	SIL3
60% $\leq$ SFF $<$ 90%	SIL1	SIL2	SIL3	×
90% $\leq$ SFF	SIL2	SIL3	×	×



Frequency	Design basis event	3 or more diverse trains OR 2 automatic 2-train systems	1 train + 1 automatic 2-train system	2 diverse trains	1 automatic 2-train system
1 per 1–10 year	Reactor trip Loss of condenser	▨			
1 per 10–100 year	Loss of offsite power Stuck open relief valve Loss of instrm/cntr air	▨	▨		
1 per 100–1000 year	SGTR Safety-related DC bus RCP seal LOCA	▨	▨	▨	
1 per 1000–10000 year	LOCAs Other design basis accident	▨	▨	▨	▨

Defense-in-depth is not confirmed

Defense-in-depth is confirmed

Fig. 3.2. Defense-in-depth matrix [18]

3.8 Level of Defense-in-depth

Figure 3.2 considers the levels of defense-in-depth for initiating events with different annual frequencies. This matrix ensures that adequate defense-in-depth is available to mitigate the initiating events. Diverse and redundant trains and systems are introduced in evaluating the level of defense-in-depth.

Note the similarity between Figure 3.2 of NEI 00-04 [18] and the safety-layer matrix of Figure 2.5 of IEC 61511 [11]. From the point of view of the safety-layer matrix, the core damage is a consequence labeled as extensive. We saw in Figure 2.5 that SIL requirement could be relaxed as the protection layers increase.

Assume that SSCs have been categorized into HSS and LSS. The defense-in-depth requirements are examined in the following way:

1) For each initiating event, identify the HSS systems and trains that can provide an alternative success path *without* the current LSS SSCs.
2) For each initiating event, identify which region of Figure 3.2 the plant mitigation capability lies *without* credit for the current LSS SSCs.
3) If the result is in the region entitled “Defense-in-depth confirmed”, then the categorization into HSS and LSS has been confirmed.
4) If the result is in the region entitled “Defense-in-depth not confirmed”, then the LSS SSCs should be recategorized or additional HSS systems and trains should be added to the current design.

Similarly to the case of Figure 2.8, the low safety-significant SSCs still remains a candidate of LSS even if defense-in-depth is confirmed for all the relevant initiating events. The IDP (integrated decision-making panel) will provide a final decision.

Defense-in-depth should also be assessed for SSCs that play a role in preventing large, early releases.

Example: Defense-in-depth Level [18]

Suppose that a low-pressure core spray (LPCS) system pumps in a BWR are categorized as LSS prior to defense-in-depth assessment in Figure 2.8. The LPCS pumps provide coolant makeup to the reactor pressure vessel (RPV) at low pressure. This function is required either 1) in response to a large LOCA, or 2) in response to other transients and LOCAs where other coolant makeup systems are failed.

For mitigation of a large LOCA, the low-pressure coolant injection (LPCI) function of the residual-heat-removal (RHR) system can also support the coolant-makeup function. The LPCI function is automatic and consists of at least two trains. Thus, for this LOCA event, in the bottom row of Figure 3.2, the presence of LPCI as an automatic 2-train system confirms the LSS of LPCS.

In order to confirm low safety significance in high-frequency transient events, such as a reactor trip, either two automatic 2-train systems are required or 3 or more diverse trains must exist. It is known that these redundancy and diversity requirements are satisfied at the BWR.

In order to confirm low safety significance for mitigation of a stuck-open relief valve, one train plus one automatic 2-train system is required. The BWR provides these requirements.

Two diverse trains confirm low safety significance for mitigation of loss of one safety-related DC bus. The BWR satisfies this requirement. The LPCS pumps can thus remain a candidate of LSS.

3.9 Performance Evaluation after Categorization

3.9.1 Evaluation of Changes of Special Treatment

Consider that the categorization of SSCs has been made as described in Section 2.3. The unreliability of all RISC-3 SSCs is increased by a multiplier (such as 2 to 5) to reflect changes in special treatment. RISC-4 SSCs may have the same unreliability because there is no change in treatment. The multiplier is determined in such a way that the resultant CDF and LERF are consistent with the quantitative acceptance guidelines of Regulatory Guide 1.174 [18].

A monitoring and corrective-action program should be implemented to maintain the unreliability increase within the multiplier assumed. For example, assume the preimplementation number of failures of all RISC-3 MOVs in a three-year period was 5 failures and the multiplier used in the sensitivity was 3. Then, the assessment would monitor the postimplementation performance at 15 failures in three years. If the number of failures exceeded this value, then the appropriate changes to treatment would be made to return performance to an acceptable level.

It is noted that the recommended FV and RAW threshold values used in the screening (*e.g.,* Table 2.16) may be changed by the PRA team after the sensitivity study. If the risk evaluation shows that the changes in CDF and LERF as a result of changes in special treatment requirements are not within the acceptance guidelines of the Regulatory Guide 1.174, then a lower FV threshold value may be needed (*e.g.*, 0.0025) for a re-evaluation of SSCs risk ranking. This may result in recategorizing some of the candidate low safety-significant SSCs into safety-significant SSCs.

3.9.2 SIS Quantification

Suppose that the SIL has been determined for a SIS in a way described in Section 2.2. The problem is now to evaluate whether a SIS specification and design satisfy the performance demanded by SIL. Suppose that the configurations shown in Figure 3.3 are the candidates obtained after the evaluation of hardware fault tolerance described in Section 3.7.5.

Major Assumptions and Symbols

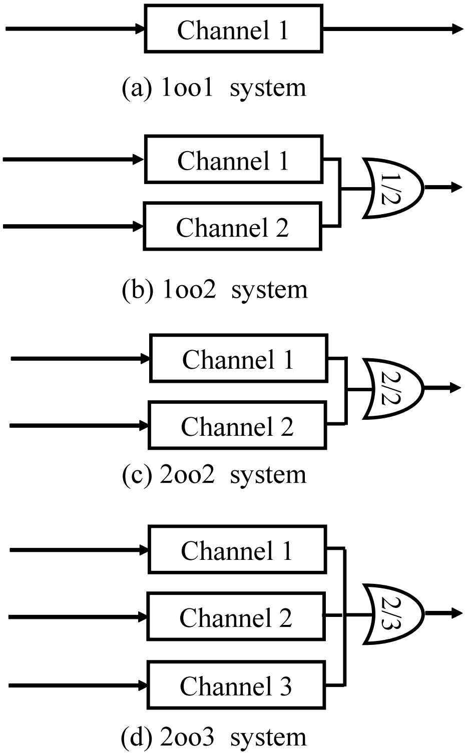
1) Failure rates are small and constant.
2) An automated online diagnostic test and a proof test are carried out.
3) Both types of tests have the same MTTR.
4) The variance of TTRs is sufficiently small and each TTR is treated as being equal to MTTR.
5) The diagnostic test is performed almost continuously, and hence the test interval is almost zero as compared with MTTR.
6) The detected dangerous-failure rate is denoted by λ_{DD}, while the undetected dangerous-failure rate is by λ_{DU}.
7) The following Taylor-series approximation is used for small $(\lambda_{\mathrm{D}} + \lambda_{\mathrm{S}})\tau$, where $\lambda_{\mathrm{D}} + \lambda_{\mathrm{S}}$ is failure rate and τ is time:

$$\frac{\lambda}{\lambda_{\mathrm{D}} + \lambda_{\mathrm{S}}} \Big[1 - \exp[-(\lambda_{\mathrm{D}} + \lambda_{\mathrm{S}})\tau]\Big] = \lambda\tau \tag{3.5}$$

8) The proof-test interval is denoted by T. All failures can be detected and restored by the proof test.
9) Operation of the process is continued while the failed part is being repaired.

Demand-failure Probability: Independent Failures

A profile of demand-failure probability for a demand at time t is shown in Figure 3.4. Shift the time axis so that the most recent proof test n can start at time zero.



(a) 1oo1 system

(b) 1oo2 system

(c) 2oo2 system

(d) 2oo3 system

Fig. 3.3. SIS m-out-of-n (moon) structures

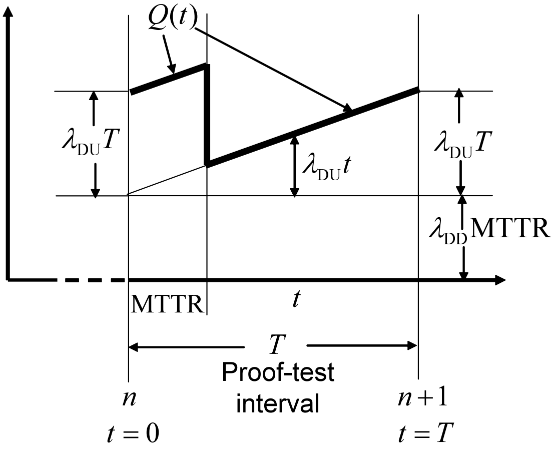


Fig. 3.4. Time profile of demand-failure probability of a single channel

Consider first the case where the time t of demand is less than the MTTR. Under a rare-event assumption, the demand-failure probability at this time is the sum of the following elements.

1) λ_{DD}MTTR: This is a contribution of dangerous failures detected by online diagnostic tests. Detected dangerous failures that occurred in past time interval $[t - \mathrm{MTTR}, t]$ have not yet been restored at the demand time t. The probability of the detected dangerous failure in this interval is λ_{DD}MTTR from Equation 3.5.
2) $\lambda_{\mathrm{DU}}t$: This is a contribution of undetected dangerous failures in interval $[0, t]$ after the proof test at time zero. Again, the approximation of Equation 3.5 is used.
3) $\lambda_{\mathrm{DU}}T$: This is a contribution of undetected dangerous failures in the previous proof-test interval $[-T, 0]$. These failures have not yet been restored at demand time t less than MTTR. This contribution only exists in this period of demand time.

Consider next the case where demand time t is equal to or larger than MTTR. The demand-failure probability at this time is the sum of the following elements.

1) λ_{DD}MTTR: This is a contribution of detected dangerous failures by online diagnostic tests. The detected dangerous failures that occurred in time interval $[t - \mathrm{MTTR}, t]$ have not yet been restored at the demand time t. The probability of the detected dangerous failure in this interval is λ_{DD}MTTR.
2) $\lambda_{\mathrm{DU}}t$: This is a contribution of undetected dangerous failures in interval $[0, t]$ after the proof test at time zero.

A 1-out-of-1 (1oo1) structure is the simplest to be quantified. The demand-failure probability $Q_{1\mathrm{oo}1}$ is defined as a failure probability $Q(t)$ on demand averaged over time interval T:

$$Q_{1\mathrm{oo}1} = \frac{1}{T}\int_0^T Q(t)\mathrm{d}t \tag{3.6}$$

This integral can easily be calculated from profile $Q(t)$ of Figure 3.4, yielding:

$$Q_{1\mathrm{oo}1} = \lambda_{\mathrm{DU}}\left(\frac{T}{2} + \mathrm{MTTR}\right) + \lambda_{\mathrm{DD}}\mathrm{MTTR} \tag{3.7}$$

This equation coincides with the one in Appendix B to IEC 61508-7 [1]. Alternatively, the maximum value of $Q(t)$ might be used for the demand-failure probability.

Consider the case of $\lambda_{\mathrm{DD}} = \mathrm{MTTR} = 0$, *i.e.* failures can only be detected at the proof test, and repaired instantaneously there. The demand failure probability equals the result in reference [35]:

$$Q_{1\mathrm{oo}1} = \frac{\lambda_{\mathrm{DU}}T}{2} \tag{3.8}$$

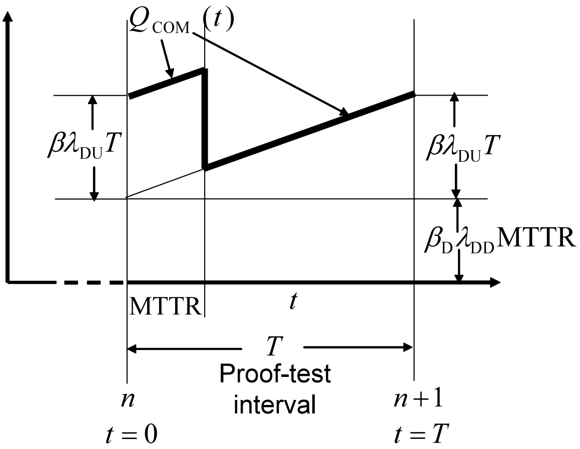

$Q_{\mathrm{COM}}(t)$
$\beta\lambda_{\mathrm{DU}}T$
$\beta\lambda_{\mathrm{DU}}T$
$\beta_{\mathrm{D}}\lambda_{\mathrm{DD}}\mathrm{MTTR}$
MTTR
t
T
Proof-test interval
n
$t=0$
$n+1$
$t=T$

Fig. 3.5. Time profile of demand-failure probability due to common-cause failures

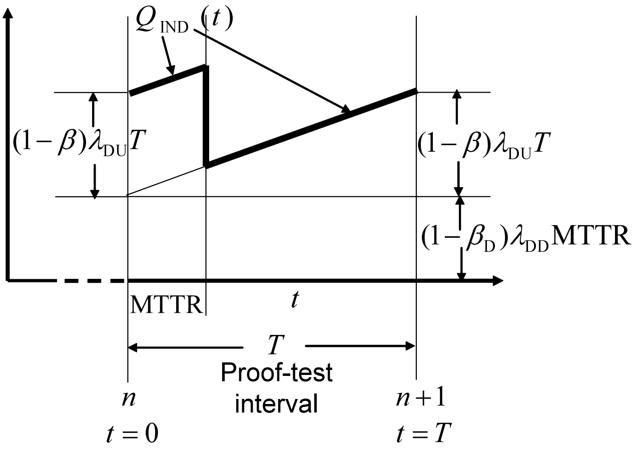

$Q_{\mathrm{IND}}(t)$
$(1-\beta)\lambda_{\mathrm{DU}}T$
$(1-\beta)\lambda_{\mathrm{DU}}T$
$(1-\beta_{\mathrm{D}})\lambda_{\mathrm{DD}}\mathrm{MTTR}$
MTTR
t
T
Proof-test interval
n
$t=0$
$n+1$
$t=T$

Fig. 3.6. Time profile of demand-failure probability due to independent failures

Demand-failure Probability: CCF

A 1-out-of-2 (1oo2) structure requires a common-cause failure contribution. A so-called beta-factor model (Section 8.2.5) assumes independent failures and common-cause failures in the following way for structures containing $m \geq 1$ component.

1) For the undetected dangerous failures, two types of failures occur:
   1-1) The structure behaves like a single-component system with failure rate $\beta\lambda_{\mathrm{DU}}$. This contribution is shown in Figure 3.5 by the portion with the failure rate $\beta\lambda_{\mathrm{DU}}$.

1-2) The structure behaves like an m-component system where each component fails independently with failure rate $(1-\beta)\lambda_{\mathrm{DU}}$. This contribution is shown in Figure 3.6 by the portion with the failure rate $(1-\beta)\lambda_{\mathrm{DU}}$.

2) For the detected dangerous failures, failure types are similar to the undetected failure case except for a different β_{D} replacing β:

2-1) The structure behaves like a single-component system with failure rate $\beta_{\mathrm{D}}\lambda_{\mathrm{DD}}$. This contribution is shown in Figure 3.5 by the portion with failure rate $\beta_{\mathrm{D}}\lambda_{\mathrm{DD}}$.

2-2) The structure behaves like an m-component system where each component fails independently with failure rate $(1-\beta_{\mathrm{D}})\lambda_{\mathrm{DD}}$. This contribution is shown in Figure 3.6 by the portion with the failure rate $(1-\beta_{\mathrm{D}})\lambda_{\mathrm{DD}}$.

1oo1 Structure

The simplest case is the 1oo1 structure. The average demand probability is:

$$Q_{1\mathrm{oo}1} = \frac{1}{T}\int_0^T Q_{\mathrm{IND}}(t) + Q_{\mathrm{COM}}(t)\mathrm{d}t \tag{3.9}$$

Profiles of $Q_{\mathrm{COM}}(t)$ and $Q_{\mathrm{IND}}(t)$ are shown in Figures 3.5 and 3.6, respectively. This can be calculated analytically, yielding the same result as before:

$$\begin{aligned} Q_{1\mathrm{oo}1} &= (1-\beta)\lambda_{\mathrm{DU}}\Big(\frac{T}{2} + \mathrm{MTTR}\Big) + (1-\beta_{\mathrm{D}})\lambda_{\mathrm{DD}}\mathrm{MTTR} \\ &+\ \beta\lambda_{\mathrm{DU}}\Big(\frac{T}{2} + \mathrm{MTTR}\Big) + \beta_{\mathrm{D}}\lambda_{\mathrm{DD}}\mathrm{MTTR} && (3.10) \\ &= \lambda_{\mathrm{DU}}\Big(\frac{T}{2} + \mathrm{MTTR}\Big) + \lambda_{\mathrm{DD}}\mathrm{MTTR} && (3.11) \end{aligned}$$

1oo2 Structure

Consider next the average demand-failure probability $Q_{1\mathrm{oo}2}$ for the 1oo2 structure. This consists of the elements (see also Table 8.3):

1) Independent failure contribution: Both channels must fail for the structure to fail. The contribution becomes the average of $Q^2_{\mathrm{IND}}(t)$.
2) Common-cause failure contribution: This is the average of $Q_{\mathrm{COM}}(t)$.

The following equation can easily be derived by adding these contributions:

$$\begin{aligned} &Q_{1\mathrm{oo}2} = Q_{1\mathrm{oo}2,\mathrm{IND}} + Q_{1\mathrm{oo}2,\mathrm{COM}} && (3.12) \\ &Q_{1\mathrm{oo}2,\mathrm{IND}} \equiv \Big[\frac{T}{2}(1-\beta)\lambda_{\mathrm{DU}} + \{(1-\beta)\lambda_{\mathrm{DU}} + (1-\beta_{\mathrm{D}})\lambda_{\mathrm{DD}}\}\mathrm{MTTR}\Big]^2 \\ &+ \frac{T^2}{12}(1-\beta)^2\lambda^2_{\mathrm{DU}} && (3.13) \\ &Q_{1\mathrm{oo}2,\mathrm{COM}} \equiv \beta\lambda_{\mathrm{DU}}\Big[\frac{T}{2} + \mathrm{MTTR}\Big] + \beta_{\mathrm{D}}\lambda_{\mathrm{DD}}\mathrm{MTTR} && (3.14) \end{aligned}$$

Consider a special case without the common-cause contribution and without the undetected dangerous failure, *i.e.* $\beta = \beta_{\mathrm{D}} = \lambda_{\mathrm{DU}} = 0$. The demand-failure probability of a 1oo2 structure becomes:

$$Q_{1\mathrm{oo}2} = (\lambda_{\mathrm{DD}}\mathrm{MTTR})^2 \tag{3.15}$$

This is correct since each channel is being failed dangerous at time t with probability $\lambda_{\mathrm{DD}}\mathrm{MTTR}$. The formula in Appendix B to IEC 61508-6 yields, in this special case, the demand-failure probability two times larger than the correct value:

$$Q_{1\mathrm{oo}2} = 2(\lambda_{\mathrm{DD}}\mathrm{MTTR})^2 \tag{3.16}$$

The difference between the independent contribution of Equation 3.13 and that of IEC 61508-7 seems small, except for DCs close to unity.

Consider the case of $\lambda_{\mathrm{DD}} = \mathrm{MTTR} = \beta = \beta_{\mathrm{D}} = 0$, *i.e.* failures can only be detected at the proof test, and repaired instantaneously there. There is no common cause. The demand failure probability equals the result in reference [35]:

$$Q_{1\mathrm{oo}1} = \frac{\lambda_{\mathrm{DU}}^2 T^2}{3} \neq \left(\frac{\lambda_{\mathrm{DU}} T}{2}\right)^2 \tag{3.17}$$

2oo3 Structure

The 2-out-of-3 structure (2oo3) has an independent failure contribution three times as large as the 1oo2. All the components fail by the common causes for the beta-factor model and the common-cause contribution is the same as the 1oo2:

$$Q_{2\mathrm{oo}3} = Q_{2\mathrm{oo}3,\mathrm{IND}} + Q_{2\mathrm{oo}3,\mathrm{COM}} \tag{3.18}$$

$$Q_{2\mathrm{oo}3,\mathrm{IND}} = 3Q_{1\mathrm{oo}2,\mathrm{IND}} \tag{3.19}$$

$$Q_{2\mathrm{oo}3,\mathrm{COM}} = Q_{1\mathrm{oo}2,\mathrm{COM}} \tag{3.20}$$

The independent contribution differs from that in Appendix B to IEC 61508-6.

2oo2 Structure

The 2-out-of-2 structure (2oo2) has an independent failure contribution twice that of the independent contribution of the 1oo1 structure. The common-cause contribution is the same as that of 2oo2 (Table 8.3):

$$Q_{2\mathrm{oo}2} = Q_{2\mathrm{oo}2,\mathrm{IND}} + Q_{2\mathrm{oo}2,\mathrm{COM}} \tag{3.21}$$

$$\begin{aligned} Q_{2\mathrm{oo}2,\mathrm{IND}} &= 2(1-\beta)\lambda_{\mathrm{DU}}\left(\frac{T}{2} + \mathrm{MTTR}\right) + 2(1-\beta_{\mathrm{D}})\lambda_{\mathrm{DD}}\mathrm{MTTR} \\ &= 2Q_{1\mathrm{oo}1,\mathrm{IND}} \end{aligned} \tag{3.22}$$

$$Q_{2\mathrm{oo}2,\mathrm{COM}} = \beta\lambda_{\mathrm{DU}}\left(\frac{T}{2} + \mathrm{MTTR}\right) + \beta_{\mathrm{D}}\lambda_{\mathrm{DD}}\mathrm{MTTR} \tag{3.23}$$

Appendix B to IEC 61508-6 does not consider the common-cause failure contribution for the 2oo2 structure.

Example: Redundant Sensors and Logic Solvers
Consider the structure shown in Figure 3.7 [1]. Three sensors are used. Two logic units are available. Each unit is a 2/3 voting logic. The output of the logic unit actuates a vent valve and a shutdown valve. Each valve is actuated by a 1/2 voting logic *belonging to* the valve. Both valves must be activated for successful operation of the SIL2 functional safety system. A perfect power source is assumed.

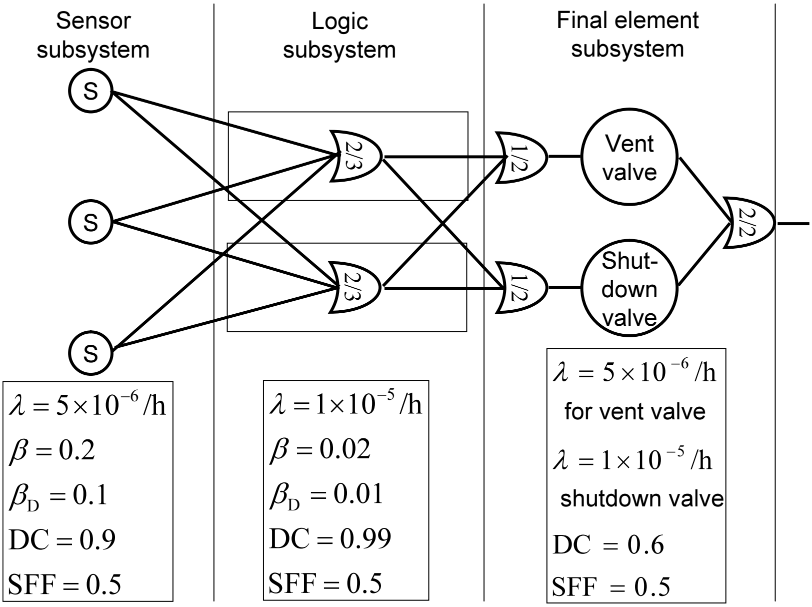


Fig. 3.7. Example structure of SIL2 safety-function system on demand mode

The sensor subsystem forms two 2oo3 structures. The logic subsystem is a 1oo2 structure. The two valves form a 2oo2 structure *without* common-cause failures. The demand-failure probability of this 2oo2 structure is a simple sum of the two demand-failure probabilities of the valves.

The proof-test interval T is one year (365 × 24 h) and the MTTR is 8 h. The safe-failure fraction is 0.5. The demand-failure probability equations just described yield the following results:

$$Q_{2oo3} = 2.2 \times 10^{-4} \tag{3.24}$$

$$Q_{1oo2} = 4.8 \times 10^{-6} \tag{3.25}$$

$$Q_{2oo2} = 4.4 \times 10^{-3} + 8.8 \times 10^{-3} = 1.3 \times 10^{-2} \tag{3.26}$$

The system-demand-failure probability is the sum of these subsystem probabilities:

$$Q_{\mathrm{S}} = (2.2 \times 10^{-4}) + (4.8 \times 10^{-6}) + (1.3 \times 10^{-2}) = 1.3 \times 10^{-2} \tag{3.27}$$

This is larger than 10^{-2}. The system does not satisfy the SIL2 requirement.

The proof-test interval is shortened to 6 months to improve the system. The subsystem- and system-demand probabilities become:

$$Q_{2\mathrm{oo}3} = 1.1 \times 10^{-4} \tag{3.28}$$

$$Q_{1\mathrm{oo}2} = 2.6 \times 10^{-6} \tag{3.29}$$

$$Q_{2\mathrm{oo}2} = (2.2 \times 10^{-3}) + (4.4 \times 10^{-3}) = 6.6 \times 10^{-3} \tag{3.30}$$

$$Q_{\mathrm{S}} = 6.7 \times 10^{-3} \tag{3.31}$$

This satisfies the SIL2 requirements.

A continuous demand mode can be handled similarly. For the 1oo2 structure, for instance, the system fails due to a channel 1 failure when channel 2 is already failed and undetected.

3.10 Concluding Remarks

Dependent failure countermeasures, sufficient safety margins, human-factors reviews, early detection and treatment, and defense-in-depth are *nonlinear* qualitative defenses necessary to ensure the performance required for each categorization. The performance is quantitatively evaluated by PRA types of methodologies.

4

Hazard Identification and Risk Reduction

4.1 Introduction

Risks cannot exist without hazards. A reasonably complete identification of hazards should be made. Initiating events as accident initiators are found, and risk-reduction measures are established. This chapter describes risk-reduction approaches based on hazard identification, hazard elimination, prevention and mitigation of initiating events and accident mitigation. Safety systems described in Chapters 2 and 3 are types of products from the risk-reduction framework given in this chapter.

4.2 Hazard, Source and Risk

The r2p2 reference [21] of HSE defines a hazard as the potential for harm arising from an intrinsic property or disposition of something to cause detriment. The reference defines the risk as the chance that someone or something that is valued will be adversely affected in a stipulated way by the hazard. It is thus required that hazards are identified, the risks they give rise to are assessed and appropriate control measures are introduced to address the risks.

The r2p2 reference further describes that it is often possible to regard any hazard as having more remote causes that themselves represent the "true hazard". For example, when considering the risk of explosion from the storage of a flammable substance, it can be argued that it is not the storage *per se* that is the hazard but the intrinsic properties of the substance stored. Nevertheless, it makes sense to consider the storage as the basis for the estimation of risk since this approach will be the most productive in identifying the practical control measures necessary for managing the risks, such as not storing the substance in the first place, using less of it or a safer substance, or if there is no alternative to storing the substance, using better means of storing it.

Table 4.1. Source and harm of hazard

	Hazard	Source	Harm
1	Motion	Vehicle, Turntable, Missile	Collision
		Vibration stand, Pump	Being caught
2	Height	Suspended object	Fall, Collision
3	Stress	Spring mechanism, Load	Stab, Collision
4	Pressure	Pressure tank, High, Low, Sudden change	Destruction, Fatality
5	Temperature	Furnace, Cold room, High, Low, Sudden change	Ignition, Fatality
6	Moisture	Bath, Wet, Dry, Sudden change	Electric shock, Mold
7	Electricity	Battery, Capacitor, Static electricity	Electric shock
		Ionization, Generator	Noise
8	Magnetism	EM field, Magnet	Semiconductor failure
9	Explosive	Propulsion, Detonator, Powder	Explosion, Fire
10	Flammable	Fuel, Ignitable	Fire
11	Corrosive	Acid, Alkali	Leakage
12	Reactive	Electrolysis	Alien substance
13	Heat	Heater, Infrared	Fire
14	Light	Laser	Eye disease
15	Sound	Noise	Hearing problem
16	Radiation	X-ray, UV	Skin cancer
17	Pathogenic	Food, Medical equipment	Food poisoning
18	Carcinogen	Raw material, Additive,	Cancer
		Gas, Aerosol	Cancer
19	Suffocation	Nitrogen, Carbon dioxide	Fatality
20	Poison	Poison, Off-gas, Effluent, Waste	Disease
21	Contaminant	Oil, Radioactivity	Contamination
22	Sharp	Knife, Edge	Injury
23	Particle	Pollen, Powder, Coal dust	Pneumoconiosis
24	Human	Error, Sabotage	System failure

4.2.1 Classification of Hazards

Table 4.1 lists hazards, hazard sources, and harms resulting from the hazards. The hazards are closely related to harmful energy. For instance, a vehicle has a kinetic energy and causes a traffic accident. An object suspended at a height has a potential energy and causes harms by falls. ISO 14121 and 12100 classify hazards by origins and harms.

4.2.2 Typical Measures for Hazards

Table 4.2 shows typical measures to deal with hazards. These were originally proposed by MORT (management oversight and risk tree) [39]. The devitalization is the first measure. This is similar to the inherent safety to remove hazards. Weak hazards can accumulate. Thus, the second measure is the prevention of buildup by detection, control, and relief mechanism. Measures 3 to

8 are cases after the activation of hazards. A ground wire is used to separate the electrical hazard from humans and equipment. The containment of the nuclear power plant is an example of a guard on origin. Measures 6 and 7 can be interpreted similarly. Increasing resistance against hazards is measure 8. Measure 9 includes treatment and recovery.

Table 4.2. Typical risk-reduction measures

	Barrier	Example
1	Devitalize hazard	Low-voltage device, Safer solvent, Downsizing
2	Prevent buildup	Gas detector, Control, Relief valve
3	Mitigation	Damper, Seat belt, Air bag
4	Separation	Ground wire, Entry control
5	Guard on origin	Containment, Insulation, Soundproof
6	Guard in between	Fire door
7	Guard on destination	Helmet, Oxygen inhaler
8	Increase resistance	Selection, Adaptation
9	Treatment and recovery	Emergency shower, First aid

4.3 Hazard Association

There is no countermeasure for a hazard overlooked. Hazards must be recalled. The recollection is performed via guide words, abnormal-event vocabularies, and function names susceptible to failure.

4.3.1 HAZOP

HAZOP (hazard and operability study) [40] considers deviations of attributes of objects. The attributes include physical quantities such as flow rate, temperature, pressure, concentration, strength, length, thickness, electric current, voltage, data flow rate, response time, and occurrence interval. Relations such as 1-to-1 and 1-to-many are also considered as attributes. A leak of a secret is a change from 1-to-1 to 1-to-many.

HAZOP uses the guide words to recall abnormal events originated from hazards. These guide words are listed in Table 4.3. Some guide words are illustrated in Figure 4.1. The original intention of the design of equipment or process or activity is depicted by a shaded disk. A blank area indicates an unnecessary harmful thing. Thus, “as well as” means a simultaneous existence of original intention and an extra thing. The word “part of” means lack of original intention, while “other than” the lack plus the extra thing. These three guide words express qualitative deviations. Guide word “no” represents qualitative or quantitative deviations. Other words are concerned with quantitative deviations.

Table 4.3. Guide words for association of abnormal events

No	Word	Meaning	Attribute	Value
1	No	Complete loss of intention None	Flow Signal Data rate Task	None None Zero Lack
2	More	Increase, Too much	Flow	Increase
3	Less	Decrease, Too little	Flow	Decrease
4	Reverse	Opposite	Flow	Backward
5	Early	Too early	Timing	Too early
6	Late	Too late	Timing	Too late
7	Before	Incorrect order	Step	One step early
8	After	Incorrect order	Step	One step late
9	As well as	Superfluity	Task	Extraneous act
10	Part of	Partial lack of intention	Flow	Lack of components
11	Other than	Lack and superfluity	Data	Error

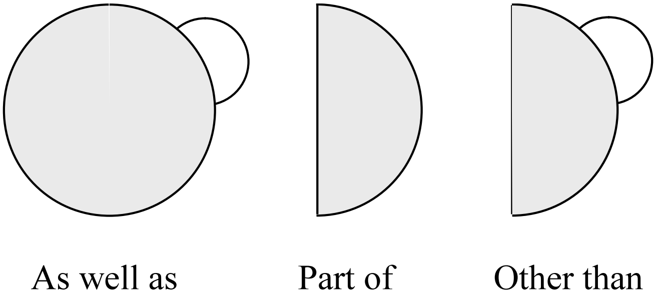


Fig. 4.1. HAZOP guide words "as well as", "part of" and "other than"

Consider the pressure-tank system of Figure 2.2. The word "High" guides us to a deviation of high pressure. In HAZOP, the causes of a deviation are also searched for. The current case leads to the timer contact stuck-closed failure as a cause of the high pressure. The HAZOP thus finds an initiating event.

4.3.2 Abnormal-event Vocabularies

Without a vocabulary we can not recall the hazard. Table 4.4 lists vocabularies representing abnormal events.

The deformation is a change of shape without a change of mass. Abnormal events such as drip may be observed on a surface. Separation is a division and similar to the guide word "part of". An impurity classified as "alien" resembles the guide word "as well as" and "other than".

Table 4.4. Vocabularies expressing abnormal events

Type	Example of phrases
1) Deformation	Deformation, Distortion, Strain, Buckling, Contortion, Expansion, Reduction, Cave-in
2) Surface	Discoloration, Drip
3) Separation	Damage, Destruction, Broken, Fracture, Collapse, Rupture, Lack, Drop-out, Flake-off, Wearout, Crack, Cut, Damage, Pitting corrosion
4) Alien	Adhesion, Precipitation, Pollution, Separation, Electrification, Jam, Impurity, Bug, Rust, Disturbance, Noise, Vibration
5) Leakage	Leak, Outflow, Discharge, Exudation, Short circuit, Radiation, Dispersion, Movement, Overflow, Derailment
6) Blockage	Blocking, Obstruction
7) Fixation	Ricketiness, Loosening
8) Connection	Cut, Interruption
9) Deterioration	Aging, Fatigue, Brittleness, Softening, Stiffening, Weakening
10) Performance	Error, Disorder, Variation, Fluctuation, Incident, Impossiblility, Uselessness, Impurity
11) Concentration	Condensation, Dilution
12) Movement	Vibration, Rotation, Collapse, Fall, Sinking, Crash, Runaway, Rising, Open, Close, Loosen, Decelerate, Activate, Ascend, Descend, Up-Down, Return, Instability, Release
13) Stoppage	Collision, Stranded, Stuck, Stoppage, Stagnation, Adherence, Friction
14) Existence	Creation, Existence
15) Nonexistence	Extinction, None, Blackout
16) Phase	Vaporization, Evaporation, Melting, Dissolution, Condensation, Freezing, Boiling, Phase transition
17) Physics	Heating, Cooling, Heat retention, Magnetization, Heat generation
18) Chemistry	Oxidization, Ignition, Combustion, Fire, Explosion, Extinction, Heat generation, Corrosion, Criticality
19) Quantity	Increase, Decrease, Decline, Ascent, Overload, Excess,
20) Location	High, Low
21) Time	Early, Late
22) Function	Premature start, Premature activation, Premature stoppage, Change error, Operation error, Trouble
23) Communication	Communication error, Instruction error
24) Perception	Oblivion, Mistake, Dependence, Overconfidence, Looking away, Impatience, Neglection
25) Action	Ignorance, Inaction, Abandonment, Approach, Removal, Addition, Connection, Contact, Slide, Topple, Vibration, Slip, Operation error, Misuse, Carelessness, Conceit, Confusion, Inexperience, Unreasonableness, Doze
26) Harm	Fatality, Injury, Fracture, Losing sight, Burn, Suffocation, Electric shock, Disease infection, Exposure, Aftereffect
27) Nature	Earthquakes, Typhoon, Flood, Landslide

Leakage and blockage are typical causes of accidents and human fatalities. Many failures are related to type of “fixation”, “connection”, and “deterioration”. These vocabularies can be used to identify hazards.

Table 4.5. Function associated with device name

Device name	Function verb	Device name	Function verb
Function related to movability			
Rotor	Move, Rotate	Mover	Move, Slide
Vibrator	Shake, Swing	Switch	Open, Close
Transmission	Transmit		
Function related to immovability			
Fixer	Suspend, Keep	Supporter	Support
Connector	Connect	Container	Contain
Canister	Seal, Store	Conduit	Restrict
Paint spray	Insulate	Guard	Keep
Reflector	Copy	Sealer	Seal
Function related to change			
Reactor	Change	Mixer	Mix
Illuminator	Illuminate	Heat exchanger	Exchange
Combustor	Burn	Heater	Heat
Cooler	Cool	Absorber	Absorb
Separator	Select		
Others			
Battery	Flow	Control	Move
Actuator	Drive	Brake	Stop
Bearing	Slide, Support	Pump	Flow
Sensor	Measure	Damper	Mitigate
Circuit	Flow	Lubricator	Slide
Stopper	Stop		

4.3.3 Function Names

When we know a function name, we can recall failures of the function. Function names are listed in Table 4.5. There are at least four types of function names.

1) Functions related to movability.
2) Functions related to immovability.
3) Functions related to change.
4) Others.

Functions typically have two failure modes: inactive failure and premature activation.

Table 4.6. Severity rating [41]

Rating	Definition
10	Failure could injure the customer or an employee
9	Failure would create noncompliance with federal regulations
8	Failure renders the unit inoperable or unfit for use
7	Failure causes a high degree of customer dissatisfaction
6	Failure results in a subsystem or partial malfunction of the product
5	Failure creates enough of a performance loss to cause the customer to complain
4	Failure can be overcome with modifications to the customer's process or product, but there is minor performance loss
3	Failure would create a minor nuisance to the customer, but the customer can overcome it in the process or product without performance loss
2	Failure may not be readily apparent to the customer, but would have minor effects on the customer's process or product
1	Failure would not be noticeable to the customer and would not affect the customer's process or product

Table 4.7. Frequency rating [41]

Rating	Continuous	Discrete
10	>1 per day	>3 in 10
9	≃1 per 3 to 4 days	≃3 in 10
8	≃1 per week	≃5 in 100
7	≃1 per month	≃1 in 100
6	≃1 per 3 months	≃3 in 1000
5	≃1 per 6 months	≃1 in 10 000
4	≃1 per year	≃6 in 100 000
3	≃1 per 3 years	≃6 in 10^7
2	≃1 per 5 years	≃2 in 10^9
1	<1 per 5 years	<2 in 10^9

4.4 FMEA

The FMEA (failure mode and effects analysis) [41] is a first step to understanding the plant from a failure point of view. A tabular form is used. The plant is examined in component-by-component bases. For a given component, a failure mode and its effects are listed. The causes of the failure mode are also listed.

Each pair of failure mode and effect are scored from three viewpoints: 1) severity, 2) frequency, and 3) detectability. These scoring schemes are shown

Table 4.8. Detection rating [41]

Rating	Definition
10	The product is not inspected or the defect caused by failure is not detectable
9	Product is sampled, inspected, and released based on acceptable quality level sampling plans
8	Product is accepted based on no defectives in a sample
7	Product is 100% manually inspected in the process
6	Product is 100% manually inspected using go/no-go or other mistake-proofing gauges
5	Some statistical process control (SPC) is used in process and product is finally inspected offline
4	SPC is used and there is immediate reaction to out-of-control conditions
3	An effective SPC program is in place
2	All product is 100% automatically inspected
1	The defect is obvious or there is a 100% inspection with regular calibration and preventive maintenance of the inspection equipment

Table 4.9. Fishing problem FMEA

Item	Failure mode	Effect	Severity	Cause	Frequency	Detection Method	Detectability	RPN	Action (1)	Responsibility and target completioin date	Action taken	Revised severity	Revised frequency	Revised frequency	Revised RPN
Hook	Wear	Not hooked	8	Aging	10	None	10	800	Palpation	K、4/1	(1)	8	10	2	160
Hook Line	Scratch	Snap	8	Aging	10	None	10	800	Palpation	K、4/1	(1)	8	10	2	160
Hook	Small	Deformation	8	Hit emphasis	8	None	10	640	Adaptation to fish	K、4/1	(1)	8	4	10	320
Hook Line	Thin	Snap	8	Hit emphasis	8	None	10	640	Adaptation to fish	K、4/1	(1)	8	4	10	320
Hook	Large	Poor hit	6	Whopper emphasis	8	None	10	480	Adaptation to fish	K、4/1	(1)	6	4	10	240
Hook Line	Thick	Poor hit	6	Whopper emphasis	8	None	10	480	Adaptation to fish	K、4/1	(1)	6	4	10	240
Hook	Twist	Poor hit	6	Aging	10	None	4	240	Replace hook	K、4/1	(1)	6	5	4	120
Guides	Loose	Tangled line	4	Alien Salt	6	None	10	240	Audible inspection	K、4/1	(1)	4	6	5	120
Mini Sinker	Position shift	Poor hit	6	Aging	6	None	4	144	Visual inspection	K、4/1	(1)	6	3	4	72
Mini Sinker	Off	No signal from float	6	Aging	4	None	4	96	Visual inspection	K、4/1	(1)	6	4	2	48
Main Line	Twist	Tangled line	4	Aging	6	None	4	96	Replace line	K、4/1	(1)	4	3	4	48
Float	Broken	No fishing	10	Aging	4	None	2	80	Standby float	K、4/1	(1)	5	4	2	40
Rod	Broken	No fishing	10	Scratch	2	None	2	40	Standby rod	K、4/1	(1)	5	2	2	20
Reel	Broken	No fishing	10	Aging	1	None	2	20	Standby reel	K、4/1	(1)	5	1	2	10

in Tables 4.6, 4.7, and 4.8. The product of these three scores is called a RPN (risk priority number). The FMEA can apply to product, production process, and service.

Consider, for instance, the pressure-tank system in Figure 2.2. Consider as a component the timer contact. A failure mode is “stuck closed”. An effect is the pump overrun. The stuck-closed failure is identified as a cause of an initiating event, “pump overrun”. Another cause is the timer failure.

A sample FMEA table is shown in Table 4.9 for a beginner of float fishing. The severity, frequency, and detectability ratings are modified from those stated already. The failure modes are arranged in a descending order of RPNs. We observe that wearout hook and scratched hook line are the most serious failure modes. As shown by the revised RPN in the last column, the most dominant failure modes after revision are too small a hook and too thin a hook line.

4.5 Master Logic Diagram

A master logic diagram (MLD) uses the fault tree to search for accident initiators. An example of an MLD for a nuclear power plant is shown in Figure 4.2 [42]. Refer to [43] for chemical-plant MLDs. The top event on the first level in the diagram represents the undesired event for which the PRA is being conducted, that is, an excessive offsite release of radionuclides. This top event is successively refined by levels. The OR gate on level 1 answers the question, “How can a release to the environment occur?” yielding “Release of core material” and “Release of noncore material”. The AND gate on level 2 shows that a release of radioactive material requires simultaneous core-damage and containment failure. The OR gate on level 3 below “Core damage” answers the question, “How can core damage occur?” After several more levels of “how can” questions, the diagram arrives at a set of potential initiating events, which are equipment failures or human errors.

A total of 50 internal initiating events were eventually found by MLD for the scenario partly shown in Figure 4.2. These events are further grouped according to mitigating system requirements. The NUREG-1150 PRA was able to reduce the number of initiating-event categories by combining several that had the same plant response. For example, the loss of steam inside and outside the containment was collapsed into loss of steam, resulting in a reduction of the initiating-event categories.

4.6 Risk-reduction Measures

4.6.1 Definition of Initiating Events

The definition of an initiating event for the nuclear power plant in the ASME PRA standard [5] can be generalized to other plants as follows. An initiating

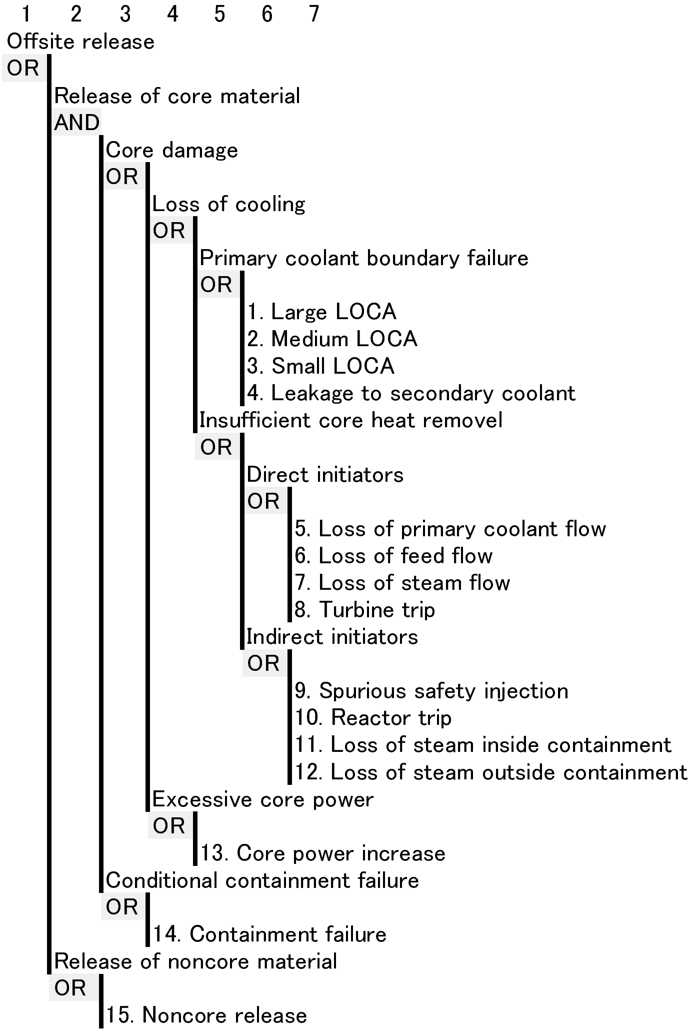


Fig. 4.2. A schematic of a master logic diagram for searching for initiating events

event is any event either internal or external to the plant that perturbs the normal operation of the plant, thereby initiating an abnormal event such as transient or loss of coolant within the plant. Initiating events trigger sequences of events that challenge plant control and safety systems whose failure could lead to an accident potentially followed by a large release of hazardous materials. For the nuclear power plant the accident is a core damage, and the hazardous-material release is an early large release of radioactivity.

4.6.2 Four Major Steps

We now give four major steps of risk reduction as Figure 4.3: 1) inherently safer design, 2) initiating-event prevention, 3) initiating-event mitigation, and 4) accident mitigation.

4.6.3 Inherently Safer Design

The inherently safer design is based on elimination of hazards. Accidents can not occur when hazards are removed by the inherently safer design. An overhead crossing is an elimination of an intersection, a typical hazard in transport. Not storing the explosive substance in the tank is another example.

4.6.4 Prevention and Mitigation

In many cases only portions of hazards can be removed by the inherently safer design. For the nuclear power plant, better means to manage the radioactive material is considered because there is no alternative to using the material. For the hazards not eliminated, initiating events are identified.

Prevention and mitigation are considered for each initiating event. The mitigation prevents the initiating event from propagating to an accident. An accident can not occur when each initiating event is prevented or mitigated successfully.

Prevention of access to a dangerous machine in operation by means of guarding can be regarded as an initiating-event prevention if the operation is a normally expected event. In this case, the access itself is an initiating event. When the machine operation is an abnormal event, this is the initiating event, and the access-prevention mechanism acts as an initiating-event mitigation.

Accident mitigations come into play after an accident occurs by failures of the initiating-event prevention and mitigation. A typical accident mitigation is a radioactive material containment to prevent a harmful release into the environment. Washing facilities for removal of contamination and first aid [44] can be regarded as a consequence mitigation. The accident mitigation includes the containment and the consequence mitigation.

The containment as an accident mitigation aims at preventing release of harmful materials. Thus, the accident is mitigated by preventing the release.

4.6.5 Initiating-event Prevention

Equipment failures and human errors can cause initiating events. The following items are important for the initiating-event prevention as well as for mitigation.

Sufficient Safety Margins
This is an approach to cope with uncertainties. A bolt with a diameter larger than a theoretical mean value is used. Equipment is designed conservatively according to proven engineering practice and regulations.

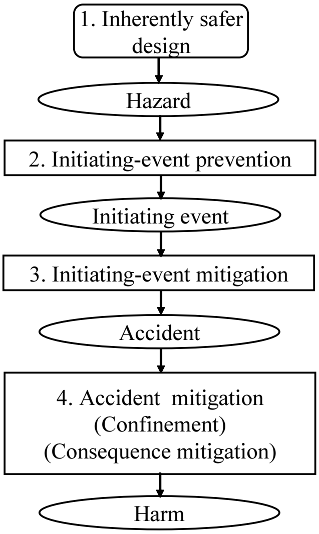

1. Inherently safer design
Hazard
2. Initiating-event prevention
Initiating event
3. Initiating-event mitigation
Accident
4. Accident mitigation (Confinement) (Consequence mitigation)
Harm

Fig. 4.3. Balance between prevention and mitigation

Standardization

Functions, materials, and specifications are standardized. Failure rates are decreased, and inspections become easier. Population size increases, yielding better estimates of residual time to failures.

Preventive Maintenance

Periodic, predictive, and planned maintenance actions taken prior to SSC failure to maintain the SSC within design operating conditions by controlling degradation or failure [45].

1) Periodic maintenance: Maintenance, inspection, and testing activities are accomplished on a routine basis (typically based on operating hours or calendar time) and include activities such as external inspections, alignments or calibrations, internal inspections, overhauls, and component or equipment replacement. Lubrication, filter changes, and teardown are some examples of activities included in periodic maintenance.
2) Predictive maintenance: These activities, including performance monitoring, are generally nonintrusive and can normally be performed with the equipment operating. Vibration analysis (includes spectral analysis), bearing temperature monitoring, lube-oil analysis (ferrography), infrared surveys (thermography), and motor voltage and current checks are some examples of activities included in predictive maintenance. The data obtained from predictive-maintenance activities are used to trend and monitor equipment performance so that planned maintenance can be performed prior to equipment failure.

Corrective Maintenance

SSCs that provide little or no contribution to system safety functions could be allowed to run to failure and are then repaired. This is corrective maintenance rather than preventive maintenance.

Online Maintenance

For a nuclear power plant, this is a planned and scheduled activity to perform preventive or corrective maintenance, with the reactor at power, while properly controlling out-of-service time of systems or equipment. The benefits include increased system and unit availability, reduction of equipment and system deficiencies that could impact operations, more focused attention during periods when fewer activities are competing for specialized resources, and reduction of work scope during outages.

Online maintenance should be carefully managed to achieve a balance between the benefits and potential impacts on safety, reliability or availability. For example, the margin of safety could be adversely impacted if maintenance is performed on multiple equipment or systems simultaneously without proper consideration of risk, or if operators are not fully cognizant of the limitations placed on the plant due to out-of-service equipment. Online maintenance should be carefully evaluated, planned, and executed to avoid undesirable conditions or transients, and to thereby ensure a conservative margin of core safety.

Change Control

Changes to configuration and material should be carefully managed. Serious accidents occurred due to insufficient management of the changes. The famous Flixborough accident occurred in England in 1974 when a pipeline was temporary installed to bypass one of six reactors that was under maintenance. Twenty eight people died due to an explosion caused by ignition of flammable material.

A systematic approach is followed to determine whether initiating events and anticipated plant response are affected by the proposed changes. The proposed changes may 1) increase the frequency of an initiator already included in the PRA, 2) increase the frequency of initiators that were initially screened out in the PRA, 3) introduce new initiating events, or 4) affect the grouping of initiating events [9].

Prevention of Human Error

A necessary condition for human actions to be low safety significance [13] is that the failure of the human (operator) action will not result in the eventual occurrence of a PRA initiating event.

Human errors are treated in Chapter 9. Individual, team, and organization are all sources of human errors.

4.6.6 Initiating-event Mitigation

This corresponds to early detection and early treatment of disease. The mitigation phase assumes that an initiating event has occurred.

Normal Control Systems
Minor disturbances for the plant are dealt with through normal feedback control systems to provide tolerance for failures that might otherwise allow faults or abnormal conditions to develop into accidents. This reduces the frequency of demand on the emergency safety systems. The control system is called a basic process-control system (BPCS) for a process plant (Figure 1.7).

Mitigation Systems
High reliability in these systems is achieved by appropriate use of fail-safe design, by protection against common-cause failures, by independence between mitigation systems (interindependence) and normal control systems (outerindependence), and by monitor and recovery provisions. Proper design ensures that failure of a single component will not cause loss of function of the mitigation system (a single-failure criterion).

Interindependence
Complete mitigation systems can make use of redundancy, diversity, and physical separations of voting components, where appropriate, to reduce the likelihood of loss of vital safety functions. For instance, both diesel-driven and steam-driven generators are installed for emergency power supply; different computer algorithms can be used to calculate the same quantity.

The conditions under which equipment is required to perform safety functions may differ from those to which it is normally exposed and its performance may be affected adversely by aging or by maintenance conditions. The environmental conditions under which equipment is required to function are identified as part of a design process. Among these are conditions expected in a wide range of accidents, including extremes of temperature, pressure, radiation, vibration, humidity, and jet impingement. Effects of external events such as earthquakes should be considered.

Because of the importance of fire as a source of possible simultaneous damage to equipment, design provisions to prevent and combat fires in the plant should be given special attention. Fire-resistant materials are used when possible. Fire-fighting capability is included in the design specifications. Lubrication systems use nonflammable lubricants or are protected against initiating and effects of fires.

Outerindependence
Mitigation systems should be independent of normal process-control systems. For instance, the safety shutdown systems for a chemical plant should be independent of the control systems used for normal operation. Common sensors or devices should only be used if reliability analysis indicates that this is acceptable.

Recovery

Not only the plant itself but also barriers, normal control systems, and mitigation systems should be inspected and tested regularly to reveal any degradation that might lead to abnormal operating conditions or inadequate performance. Operators should be trained to recognize the onset of an accident and respond properly and in a timely manner to abnormal conditions.

Automatic Actuation

Further protection is available through automatic actuation of process control and mitigation systems. Any onset of abnormal behavior will be dealt with automatically for an appropriate period, during which the operating staff can assess systems and decide on a subsequent course of action. Typical decision intervals for operator action range from 10 to 30 min or longer depending on the situation.

Symptom-based Procedures

Plant-operating procedures generally describe responses based on the diagnosis of an event (event-based procedures). If the event cannot be diagnosed in time, or if further evaluation of the event causes the initial diagnosis to be discarded, symptom-based procedures define responses to symptoms observed rather than plant conditions deduced from these symptoms.

Other topics relating to fail-safe design, fail-soft design, and robustness are described below. These are useful for prevention and mitigation of initiating events.

Fail-safe Design

According to fail-safe design principles, if a device malfunctions, it puts the system in a state where no damage can ensue. Consider a drive unit for withdrawing control rods from a nuclear reactor. Reactivity increases with the withdrawal, thus the unsafe side is an inadvertent activation of the withdrawal unit. Figure 4.4 shows a design without a fail-safe feature because the DC motor starts withdrawing the rods when a short circuit occurs. Figure 4.5 shows a fail-safe design. Any short-circuit failure stops electricity to the DC motor. A train braking system is designed to activate when actuator air is lost (de-energize to activate).

Fail-soft Design

According to fail-soft design principles, failures of devices result only in partial performance degradations. A total shutdown can be avoided. This feature is also called a graceful degradation. In a traffic-control system, satellite computers control traffic signals along a road when main computers for the area fail. Local controllers at an intersection control traffic signals when the satellite computer fails. Another example of an automobile steering system is given in Section 8.3.

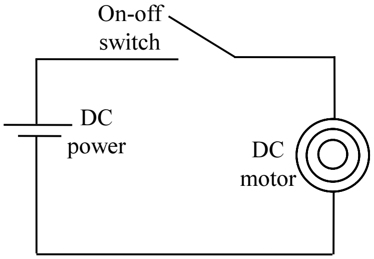


Fig. 4.4. Failed-dangerous circuit

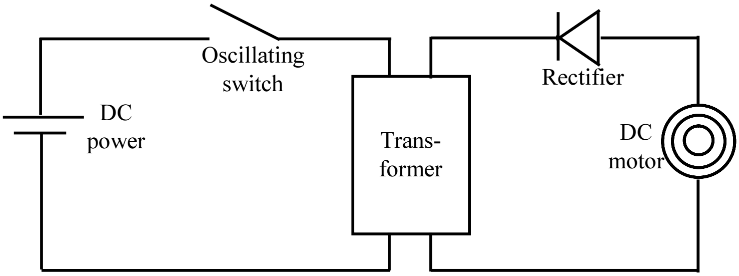


Fig. 4.5. Failed-safe circuit

Robustness

A process controller is designed to operate successfully under uncertain environment and unpredictable changes in plant dynamics. Robustness generally means the capability to cope with events not anticipated.

4.6.7 Accident Mitigation

Accident and consequence mitigation covers the period after the occurrence of an accident. The occurrence of an accident means that events beyond a design basis occurred; initiating events below a design basis, by definition, could never develop into the accident because normal control systems or mitigation systems are assumed to operate as intended.

Because accidents occur, procedural measures must be provided for managing their course and mitigating their consequences. These measures are defined on the basis of operating experience, safety analysis, and the results of safety research. Attention is given to design, siting, procedures, and training to control progressions and consequences of accidents. Limitation of accident consequences is based on safe shutdown, continued availability of utilities, adequate confinement integrity, and offsite emergency preparedness. High-consequence, severe accidents are extremely unlikely if they are effectively prevented or mitigated by defense-in-depth philosophy.

Onsite Consequence Mitigation

Confinement is the most typical accident mitigation. The onsite consequence mitigation includes preplanned and *ad hoc* operational practices that, in circumstances in which plant design specifications are exceeded, make optimum use of existing plant equipment in normal and unusual ways to restore control. This phase would have the objective of restoring the plant to a safe state.

Offsite Consequence Mitigation

Offsite countermeasures compensate for the remote possibility that mitigation measures at the plant fail. In such a case, effects on the surrounding population or the environment can be mitigated by protective actions such as sheltering or evacuation of the population. This involves closely coordinated activities with local authorities.

Accident Management

Onsite and offsite consequence mitigation after the occurrence of an accident is called accident management. For severe accidents beyond the design basis, accident management would come into full play, using normal plant systems, mitigation systems, barriers, and offsite emergency measures in mitigation of the effects of events beyond the design basis.

4.7 Concluding Remarks

Hazards should first be captured intuitively through incentives generated by guide words, vocabularies, and structured searches. Hazard, initiating event, prevention, and mitigation are key elements of risk reduction.

5

Probabilistic Risk Assessment: PRA

5.1 Introduction

This chapter overviews PRAs over three different levels. The PRA has been used most intensively in the nuclear field. The process industry is another intensive user of the PRA. Whenever there is a need for risk quantification, simpler versions of PRA are used in other fields. Risk quantification without the PRA is imperfect and in a very near future any industry with risks will use more and more complete versions of the PRA.

5.2 PRA with or without Material Hazards

5.2.1 Initiating Event and Risk Profiles

From a risk-analysis standpoint there can be no bad ending if there are only good beginnings. There are, regrettably, a variety of bad beginnings. In probabilistic risk assessment, bad beginnings are called initiating events or accident initiators. Without initiating events, no accident can occur. PRA is a methodology that transforms initiating events into risk profiles.

Risk profiles for the plant result from correlating the damage done with the frequency of accident occurrence. Onsite and offsite consequences can be prevented or mitigated by a risk reduction consisting of the four phases shown in Figure 4.3. Initiating events are decreased by inherently safer design. Occurrence likelihoods of initiating events are decreased by initiating-event prevention. An initiating event, once it occurs, is subject to initiating-event mitigation. If an initiating event develops into an accident, then onsite and offsite accident mitigations to halt accident progression by confinement and to mitigate consequences take place.

For consequences to occur, an initiating event must occur; this event must progress to an accident, and this accident must progress sufficiently to yield onsite and offsite consequences. This chain is similar to an influenza outbreak.

An outbreak of flu is an initiating event, a bad beginning; patient death is an onsite accident; airborne infections have offsite consequences. Initiating events are transformed into risk profiles that depend on the relevant risk-reduction measures. PRA provides a systematic approach for clarifying the transformation of an initiating event into a risk profile.

It should be noted that risk profiles are not the only products of a risk study. The PRA process and data identify vulnerabilities in plant design and operation. PRA predicts general accident scenarios, although some specific details might be missed. No other approach has superior predictive abilities [46].

5.2.2 PRA without Material Hazards

PRA is not restricted to a plant containing hazardous materials; PRA applies to all engineered systems or plants, with or without material hazards. The PRA approach is simpler for plants without hazardous materials. Additional steps are required for plants with material hazards because material releases into the environment must be analyzed. Using the medical analogy, both infectious and noninfectious diseases can be dealt with.

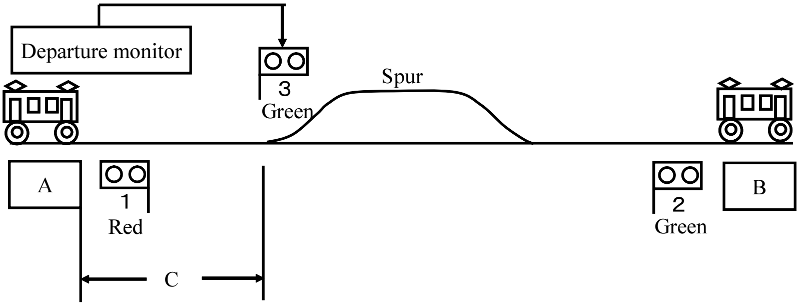


Fig. 5.1. Safety system for single-track railroad

Railway!passenger

As an example of a system without material hazards, consider a single-track passenger railway consisting of terminal A and B and spur between the terminals (Figure 5.2). An unscheduled departure from terminal A that follows failure to observe red departure signal 1 is an initiating event. This type of departure occurred in Japan when the departure signal was stuck red because of a priority override from terminal B. This override was not communicated to terminal A personnel, who might have doubted that the red signal was spurious. The traffic was heavy and the terminal A train conductor neglected the red signal and started the train.

The railway has a departure-monitoring device (DM), designed to prevent accidents due to unscheduled departures by changing traffic signal 3 at the spur branch to red, thus preventing a terminal B train from entering region C between the spur and terminal A. However, this monitoring device was not functioning because it was under maintenance when the departure occurred. A train collision occurred in region C, and 42 people died.

The unscheduled departure as an initiating event would not have yielded a train collision in region C if the departure-monitoring device had functioned, and the terminal B train had remained on the main track before the spur branch until the terminal A train had entered the spur.

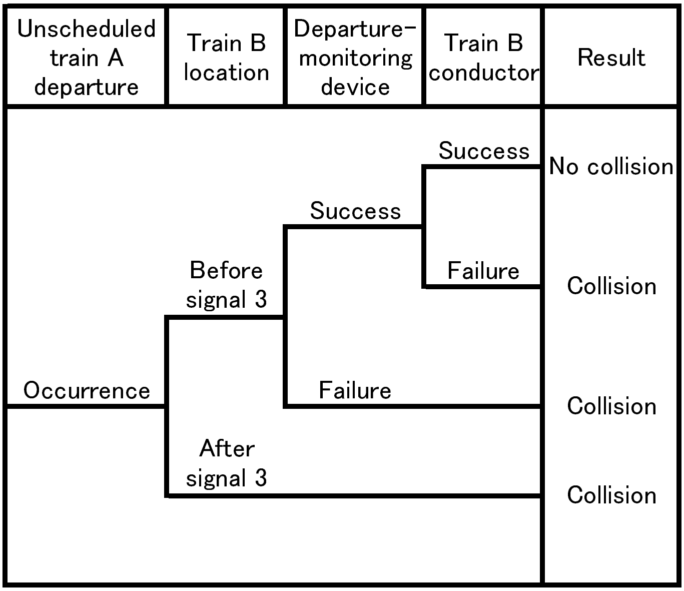


Fig. 5.2. Event tree for the railroad safety system

Two cases are possible; collision and no collision. In one case the terminal B train has not passed the spur signal 3 when the terminal A train commits the unscheduled departure. In another case the terminal B train has crossed the spur signal. Suppose also that the railway has many curves and that a collision occurs whenever there are two trains moving in opposite directions in region C.

Collision scenarios are displayed as an event tree in Figure 5.2. The initiating event develops into a collision when terminal B train is after signal 3. Suppose on the contrary that the train is before signal 3. Then the initiating event yields a collision if the departure-monitoring device fails, or if the terminal B train conductor neglects the red signal at the spur branch, when correctly set by the monitoring device.

The likelihood of collision is a function of the initiating-event frequency, that is, the unscheduled-departure frequency, terminal B train location before or after signal 3, and failure probabilities of two mitigation features, that is, the departure-monitoring device and the terminal B train conductor who should watch spur signal 3.

It should be noted that the collision does not necessarily have serious consequences. It only marks the start of an accident. The accident progression after a collision varies according to factors such as the relative speed of two trains, number of passengers, or strength of chassis to determine fatalities. Most of these factors can only be predicted probabilistically. This means that the conditional collision fatalities can only be predicted as a likelihood. A risk profile, which is a graphical plot of fatality and fatality frequency, must be generated.

5.2.3 PRA with Material Hazards

Transforming initiating events into risk profiles is more complicated if toxic, flammable, or reactive materials are involved. These hazardous materials can cause offsite and onsite consequences.

Freight Railway

For a freight container carrying a toxic gas, an accident progression after collision must include calculation of hole diameters in the gas container. Only then can the amount of toxic gas released from the tank be estimated. The gas leak is called a source term in PRA terminology. Dispersion of this source term is then analyzed and probability distributions of onsite and/or offsite fatalities are then calculated. The dispersion process depends on meteorological conditions such as wind directions and weather sequences; offsite fatalities also depend on the population density around the accident site.

Ammonia Storage Facility

Consider, as another example, an ammonia storage facility where ammonia for a fertilizer plant is transported to a tank from a ship [47]. Potential initiating events include ship-to-tank piping failure, tank failure due to earthquakes, tank overpressure, tank-to-plant piping failure, and tank underpressure. Onsite and offsite risk profiles can be calculated by a procedure similar to the one used for the railway train carrying toxic materials.

Oil Tanker

For an oil tanker, an initiating event could be failure of the marine engine system. This can lead to a sequence of events, that is, drifting, grounding, oil leakage, and sea pollution. A risk profile for the pollution or oil leakage can be predicted from information about frequency of engine failure as an accident initiator; initiating-event propagation to the start of the accident, that is, the grounding; accident-progression analysis after grounding; source-term analysis to determine the amount of oil released; released-oil dispersion; and degree of sea pollution as an offsite consequence.

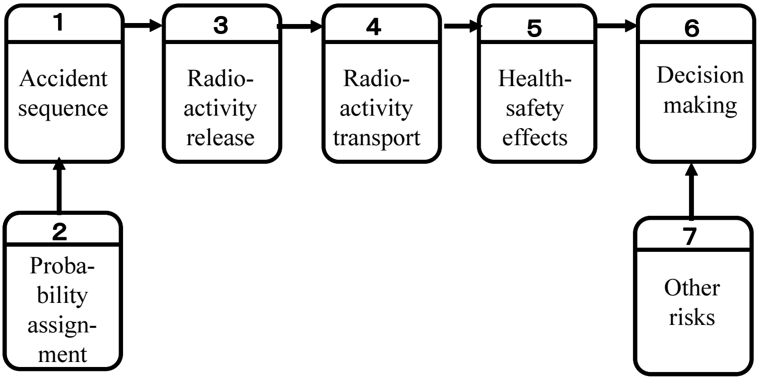


Fig. 5.3. Seven steps of WASH-1400 PRA study

5.2.4 Nuclear Power Plant PRA: WASH-1400

LOCA Event Tree

Consider as a classic example the reactor safety study, WASH-1400, an extensive risk assessment of nuclear power plants sponsored by the US Atomic Energy Commission (AEC) that was completed in 1974. This study includes the seven basic tasks shown in Figure 5.3 [48].

It was determined that the overriding risk of a nuclear power plant was that of radioactive (toxic) fission-product release, and that the critical portion of the plant, that is, the subsystem whose failure initiates the accident, was the reactor-cooling system. The PRA begins by following the potential course of events beginning with (coolant) "pipe breaks," this initiating event having an annual frequency P_A as shown in Figure 5.4. This initiating event is called a loss of coolant accident (LOCA). The second phase begins, as shown in Figure 5.3, with the task of identifying the accident sequence; the different ways in which a fission-product release might occur via core-damage and containment failure.

Fault-tree Analysis

Accidents and failures can be reduced significantly when possible causes of abnormal events are enumerated during the system-design phase. An FTA is an approach to cause enumeration. An FT is an AND/OR tree that develops a top event (the root) into more basic events (leaves) via intermediate events and logic gates. An AND gate requires that the output event from the gate occurs only when input events to the gate occur simultaneously, while an OR gate requires that the output event occurs when one or more input events occur.

FTA was developed by H.A. Watson of the Bell Telephone Laboratories in 1961 to 1962 during an Air Force study contract for the Minuteman Launch Control System. The first published papers were presented at the 1965 Safety Symposium sponsored by the University of Washington and the Boeing Company, where the technique had been applied and extended. Fault trees (FTs) were used with event trees (ETs) in the WASH-1400 study.

Since the early 1970s, when computer-based analysis techniques for FTs were developed, their use has become very widespread. Indeed, the use of FTA is now recommended by a number of governmental agencies responsible for worker and/or public safety. Risk-assessment methodologies based on FTs and ETs (called a level 1 PRA) are widely used in various industries including nuclear, aerospace, chemical, transportation, and manufacturing.

The WASH-1400 study used fault-tree techniques to obtain, by backward logic, numerical values for the Ps in Figure 5.4. This methodology seeks out the equipment failures or human errors that result in top events such as the pipe break or reactor-scram failure depicted in the headings in Figure 5.4. Failure rates, based on data for component failures, operator error, and testing and maintenance error are combined appropriately by means of fault-tree quantification to determine the unavailability of the safety systems or an annual frequency of each initiating event. This procedure is identified as task 2 in Figure 5.3.

Event-tree Analysis

Now let us return to box 1 of Figure 5.3, by considering the event tree (Figure 5.4) for a LOCA initiating event in a typical nuclear power plant. The accident starts with a coolant-pipe break having a frequency of occurrence P_A. The potential course of events that might follow such a pipe break are then examined. Figure 5.4 is the event tree, which shows all possible alternatives. At the first branch, the status of the reactor scram is considered. If it is successful, the next-in-line system, the emergency core-cooling system (ECCS), is studied. Failure of the ECCS results in fuel meltdown and varying amounts of fission-product release, depending on the containment integrity.

Forward versus Backward Logic

It is important to recognize that event trees are used to define accident sequences that involve complex interrelationships among engineered safety systems. They are constructed using forward logic: We ask the question "What happens if the pipe breaks?" Fault trees are developed by asking questions such as "How could the electric power fail?" Forward logic used in event-tree analysis and FMEA is often referred to as inductive logic, whereas the type of logic used in fault-tree analysis is deductive.

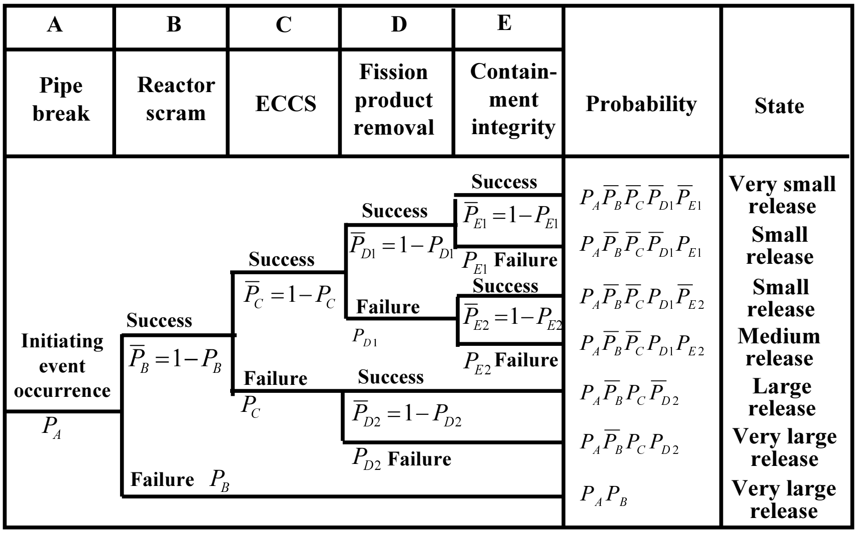

A
B
C
D
E
Pipe break
Reactor scram
ECCS
Fission product removal
Contain-ment integrity
Probability
State
Initiating event occurrence
P_A
Success
$\overline{P}_B = 1 - P_B$
Failure P_B
Success
$\overline{P}_C = 1 - P_C$
Failure
P_C
Success
$\overline{P}_{D1} = 1 - P_{D1}$
Failure
P_{D1}
Success
$\overline{P}_{D2} = 1 - P_{D2}$
P_{D2} Failure
Success
$\overline{P}_{E1} = 1 - P_{E1}$
P_{E1} Failure
Success
$\overline{P}_{E2} = 1 - P_{E2}$
P_{E2} Failure
$P_A\overline{P}_B\overline{P}_C\overline{P}_{D1}\overline{P}_{E1}$
$P_A\overline{P}_B\overline{P}_C\overline{P}_{D1}P_{E1}$
$P_A\overline{P}_B\overline{P}_C P_{D1}\overline{P}_{E2}$
$P_A\overline{P}_B\overline{P}_C P_{D1}P_{E2}$
$P_A\overline{P}_B P_C\overline{P}_{D2}$
$P_A\overline{P}_B P_C P_{D2}$
$P_A P_B$
Very small release
Small release
Small release
Medium release
Large release
Very large release
Very large release

Fig. 5.4. Simplified event tree for describing the WASH-1400 study

Event-tree Pruning

In a binary analysis of a system that either succeeds or fails, the number of potential accidents is 2^N where N is the number of systems considered at event-tree headings. In practice, as will be shown in the following discussion, the tree of Figure 5.4 is a reduced tree after the pruning.

One of the first things of interest is the success of reactor scram. The question is, what is the probability, P_B of reactor-scram failing, and how would it affect other safety systems? If there is no reactor scram, the emergency core-cooling pumps and sprays are useless – in fact, none of the postaccident functions can be effective. Thus, no choices are shown in the simplified event tree when reactor scraam is unsuccessful and a very large release with frequency $P_A P_B$ occurs. In the event that the success of reactor scram depends on the pipe that broke, the probability P_B should be calculated as a conditional probability to reflect such a dependency.

If reactor scram is successful, the next choice for study is the availability of the ECCS. It can work or it can fail, and its unavailability, P_{C1}, would lead to the sequence shown in Figure 5.4. Notice that there are still choices available that can affect the course of the accident. If the fission-product removal systems operate, a smaller radioactive release would result than if they failed. Of course, their failure would in general produce a lower probability accident sequence than one in which they operated. By working through the entire event tree, we produce a spectrum of release magnitudes and their likelihoods for the various accident sequences (Figure 5.5).

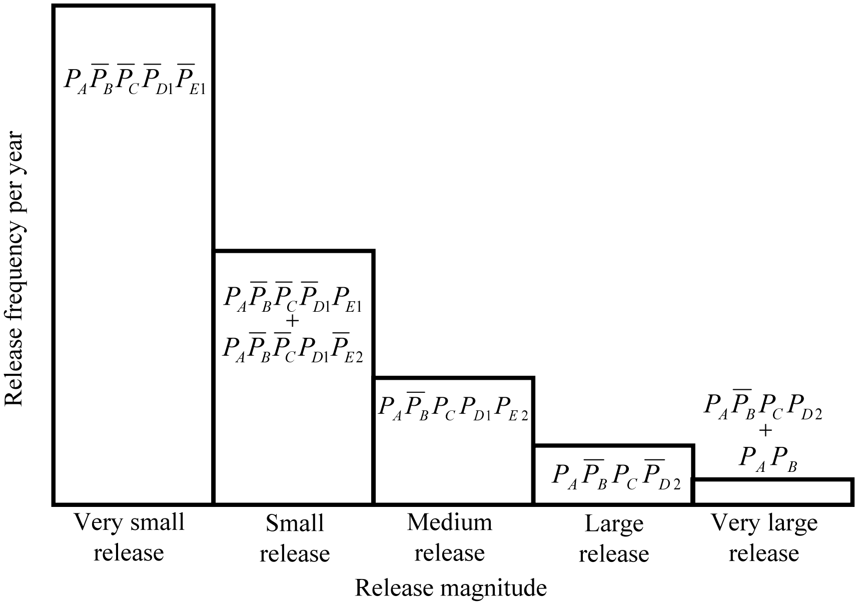


Fig. 5.5. A risk profile with the horizontal axis being the release magnitude

Deterministic Analysis

The top line of the event tree is the conventional design basis (*i.e.* specific functions to be performed by a structure, system, or component of a facility) for LOCA. In this sequence, the pipe is assumed to break but each of the safety systems is assumed to operate. The classical deterministic method ensures that safety systems can prevent accidents for an initiating event such as LOCA. In more elaborate deterministic analyses, when only a single failure of a safety system is considered, that is called a single-failure criterion. In PRA all safety-system failures are assessed probabilistically together with the potential initiating events.

Nuclear PRA with Modifications

There are many lessons to be learned from PRA evolution in the nuclear industry. Sophisticated models and attitudes developed for nuclear PRAs have found their way into other industries [49].

With suitable interpretation of technical terms, and with appropriate modifications of the methodology, most aspects of nuclear PRA apply to other fields. For instance, nuclear PRA defines core damage as an accident, while a train collision would be an accident for a railway problem. For an oil-tanker problem, grounding is an accident. For a medical problem, patient death would be an accident. Correspondences among PRAs for a nuclear power plant, a single-track railway, an oil tanker, and a disease are shown in Table 5.1 for

Table 5.1. PRA applications to different fields

Concept	Nuclear	Railroad	Tanker	Disease
Initiating event	LOCA	Illegal departure	Engine failure	Flu outbreak
Safety system	ECCS	Monitor Monitor	Distress signal	Immune system
Accident	Core damage	Collision	Stranded	Death
Accident propagation	Damage propagation	Collision propagation	Strand propagation	Flu propagation
Propagation factor	Reactor pressure	Collision speed	Hull strength	Virus toxity
Source term	Radioactivity	Poison gas	Oil	Virus
Dispersion & transportation	Radioactivity	Poison gas	Oil	Virus
Onsite consequence	Staff killed	Passenger killed	Crew killed	Patient killed
Offsite mitigation	Evacuation & decontamination	Evacuation	Oil fence	Vaccination
Offsite consequence	Surrounding area	Surrounding area	Sea pollution	Flu prevalence

terms such as initiating event, mitigation system, accident, accident progression, progression factor, source term, dispersion and transport, onsite consequence, consequence mitigation, and offsite consequence.

5.2.5 NUREG-1150 and ASME PRA Quality Standard

PRA Five Steps

According to a recent study, NUREG-1150, PRA consists of the five steps shown in Figure 5.6 [50].

1) Accident-frequency analysis.
2) Accident-progression analysis.
3) Source-term analysis.
4) Offsite-consequence analysis.
5) Risk calculation.

This figure shows how initiating events are transformed into risk profiles via four intermediate products:

1) Accident-sequence groups.
2) Accident-progression groups.
3) Source-term groups.
4) Offsite consequences.

Some steps can be omitted, depending on the application, but other steps may have to be introduced. For instance, a collision accident scenario for passenger trains does not require a source-term analysis or offsite-consequence analysis, but does require an onsite consequence analysis to estimate passenger fatalities. Parametric uncertainties in the risk profiles are evaluated by sampling likelihoods from distributions.

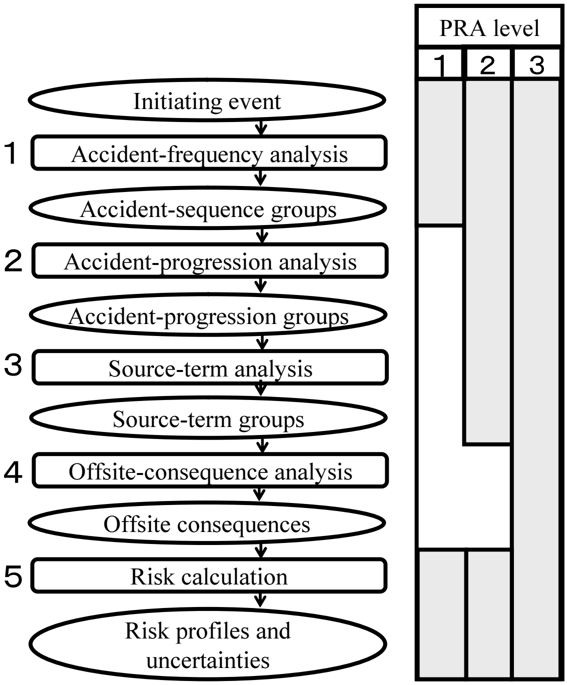

PRA level
1
2
3
Initiating event
1
Accident-frequency analysis
Accident-sequence groups
2
Accident-progression analysis
Accident-progression groups
3
Source-term analysis
Source-term groups
4
Offsite-consequence analysis
Offsite consequences
5
Risk calculation
Risk profiles and uncertainties

Fig. 5.6. Definition of 3 levels of PRA

5.3 Three PRA Levels

As shown by the “PRA level” in Figure 5.6, a level 1 PRA consists of the first and last of the five PRA steps, that is, accident-frequency analysis and risk calculation. A level 2 PRA performs accident-progression and source-term analyses in addition to the level 1 PRA analyses. A level 3 PRA performs a total of five analyses, that is, an offsite-consequence analysis and level 2 PRA analyses. Each PRA performs risk calculations. Level 1 risk profiles refer to accident occurrence, level 2 profiles to material-release magnitudes, and level 3 profiles to consequence measures such as fatalities.

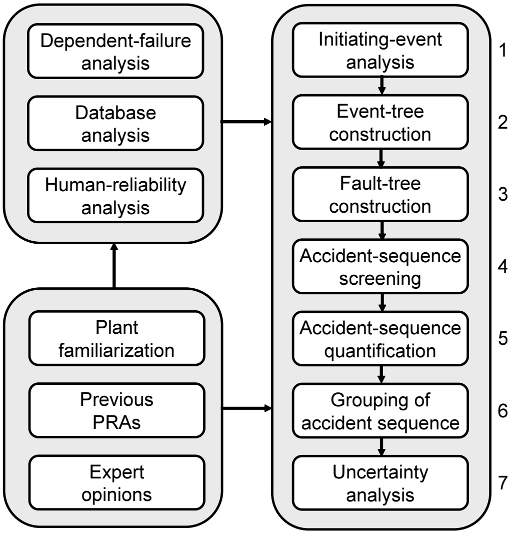

Dependent-failure analysis
Database analysis
Human-reliability analysis
Plant familiarization
Previous PRAs
Expert opinions
Initiating-event analysis
1
Event-tree construction
2
Fault-tree construction
3
Accident-sequence screening
4
Accident-sequence quantification
5
Grouping of accident sequence
6
Uncertainty analysis
7

Fig. 5.7. Steps for level 1 PRA (NUREG-1150)

5.4 Level 1 PRA – Accident Frequency

This PRA mainly deals with accident frequencies, that is, frequencies of core damage, train collisions, oil-tanker groundings, and so forth. Accident sequences and their groups are identified in a level 1 PRA. The plant states associated with these accident-sequence groups are core damage by oxidization, train damage by collision, oil-tanker damage by grounding, and so on. These accident-sequence groups are used as inputs to a level 2 PRA.

5.4.1 Accident-frequency Analysis

A level 1 PRA analyzes how initiating events develop into accidents. This transformation is called an accident-frequency analysis in PRA terminology. Level 1 PRAs identify combinations of events that can lead to accidents and then estimate their frequency of occurrence.

The definition of accident varies from application to application. Some applications involve more than one accident. For instance, for a railway it may include collision and derailment. Initiating events also differ for different applications. A loss of coolant is an initiating event for a nuclear power plant, while an unscheduled departure is an accident initiator for a railway collision.

A level 1 PRA consists of the activities shown in Figure 5.7.

1) Initiating-event analysis.
2) Event-tree construction.
3) Fault-tree construction.
4) Accident-sequence screening.

5) Accident-sequence quantification.
6) Grouping of accident sequences.
7) Uncertainty analysis

These activities are supported by the following analyses.

1) Plant familiarization.
2) Dependent-failure analysis.
3) Human-reliability analysis.
4) Database analysis.

5.4.2 ASME Level 1 Quality Standard

According to the most recent level 1 PRA standard from ASME [5], the accident-frequency analysis consists of the following steps:

1) Initiating-events analysis (IE).
2) Accident-sequence (development) analysis (AS).
3) Success-criteria analysis (SC).
4) Systems analysis (SY).
5) Human-reliability analysis (HR).
6) Data analysis (DA).
7) Quantification (QU).

Refer to reference [51] for more information about PRA scope and elements.

The ASME PRA standard addresses full power internal event PRA and a limited level 2 PRA. The internal event PRA includes internal floods. The standard consists of requirements that state what should be done rather than how. The PRA-quality requirements form a two-level structure. A high-level requirement (HLR) associates with it one or more supporting requirements (SRs). The first HLR for the initiating-events analysis (IE) is labeled as HLR-IE-A, while the first supporting requirement for HLR-IE-A is labeled as IE-A1 and the second as IE-A2.

5.4.3 Plant Familiarization

An initial PRA task is to gain familiarity with the plant under investigation, as a foundation for subsequent tasks. Information is assembled from such sources as:

1) Safety-analysis reports.
2) Piping and instrumentation diagrams.
3) Technical specifications.
4) Operating and maintenance procedures and records.

A plant visit to inspect the facility and gather information from plant personnel is part of the process. Typically, one week is spent in the initial visit to a large plant. At the end of the initial visit, much of the information needed to perform the remaining tasks will have been collected and discussed with plant personnel. The PRA team should now be familiar with the plant design and operation, and be able to maintain contact with the plant staff throughout PRA to verify information and to identify plant changes that occur during the PRA [50].

5.4.4 Initiating-event Analysis

The initiating events are analyzed in a stepwise manner. The first step is the most important.

1) Identification of initiating events by a review of previous PRAs, plant data, and other information.
2) Elimination of very low frequency initiating events. The ASME standard gives screening criteria as supporting requirement IE-C4 [5].
3) Identification of safety functions required to prevent an initiating event from developing into an accident.
4) Identification of active systems performing a safety function.
5) Identification of support systems necessary for operation of the active systems.
6) Delineation of success criteria (*e.g.*, two-out-of-three operating) and event timing for each active system responding to an initiating event.
7) Grouping of initiating events, based on similarity of safety-system response.

For a nuclear power plant, a list of initiating events is available in NUREG-1150. These include transient, LOCA, and special initiators such as instrument line breaks. A transient is an equipment- and human-induced event that disrupts the plant and leaves the primary system pressure boundary *intact*. A LOCA is an equipment- and human-induced event that disrupts the plant by causing a *breach* in the core-coolant system with a resulting loss of core-coolant inventory [5]. Systematic approaches for identifying initiating events include master logic diagrams, heat-balance fault trees, FMEA, and HAZOP (Chapter 4).

Different sets of initiating events may apply to modes of operation such as full power, low power (*e.g.*, up to 15% power), startup, and shutdown. The shutdown mode is further divided into cold shutdown, hot shutdown, refueling, and so on. An inadvertent power increase at low power may produce a plant response different from that at full power [52].

For each initiating event, an event tree is developed that details the relationships among the systems required to respond to the event, in terms of potential system successes and failures. For instance, the event tree of Figure 5.2 considers an unscheduled departure of terminal A train. If more than one initiating event is involved, these events are examined and grouped according to the mitigation system (*i.e.* safety system) response required. The word “mitigation” is used against the initiating event. An event tree is developed for each group of initiating events, thus minimizing the number of event trees required.

5.4.5 Event-tree Construction

Event Trees Coupled with Fault Trees

Event trees for a level 1 PRA are called accident-sequence event trees. Active systems and related support systems in event-tree headings are modeled by fault trees. Boolean-logic expressions, reliability block diagrams, and other schematics are sometimes used to model these systems.

A combination of event trees and fault trees is illustrated in Figure 2.3 where the initiating event is a pump overrun and the accident is a tank rupture.

Figure 5.2 is another example of an accident-sequence event tree where the unscheduled departure is an initiating event. This initiator can also be analyzed by a fault tree that should identify, as a cause of the top event, the human error of neglecting a red departure signal because of heavy traffic. The departure-monitoring system failure can also be analyzed by a fault tree that deduces basic causes such as an electronic interface failure because of a maintenance error. A so-called cause–consequence diagram is an extension of this marriage of event and fault trees [53].

Event trees enumerate sequences leading to an accident for a given initiating event. Event trees are constructed in a step-by-step process. Generally, a function event tree is created first. This tree is then converted and expanded into a system event tree. Two approaches are available for the marriage of event and fault trees; large ET/small FT approach, and small ET/large FT approach.

Function Event Trees

Initiating events are grouped according to safety system (*i.e.* mitigation system) responses; therefore, construction focuses on safety-system functions. For the single-track railway problem, the safety functions include departure monitoring and spur-signal watching. The first function could be performed either by an automatic departure-monitoring device or by a human.

A nuclear power plant has the following safety functions [54].

1) Reactivity control: shuts reactor down to reduce heat production.
2) Coolant-inventory control: maintains a coolant medium around the core.
3) Coolant-pressure control: maintains the coolant in its proper state.
4) Core heat removal: transfers heat from the core to a coolant.
5) Coolant heat removal: transfers heat from the coolant.
6) Containment isolation: closes openings in containment to prevent radionuclide release.
7) Containment temperature and pressure control: prevents damage to containment and equipment.
8) Combustible gas control: removes and redistributes hydrogen to prevent explosion inside containment.

It should be noted that the coolant-inventory control can be performed by a high-pressure core-spray system or low-pressure core-spray systems.

1) High-pressure core-spray system: provides coolant to the reactor vessel when vessel pressure is high or low.
2) Low-pressure core-spray system: provides coolant to the reactor vessel when vessel pressure is low.

Each event-tree heading except for the initiating event refers to a mitigation function or physical systems. When all headings except for the initiator are described on a function level rather than a physical system level, then the tree is called a function event tree. Function event trees are developed for each initiator group because each group generates a distinctly different functional response. The event-tree headings consist of the initiating-event group and the required safety functions.

The LOCA event tree in Figure 5.4 is a function event tree because ECCS, for instance, is a function name rather than the name of an individual physical system. Figure 5.2 is a system event tree.

System Event Trees

Some mitigating systems perform more than one function or portions of several functions, depending on plant design. The same safety function can be performed by two or more mitigation systems. There is a many-to-many correspondence between safety functions and accident-mitigation systems.

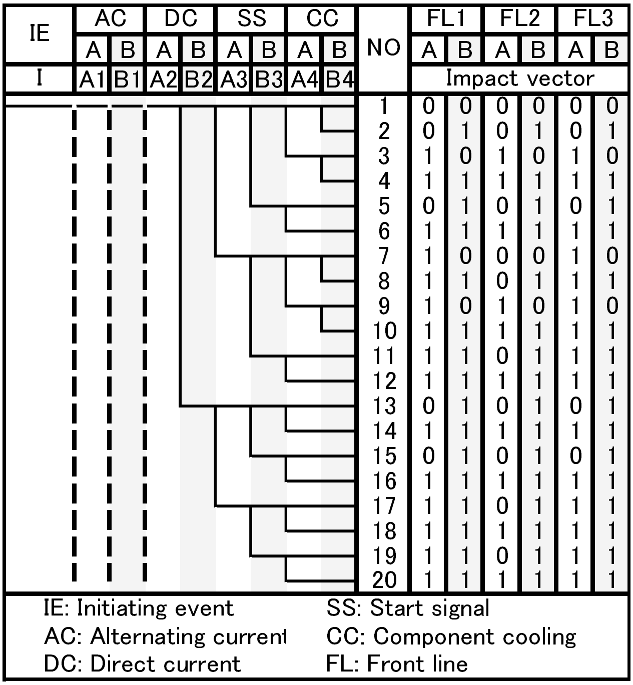
The function event tree is not an end product; it is an intermediate step that permits a stepwise approach to sorting out the complex relationships between accident initiators and the response of mitigating systems. It is the initial step in structuring plant responses in a temporal format. The function event-tree headings are eventually decomposed by identification of mitigation systems that can be measured quantitatively [54]. The resultant event trees are called system event trees.

Large ET/Small FT Approach

Each mitigation system consists of an active system and associated support systems. An active system requires supports such as AC power, DC power, cooling, or start signals from the support systems. For instance, a reactor shutdown system requires a so-called reactor trip signal. This signal may also be used as an input to actuate other systems.

In the large ET/small FT approach, a special-purpose tree called a support-system event tree is sometimes constructed to represent the status of different support systems. This support-system event tree is then assessed with respect to its impact on the operability of a set of active systems [55]. This approach is also called an explicit method, event trees with boundary conditions, or small fault-tree models with support-system states. The fault-tree size is reduced, but the total number of fault trees increases because there are more headings in the support-system event tree.

Figure 5.8 is an example of a support-system event tree. Four types of support systems are considered: AC power, DC power, component cooling (CC), and start signal (SS). Three kinds of active systems exist: FL1, FL2,



NO	FL1		FL2		FL3	
	A	B	A	B	A	B
1	0	0	0	0	0	0
2	0	1	0	1	0	1
3	1	0	1	0	1	0
4	1	1	1	1	1	1
5	0	1	0	1	0	1
6	1	1	1	1	1	1
7	1	0	0	0	1	0
8	1	1	0	1	1	1
9	1	0	1	0	1	0
10	1	1	1	1	1	1
11	1	1	0	1	1	1
12	1	1	1	1	1	1
13	0	1	0	1	0	1
14	1	1	1	1	1	1
15	0	1	0	1	0	1
16	1	1	1	1	1	1
17	1	1	0	1	1	1
18	1	1	1	1	1	1
19	1	1	0	1	1	1
20	1	1	1	1	1	1

IE: Initiating event
AC: Alternating current
DC: Direct current
SS: Start signal
CC: Component cooling
FL: Front line

Fig. 5.8. Support-system event tree

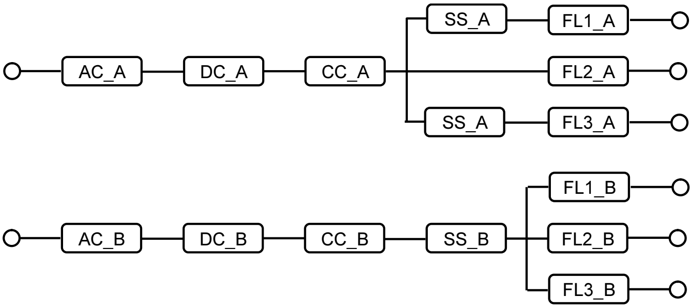


Fig. 5.9. Reliability block diagram representing dependency of front-line systems on support systems

and FL3, where symbol “FL”means “front line”. Each of these support or active systems is redundantly configured, as shown by columns A and B.

Figure 5.9 shows how active systems are related to support systems. Active systems except for FL2_A require start signals in addition to the AC power, DC power, and component cooling. In other words, start signal SS_A is not required for active system FL2_A.

Sequence 1 in Figure 5.8 shows that all support systems are normal, hence all active systems are supported correctly as indicated by impact vector $(0,0,0,0,0,0)$. Support system CC_B is failed in sequence 2, and three active systems in column B are failed, as indicated by impact vector $(0,1,0,1,0,1)$. Other combinations of support-system states and corresponding impact vectors are interpreted similarly.

From the support-system event tree of Figure 5.8, six different impact vectors are deduced. In other words, support systems influence active systems in six different ways:

$$\begin{gathered}(0,0,0,0,0,0),(0,1,0,1,0,1)\\(1,0,1,0,1,0),(1,1,1,1,1,1)\\(1,0,0,0,1,0),(1,1,0,1,1,1)\end{gathered}\tag{5.1}$$

Sequences that result in the same impact vector are grouped together. An active system event tree is constructed for each of the unique impact vectors. Impact vectors give explicit boundary conditions of active system event trees.

Small ET/Large FT Approach

Another approach is a small ET/large FT configuration. Here, each event-tree heading represents a mitigation-system failure, including both active and support systems; failures of relevant support systems appear in a fault tree that represents a mitigation system failure. Therefore, the small ET/large FT approach results in larger and smaller fault trees in size and in number, respectively; the event trees become smaller.

Dependencies along Accident Sequence

The ASME Standard lists the following dependencies to impact the ability of mitigating systems [5].

1) Mitigating systems impacted by the initiating event.
2) Dependence on success or failure of preceding functions. For instance, low-pressure system injection is dependent on the success of pressure-vessel depressurization.
3) Harsh environment of temperature, pressure, debris, water levels, humidity that could impact on the success of the system or function. An example is loss of pump net positive suction head.
4) If the probability of event B is dependent on the occurrence or nonoccurrence of event A, event A is placed to the left of event B in the ordering of event-tree headings.
5) For large ET/small FT approach, develop the event trees to a level of detail sufficient to identify intersystem dependencies (Section 4.6.6) and train-level interfaces.
6) Include events for which time-phased dependencies might exist. For a station blackout initiating event, for example, include AC power recovery time.

5.4.6 System Models: Fault-tree Constuction

Each event-tree heading describes the failure of a mitigation system, an active system, or a support system. The term system modeling is used to describe both quantitative and qualitative failure modeling. Fault-tree analysis is one of the best analytical tools for system modeling. Other tools include decision trees, decision tables, reliability block diagrams, Boolean algebra (Chapter 7), and Markov transition diagrams (Section 8.3). Each system model can be quantified to evaluate the occurrence probability of the event-tree heading.

Failure modes should be included for components contained in the model, consistent with the available data and model level of detail [5].

1) active component fails to start;
2) active component fails to continue to run;
3) failure of a closed (open) component to open (close);
4) failure of a closed (open) component to remain closed (open);
5) active component spurious operation;
6) plugging, leakage, or rupture of an active or passive component;
7) internal leakage or rupture of a component;
8) failure to provide signal (*e.g.*, from or to instrumentation);
9) spurious signal;
10) preinitiator (or postinitiator) human error events;
11) other failures of a component to perform its required function.

Proceduralized recovery actions should not be used as the sole basis for eliminating (or screening out) a support system from the model; however, these recovery actions may be included in the model quantification. Some systems are components and equipment that are required for operation of other systems. Components that may otherwise be screened from a system model should be included if their failure affects more than one system. An example is a common suction pipe feeding two separate systems [5].

5.4.7 Accident-sequence Screening and Quantification

Accident-sequence Screening

An accident sequence is an event-tree path. The path starts with an initiating event followed by success or failure of active and/or support systems. A partial accident sequence containing a subset of failures is not processed further and is dropped if its frequency estimate is less than, for instance, 10^{-9} per year, since each additional failure-occurrence probability reduces the estimate further. However, if the frequency of a partial accident sequence is above the cutoff value, the sequence is developed and recovery actions pertaining to specific situations are applied to the appropriate remaining sequences.

Accident-sequence Quantification

A Boolean reduction, when performed for fault trees (or decision trees, reliability block diagrams, *etc.*) along an accident sequence, reveals a combination of failures that can lead to the accident (Section 7.5). These combinations are called minimal cut sets. Once important failure events are identified, frequencies or probabilities are assigned to these events and the accident-sequence frequency is quantified via the minimal cut sets. Dependent failures and human reliability as well as hardware databases are used in the assignment of likelihoods.

A clear description of success criteria is required to evaluate each plant state resulting from an accident sequence. Plant parameters (*e.g.*, highest temperature) and acceptance criteria (*e.g.*, temperature limit) are specified to be used in determining the occurrence of core damage. Computer-code-predicted acceptance criteria are defined with sufficient margin to allow for limitations of the codes, sophistication of the models, and uncertainties in the results [5].

5.4.8 Dependent Failure Analysis

Explicit Dependency

As described in Section 3.4.2, system analysis generally tries to include explicit dependencies in the basic plant-logic model. Functional and common-equipment dependencies arise from the reliance of active systems on support systems, such as the reliance of emergency coolant injection on service water and electrical power. Dependent failures are usually modeled as integral parts of fault and event trees. Interaction among various components within systems, such as common maintenance or test schedules, common control or instrumentation circuitry, and location within plant buildings (common operating environments), are often included as basic events in system fault trees.

Implicit Dependency

Even though the fault- and event-tree models explicitly include major dependencies, in some cases it is not possible to identify the specific mechanisms of a dependent failure. In other cases, there are many different types of dependent failures, each with a low probability, and it is not practical to model them separately. Parametric models (Section 8.2.2) can be used to account for the collective contribution of residual common-cause failures to *identical* or *similar* components. The accident-frequency analysis shall provide a reasonably complete treatment of common-cause failures and intersystem and intrasystem dependencies [5].

5.4.9 Human-reliability Analysis

Human-reliability analysis identifies human actions in the PRA process. It also determines the human-error rates to be used in quantifying these actions. The NUREG-1150 analysis considers preinitiator human errors that occur before an initiating event (inclusive), and postinitiator human errors after the initiating event. The postinitiator errors are further divided into accident-procedure errors and recovery errors. The human-reliability analysis is described in Chapter 9.

Preinitiator errors are usually incorporated into system models. For example, a cause of the departure-monitoring failure of Figure 5.2 is included in the fault tree as a maintenance error before the unscheduled departure.

Accident-procedure errors are typically included at the event-tree level as a heading or a top event because they are an expected plant/operator response to the initiating event. These errors are examples of postinitiator errors. The event tree of Figure 5.2 includes a train B conductor human error after the unscheduled departure. Accident-procedure errors are included in the system models if they impact only local components.

Recovery actions are included either in the event trees or the system models. Recovery actions are usually considered when a relevant accident sequence without recovery has a non-negligible likelihood.

To support accident-sequence quantification, estimates are required for human-error rates. These probabilities can be evaluated, for instance, using THERP techniques [56] and plant-specific characteristics.

5.4.10 Database Analysis

This task involves the development of a database for quantifying initiating-event frequencies and basic event probabilities for event trees and system models [50]. A generic database representing typical initiating-event frequencies as well as plant component-failure rates and their uncertainties are developed.

Data for plant being analyzed may differ significantly, however, from averaged industry-wide data. In this case, the operating history of the plant is reviewed to develop plant-specific initiating-event frequencies and to determine whether any plant components have unusually high or low failure rates. Test and maintenance practices and plant experiences are also reviewed to determine the frequency and duration of these activities and component service hours. This information is used to supplement the generic database via a Bayesian update analysis. The basic event quantification is described in Chapter 6.

5.4.11 Grouping of Accident Sequence

There may be a variety of accident progressions even if an accident sequence is given; a chemical plant fire may or may not result in a storage-tank explosion. On the other hand, different accident sequences may progress in a similar way. For instance, all sequences that include delayed fire-department arrival would yield a serious fire.

Accident sequences are regrouped into sequences that result in similar accident progressions. A large number of accident sequences may be identified and their grouping facilitates accident-progression analyses in a level 2 PRA. This is similar to the grouping of initiating events prior to accident-frequency analysis.

5.4.12 Uncertainty Analysis

The uncertainty analysis of statistical parameters relating to the frequency of an accident sequence or an accident-sequence group can be accomplished by Monte Carlo calculations that sample basic likelihood. Uncertainties in basic likelihoods are represented by distributions of frequencies and probabilities that are sampled and combined along an accident sequence or accident-sequence group levels. Statistical parameters such as median, mean, 95% upper bound, and 5% lower bound are thus obtained [53].

5.4.13 Products from Level 1 PRA

An accident-sequence analysis (level 1 PRA) typically yields the following products.

1) Definition and estimated frequency of accident sequences.
2) Definition and estimated frequency of accident-sequence groups.
3) Total frequency of abnormal accident frequencies.

5.5 Level 2 PRA – Accident Progression and Source Term

A level 2 PRA consists of accident-progression and source-term analyses in addition to the level 1 PRA.

5.5.1 Accident-progression Analysis

This investigates physical processes for accident-sequence groups. For the single-track-railway problem, physical processes before and after a collision are investigated; for the oil-tanker problem, grounding scenarios are investigated; for plant fires, propagation is analyzed.

The principal tool for an accident-progression analysis is an accident-progression event tree (APET). Accident-progression scenarios are identified by this extended version of event trees. In terms of the railway problem, an APET may include branches with respect to factors such as relative collision speed, number of passengers, toxic-gas inventory, train position after collision, and hole size in gas containers. The output of APET is a listing of different outcomes for the accident progression.

Unless hazardous materials are involved, onsite-consequences such as passenger fatalities by a railway collision are investigated together with their likelihoods. When hazardous materials are involved, outcomes from APET are grouped into accident-progression groups (APGs) as shown in Figure 5.6. Each outcome of an APG has similar characteristics, and becomes the input for the next stage of analysis, that is, source-term analysis.

Accident-progression analyses yield the following products.

1) accident-progression groups;
2) conditional probability of each accident-progression group, given an accident-sequence group.

5.5.2 Source-term Analysis

This is performed when there is a release of toxic, reactive, flammable, or radioactive materials. A source-term analysis yields the fractions of the inventory of toxic material released. The amount of material released is the inventory multiplied by a release fraction. In the nuclear industry, source terms are grouped in terms of release-initiation time, duration of release, and contributions to immediate and latent health problems, since different types of pollutants are involved.

5.6 Level 3 PRA – Offsite Consequence

A level 3 PRA considers, in addition to a level 2 PRA, the full range of consequences caused by dispersion of hazardous materials into the environment. An offsite consequence analysis yields a set of consequence measure values for each source-term group. For NUREG-1150, these measures include early fatalities, latent cancer fatalities, population dose (within 50 miles and total), and two measures for comparison with NRC's safety goals (average individual early fatality probability within 1 mile and average individual latent probability within 10 miles).

5.7 Risk Calculations

5.7.1 Level 3 PRA Risk Profile

The final result of a PRA is the risk profiles produced by assembling the results of all three PRA risk-analysis studies.

Consequence Measure
Consider a particular consequence measure denoted by CM divided into m small intervals, $I_l,\ l = 1, \ldots, m$.

Frequency and Probability
Define the following frequencies and conditional probabilities (see Figure 5.10).

1) $f(\mathrm{IE}_h)$: Annual frequency of initiating event h.
2) $\Pr\{\mathrm{ASG}_i|\mathrm{IE}_h\}$: Conditional probability of accident-sequence group i, given occurrence of initiating event h. This is obtained by an accident-frequency analysis using accident-sequence event and fault trees.

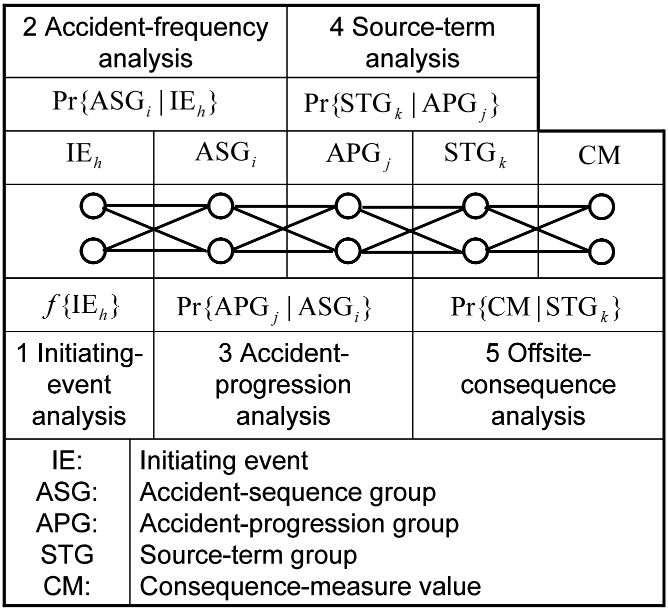

2 Accident-frequency analysis
4 Source-term analysis
Pr{ASG$_i$ | IE$_h$}
Pr{STG$_k$ | APG$_j$}
IE$_h$
ASG$_i$
APG$_j$
STG$_k$
CM
f{IE$_h$}
Pr{APG$_j$ | ASG$_i$}
Pr{CM | STG$_k$}
1 Initiating-event analysis
3 Accident-progression analysis
5 Offsite-consequence analysis
IE: Initiating event
ASG: Accident-sequence group
APG: Accident-progression group
STG Source-term group
CM: Consequence-measure value

Fig. 5.10. Frequency and conditional probabilities in PRA

3) $\Pr\{\mathrm{APG}_j|\mathrm{ASG}_i\}$: Conditional probability of accident-progression group j, given occurrence of accident-sequence group i. This is obtained by an accident-progression analysis using APETs.
4) $\Pr\{\mathrm{STG}_k|\mathrm{APG}_j\}$: Conditional probability of source-term group k, given occurrence of accident-progression group j. This is usually a zero–one probability. In other words, the matrix element for given values of j and k is 1.0 if APG_j is assigned to STG_k, and 0.0 otherwise. This assignment is performed by a source-term analysis.
5) $\Pr\{\mathrm{CM} \in I_l|\mathrm{STG}_k\}$: Conditional probability of consequence measure CM being in interval I_l, given the occurrence of source-term group k. For a fixed source-term group, a consequence value is not uniquely determined because it depends on probabilistic factors such as a combination of wind direction and weather. Typically, 2500 weather trials were performed in NUREG-1150 for each STG_k to estimate the conditional probability. Denote by W_n a particular weather trial. The conditional probability is:

$$\Pr\{\mathrm{CM} \in I_l|\mathrm{STG}_k\} = \sum_n \Pr\{\mathrm{CM} \in I_l|\mathrm{W}_n, \mathrm{STG}_k\}\Pr\{\mathrm{W}_n|\mathrm{STG}_k\} \quad (5.2)$$

where $\Pr\{\mathrm{CM} \in I_l|\mathrm{W}_n, \mathrm{STG}_k\}$ is unity for a particular interval I_l because the source-term group and weather conditions are both fixed. We can assume in Equation 5.2 that weather is statistically independent of the source-term group. Figure 5.11 shows the conditional probability

$\Pr\{\mathrm{CM} \in I_l|\mathrm{STG}_k\}, l = 1, \ldots, m$, reflecting latent cancer-fatality variations due to weather conditions.

Risk Profile

Likelihood L_l (frequency per year) of consequence measure CM falling in interval I_l can be calculated by:

$$L_l \equiv f(\mathrm{CM} \in I_l) = \sum_h \Pr\{\mathrm{CM} \in I_l|\mathrm{IE}_h\} f(\mathrm{IE}_h) \tag{5.3}$$

$$= \sum_{h,i,j,k} f(\mathrm{IE}_h)\Pr\{\mathrm{ASG}_i|\mathrm{IE}_h\}\Pr\{\mathrm{APG}_j|\mathrm{ASG}_i\} \times \Pr\{\mathrm{STG}_k|\mathrm{APG}_j\}\Pr\{\mathrm{CM} \in I_l|\mathrm{STG}_k\} \tag{5.4}$$

A risk profile for consequence measure CM is obtained from pairs $(I_l, L_l), l = 1, \ldots, m$. A large number of risk profiles such as this are generated by uncertainty analysis.

Expected Consequence

Denote by $E(\mathrm{CM}|\mathrm{STG}_k)$ a conditional expected value of consequence measure CM, given source-term group STG_k. This value was calculated by a sample mean of 2500 weather trials. An unconditional expected value $E(\mathrm{CM})$ of consequence measure CM can be calculated by:

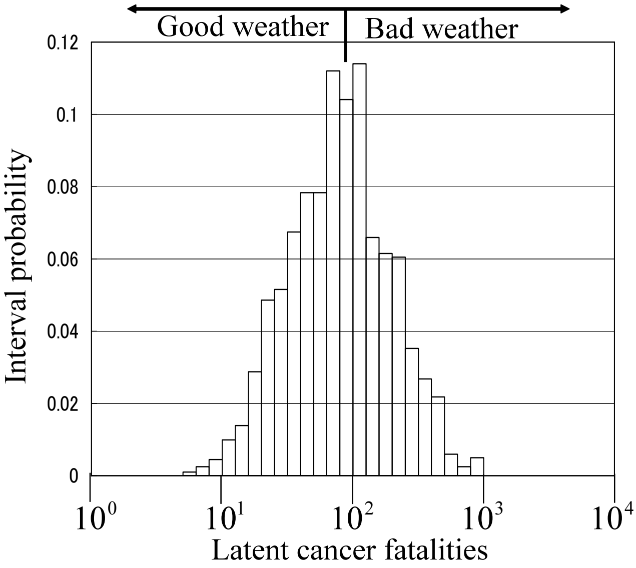


Fig. 5.11. Variation of cancer fatalities by weather, given a source-term group [50]

$$E(\mathrm{CM}) = \sum_{h,i,j,k} f(\mathrm{IE}_h)\Pr\{\mathrm{ASG}_i|\mathrm{IE}_h\}\Pr\{\mathrm{APG}_j|\mathrm{ASG}_i\} \times \Pr\{\mathrm{STG}_k|\mathrm{APG}_j\}E(\mathrm{CM}|\mathrm{STG}_k) \tag{5.5}$$

5.7.2 Level 2 PRA Risk Profile

Release Magnitude

Consider a level 2 PRA dealing with releases of a toxic material. Divide the release magnitude range into small intervals I_l. Denote by $\Pr\{\mathrm{RM} \in I_l|\mathrm{STG}_k\}$ the conditional probability of release magnitude RM falling in interval I_l, given the occurrence of source-term group k. This is a zero–one probability because each source-term group has a unique release magnitude.

Risk Profile

Annual frequency L_l of release magnitude RM falling in interval I_l is calculated in the same way as a consequence-measure likelihood. A risk profile for release magnitude RM is obtained from pairs (I_l, L_l):

$$L_l \equiv f(\mathrm{RM} \in I_l) = \sum_h \Pr\{\mathrm{RM} \in I_l|\mathrm{IE}_h\}f(\mathrm{IE}_h) \tag{5.6}$$

$$= \sum_{h,i,j,k} f(\mathrm{IE}_h)\Pr\{\mathrm{ASG}_i|\mathrm{IE}_h\}\Pr\{\mathrm{APG}_j|\mathrm{ASG}_i\} \times \Pr\{\mathrm{STG}_k|\mathrm{APG}_j\}\Pr\{\mathrm{RM} \in I_l|\mathrm{STG}_k\} \tag{5.7}$$

PRA without Material Hazards

If hazardous materials are not involved, then a level 2 PRA only yields accident-progression groups; source-term analyses need not be performed. On-site consequences are calculated after accident-progression groups are identified.

Consider, for instance, the single-track passenger railway problem. Divide a fatality range into small intervals I_l. Each interval represents a subrange of fatalities, NF. Denote by $\Pr\{\mathrm{NF} \in I_l|\mathrm{APG}_j\}$ the conditional probability of the number of fatalities falling in interval I_l, given the occurrence of accident-progression group j. This is a zero–one probability where each accident-progression group uniquely determines the number of fatalities. The annual frequency L_l of fatality interval I_l is calculated as:

$$L_l \equiv f(\mathrm{NF} \in I_l) = \sum_h \Pr\{\mathrm{NF} \in I_l|\mathrm{IE}_h\}f(\mathrm{IE}_h) \tag{5.8}$$

$$= \sum_{h,i,j} f(\mathrm{IE}_h)\Pr\{\mathrm{ASG}_i|\mathrm{IE}_h\}\Pr\{\mathrm{APG}_j|\mathrm{ASG}_i\} \times \Pr\{\mathrm{NF} \in I_l|\mathrm{APG}_j\} \tag{5.9}$$

A risk profile for the number of fatalities NF is obtained from pairs (I_l, L_l).

5.7.3 Level 1 PRA Risk Profile

A level 1 PRA deals mainly with accident frequencies (*e.g.,* the annual frequency of railway collisions). Denote by $\Pr\{\mathrm{A}|\mathrm{ASG}_i\}$ the conditional probability of accident A, given the occurrence of accident-sequence group i. This is a zero–one probability. Annual frequency L_A of accident A is given by:

$$L_A \equiv f(\mathrm{A}) = \sum_h \Pr\{A|\mathrm{IE}_h\} f(\mathrm{IE}_h) \tag{5.10}$$

$$= \sum_{h,i} f(\mathrm{IE}_h) \Pr\{\mathrm{ASG}_i|\mathrm{IE}_h\} \Pr\{\mathrm{A}|\mathrm{ASG}_i\} \tag{5.11}$$

5.7.4 Uncertainty of Risk Profiles

Likelihood Samples

The accident-frequency analyses, accident-progression analyses, and source-term analyses are performed several hundred times (200 in NUREG-1150) by sampling frequencies and probabilities from failure-data distributions. This yields several hundred combinations of the three analyses. Each sample or observation uniquely determines the following quantities:

1) initiating-event frequency $f(\mathrm{IE}_h)$;
2) accident-sequence group probability $\Pr\{\mathrm{ASG}_i|\mathrm{IE}_h\}$;
3) accident-progression group probability $\Pr\{\mathrm{APG}_j|\mathrm{ASG}_i\}$;
4) source-term group probability $\Pr\{\mathrm{STG}_k|\ \mathrm{APG}_j\}$;
5) consequence probability $\Pr\{\mathrm{CM} \in I_l|\mathrm{STG}_k\}$;

Uncertainty as Distributions

Each observation yields a unique risk profile for a consequence measure, and several hundred risk profiles are obtained by the random sampling. Distribution patterns of these risk profiles indicate uncertainty in the risk profile. Figure 5.12 shows a 95% upper bound, 5% lower bound, mean, and median risk profiles on a logarithmic scale.

Samples of expected consequence $E(\mathrm{CM})$ of consequence measure CM are obtained in a similar way. If conditional expected values $E(\mathrm{CM}|\mathrm{STG}_k)$ obtained from weather trials are used for a fixed source-term group, repetition of time-consuming consequence calculations for weather are avoided as long as an observation during the uncertainty analysis yields the source-term group. Variations of expected consequence $E(\mathrm{CM})$ are depicted in Figure 5.13, which includes 95% upper bound, 5% lower bound, median and mean values.

5.8 Evaluation of Seismic Hazards

We briefly review introductory subjects on seismic-event analysis. Earthquakes have unique aspects that 1) the risk depends on the distance from

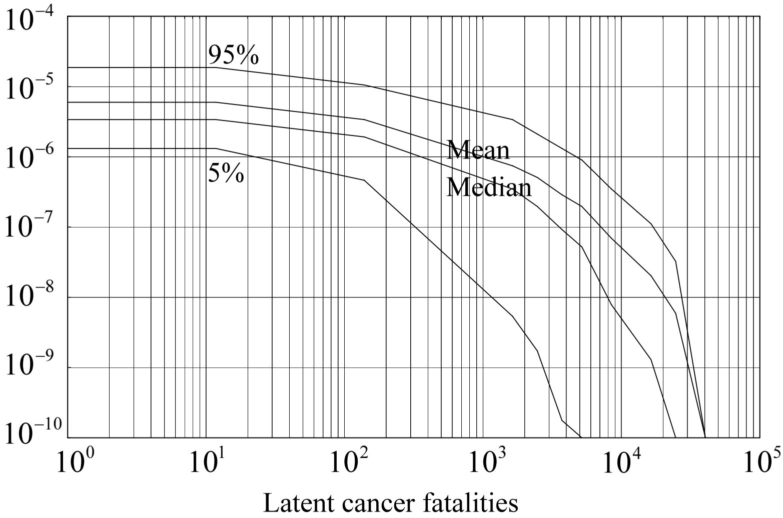


Fig. 5.12. Distribution of latent cancer-fatality risk profiles with upper and lower bounds [50]

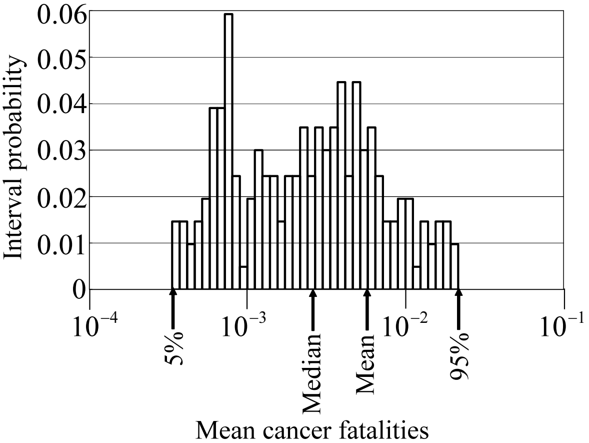


Fig. 5.13. Distribution of mean cancer fatalities [50]

the hazard source, and that 2) it is a typical cause of dependent failures. External events means extreme events such as earthquakes, flood, storm, *etc.* [57]. Fires are traditionally treated as an external event even though these occur inside a plant.

5.8.1 Seismic Hazard Curve

The location of the facility under assessment is called a site. Consider the maximum acceleration A of ground vibration at this site. The seismic hazard

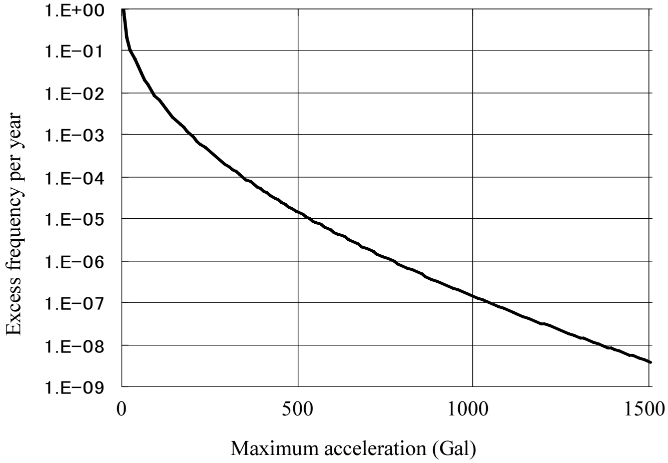


Fig. 5.14. Seismic hazard curve

curve represents the annual frequency that the maximum acceleration A exceeds the value a, *i.e.* excess annual frequency of A. The frequency is usually small enough to be regarded as a probability.

A schematic of the hazard curve is shown in Figure 5.14. The curve can be obtained from 1) the probability distribution of the distance of the epicenter from the site, 2) the probability distribution of the earthquake magnitude, 3) the earthquake frequency, and 4) the attenuation of the acceleration during earthquake propagation.

Probability Density of Epicenter Distance

The continental-drift theory and plate tectonics tell us that earthquakes frequently occur near the boundaries of plates. Earthquakes also occur along active faults. These boundaries and faults are called seismic areas, and we can consider a total of n areas.

The area is not a point location. Thus, we can only predict probabilistically the place of an epicenter, given an earthquake area. Figure 5.15 shows the probability density $f(X|i)$ of the distance between the site and the epicenter, given a seismic area i. This is the density of epicenter-distance distribution.

Probability Density of Earthquake Magnitude

The well-known Gutenberg–Richter law is applicable to earthquakes near plate boundaries. Charles Richter (1900–1985) defined the magnitude of an earthquake as a proportional quantity to the log of the maximum amplitude of the ground motion. Thus, the ground moves 10 000 times more in the magnitude 8 earthquake than in the magnitude 4 earthquake. The energy is proportional

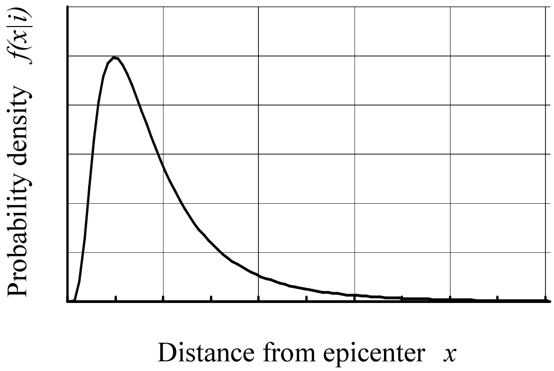


Fig. 5.15. Probability density of distance from epicenter

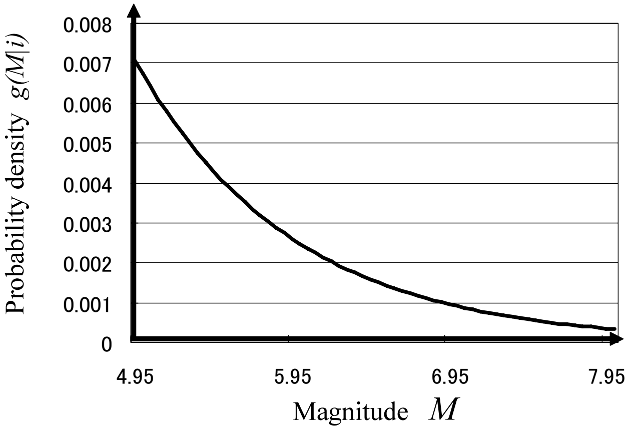


Fig. 5.16. Probability density of earthquakes magnitudes

to the square of the motion amplitude, the magnitude 8 earthquake releases 10^8 times more energy than the magnitude 4 earthquake.

Consider an interval $[M_{\mathrm{L}}, M_{\mathrm{U}}]$ of magnitude M. A typical lower bound M_{L} is 4 or 4.95. Consider the distribution of magnitudes for earthquakes in a seismic area i. The Gutenberg–Richter law states that the frequency N is proportional to 10^{-bM}.

Let the horizontal axis denote magnitude, and the vertical axis the log of probability density $g(M|i)$ of the magnitude, for a given occurrence of earthquakes in seismic area i. Then, the density becomes a straight line with slope $-b$:

$$\log g(M|i) = a - bM \tag{5.12}$$

Constant b can be approximated by 1. Thus, the density decreases to 10% of the original level when the magnitude increases by 1. The density is shown in Figure 5.16 where the vertical axis is an ordinary scale. This is a truncated exponential distribution. The law does not apply to the earthquakes near the active faults, for which other densities are used.

Frequency of Earthquakes

The occurrence frequency of earthquakes in seismic area i is estimated from historical and geological data. Denote by $\Pr\{i\}$ the annual frequency. Again, for the earthquakes of interest, the frequency can be regarded as a probability.

Ground-motion Propagation

This estimates the vibratory ground motion at the site, given the occurrence of an earthquake of magnitude M and distance X. Denote by $h(A|i, X, M)$ the probability density of the maximum ground-motion acceleration, given an earthquake in area i, of distance X, and magnitude M.

Excess Frequency

Suppose that an earthquake occurs in area i. Suppose also that the magnitude is M and distance X. The conditional probability that the maximum acceleration A exceeds value a is:

$$\Pr\{A > a|i, X, M\} = \int_a^\infty h(A|i, X, M)\mathrm{d}A \tag{5.13}$$

Thus, the unconditional frequency that the maximum acceleration exceeds a at the site is:

$$\Pr\{A > a\} = \sum_i \Pr\{i\} \int\int f(X|i)g(M|i)\Pr\{A > a|i, X, M\}\mathrm{d}X\mathrm{d}M \tag{5.14}$$

Similarly, the probability (or frequency) density of the maximum acceleration at the site is:

$$\mathrm{p}\{A\} = \sum_i \Pr\{i\} \int\int f(X|i)g(M|i)h(A|i, X, M)\mathrm{d}X\mathrm{d}M \tag{5.15}$$

5.8.2 Calculation of Damage Probability

The maximum acceleration of a component can be predicted by a probability density $f(R|A)$, given the maximum acceleration A. A lognormal distribution is typically used for the probability density. The component-damage probability can be calculated from the distribution of the component resistance (or fragility), as shown by Equation 6.149. Strong dependencies are accounted for failures of different components because these are subject to the similar accelerations.

Other factors such as the spectral density of acceleration are considered to estimate damage probabilities.

5.9 External Event PRA Standards

ANS published a standard for external events in December 2003 [57, 58]. This standard deals with seismic, high wind, external flood, and other hazards such as aircraft crash and chemical release.

5.10 Concluding Remarks

The PRA has been developed steadily and today its quality is being evaluated by internal and external event standards. Simpler versions of PRA have been used in fields other than nuclear power plants. Full-scale versions will be used in these fields more frequently because the PRA is a place where various risk quantification methods come together to analyze mitigation scenarios triggered by initiating events.

6

Basic Event Quantification

6.1 Introduction

A plant can be decomposed into basic components including hardware and human. Event trees and fault trees contain events related to these basic components. The PRA integrates these events to quantify risks of the plant. The event-tree and fault-tree models facilitate the integration. This chapter describes basic event quantification prior to the integrations.

6.2 What are Basic Events?

Basic events show up as results of ultimate resolutions when a macro event is analyzed into more microscopic events. Statistical data are usually available for the occurrences of the basic events. Switch being stuck closed is a typical basic event. Microscopic human errors such as “failure to observe water level” are regarded as basic events. External events such as earthquakes and floods are sometimes treated as basic events.

The event at the top of a fault tree is called a top event. This is the most macroscopic event to be analyzed further, and ultimately into basic events through intermediate events and logic gates. A pump failing to start is an intermediate event that can be analyzed into “power failure” and “pump hardware failure”.

Component failures are typical basic events. Quantification of risk frequently needs parameters such as unreliability, unavailability, expected number of failures, *etc.* The unreliability is defined as the probability of the first failure up to time t, whereas the unavailability is defined as the probability of a failed component at time t. Complementary parameters are called reliability and availability, respectively. Failed components can be repaired, and the expected number of failures is a typical parameter to represent repair cost.

Basic event quantification becomes more understandable when three processes are introduced: 1) process from repair completion to the first failure,

2) process from failure occurrence to repair completion, and 3) combination of these two processes.

This chapter assumes on–off events. Description can be extended easily to 3 or more valued events such as “normal”, “partial degradation”, and “complete failure”.

For convenience of description, component failures as basic events are considered. The component fails when the basic event occurs, and the component repair is completed when the event disappears. The component being failed corresponds to the basic event existence.

It is intuitively conjectured that reliability, availability, and an expected number of failures are mutually dependent. These relationships are clarified.

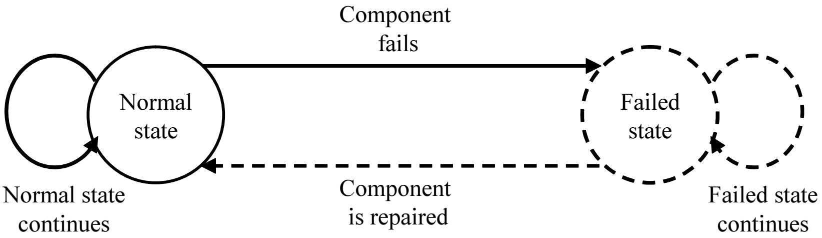


Fig. 6.1. Transition diagram between normal and failed states

6.3 Basic Two-state Transition Diagram

A component is either in a normal state or in a failed state at a given instance of time. A state transition is depicted in Figure 6.1. The component at the initial time $t = 0$ is as good as new. This means that the component enters the normal state at $t = 0$ and has an age of zero. The component stays at the normal state until a component fails and a transition to the failed state occurs.

The component is called nonrepairable when it can not be repaired. The failed component permanently stays at the failed state for the nonrepairable component. On the other hand, a repairable component eventually returns to the normal state when a repair is completed. It is assumed for simplicity that the component is renewed as good as new by the repair. A replacement of failed component by a new one can be regarded as a repair. The assumption of the complete renewal can be relaxed by introducing quasinormal states after the repair.

The state transition occurs instantaneously, and at most one transition occurs during an infinitesimal interval.

6.3.1 Repair-to-failure Process Parameters

Consider a process depicted by a solid line and a solid curve. The component stays for some time at a normal state, and then transits to the failed state. The transition means death for a human.

Reliability $R(t)$
Consider a component that jumped into the normal state at time $t = 0$. Define the following two events:

$$N_{[0,t]} = \text{the component has been normal up to time } t \tag{6.1}$$

$$N_0 = \text{the component was repaired at time zero} \tag{6.2}$$

Symbol N stands for a normal component, while suffix $[0, t]$ is the time interval where the component remains normal. Suffix 0 denotes the renewal that takes place at the initial time. Reliability $R(t)$ at time t is defined by the conditional probability:

$$R(t) = \Pr\{N_{[0,t]}|N_0\} \tag{6.3}$$

In other words, the reliability is the probability that the component experiences no failure during the time interval $[0, t]$, given that the component was normal at time zero. The conditional probability is approximately the number of normal components over interval $[0, t]$ divided by the number of components repaired at time zero. The components are restricted to those satisfying the condition N_0.

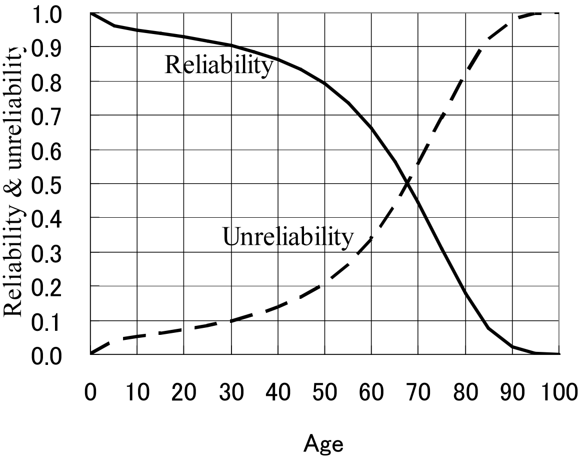


Fig. 6.2. Reliability and unreliability of human

Consider the human-longevity data in Table 6.1. The corresponding human reliability is plotted in Figure 6.2.

Table 6.1. Example of human-longevity statistics

	L	R	F	K	f	$r = f/R$
Age	Survivors	Reliability	Unreliability	Fatalities	Failure density	Failure rate
0	1 023 102	1.000	0.000	39 285	0.0077	0.0077
5	983 817	0.962	0.038	12 013	0.0023	0.0024
10	971 804	0.950	0.050	9,534	0.0019	0.0020
15	962 270	0.941	0.059	10 787	0.0021	0.0022
20	951 483	0.930	0.070	12 286	0.0024	0.0026
25	939 197	0.918	0.082	14 588	0.0029	0.0031
30	924 609	0.904	0.096	18 055	0.0035	0.0039
35	906 554	0.886	0.114	23 212	0.0045	0.0051
40	883 342	0.863	0.137	30 788	0.0060	0.0070
45	852 554	0.833	0.167	41 654	0.0081	0.0098
50	810 900	0.793	0.207	56 709	0.0111	0.0140
55	754 191	0.737	0.263	76 420	0.0149	0.0203
60	677 771	0.662	0.338	99 949	0.0195	0.0295
65	577 822	0.565	0.435	123 274	0.0241	0.0427
70	454 548	0.444	0.556	138 566	0.0271	0.0610
75	315 982	0.309	0.691	134 217	0.0262	0.0850
80	181 765	0.178	0.822	103 544	0.0202	0.1139
85	78 221	0.076	0.924	56 644	0.0111	0.1448
90	21 577	0.021	0.979	18 566	0.0036	0.1721
95	3011	0.003	0.997	3011	0.0006	0.2000
100	0	0.000	1.000	0	0.0000	

Unreliability $F(t)$
Complement $\bar{N}_{[0,t]}$ of event $N_{[0,t]}$ can be expressed as:

$$\bar{N}_{[0,t]} = \text{the first failure occurs during the time interval } [0,t] \tag{6.4}$$

Unreliability $F(t)$ is defined by:

$$F(t) = \Pr\{\bar{N}_{[0,t]} | N_0\} \tag{6.5}$$

In other words, the unreliability is the probability of the first failure up to time t. This is called a failure distribution. Human unreliability is depicted by a dotted curve in 6.2. The unreliability is the complement of the reliability:

$$R(t) + F(t) = 1 \tag{6.6}$$

Difference $F(b) - F(a)$, $a < b$ is the probability of the first failure during interval $[a, b]$. There is no difference between two interval notations $[a, b]$ and $(a, b]$ for continuous failure distribution.

Failure Density $f(t)$
Failure density $f(t)$ is a derivative of the failure distribution $F(t)$:

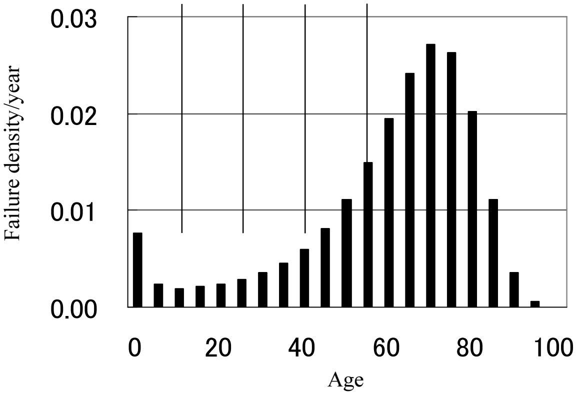


Fig. 6.3. Failure density of human

$$f(t) = \frac{\mathrm{d}F(t)}{\mathrm{d}t} \tag{6.7}$$

Quantity $f(t)\mathrm{d}t$ is the probability $\mathrm{d}F(t)$ of the first failure during an infinitesimal interval $[t, t + \mathrm{d}t]$, given condition N_0:

$$f(t)\mathrm{d}t = F(t + \mathrm{d}t) - F(t) \equiv \mathrm{d}F(t) \tag{6.8}$$

Human failure density is shown in Figure 6.3. We observe that people in that population die most frequently between ages 70 and 75.

Equivalently, the unreliability can be expressed as an integral of the failure density:

$$F(t) = \int_0^t f(u)\mathrm{d}u \tag{6.9}$$

Similarly, difference $F(\infty) - F(t) = 1 - F(t)$ is reliability $R(t)$. In other words, reliability $R(t)$ is an integral of the failure density over interval $[t, \infty]$:

$$R(t) = \int_t^\infty f(u)\mathrm{d}u \tag{6.10}$$

Failure Rate $r(t)$

Define event $\bar{N}_{[t,t+\mathrm{d}t]}$ as the occurrence of failure during an infinitesimal interval $[t, t + \mathrm{d}t]$. Denote by $r(t)$ the failure rate at time t. Then, the quantity $r(t)\mathrm{d}t$ is defined as follows:

$$r(t)\mathrm{d}t = \Pr\{\bar{N}_{[t,t+\mathrm{d}t]} | N_0, N_{[0,t]}\} \tag{6.11}$$

We should note here the two conditions: 1) N_0: the component was repaired at time zero, and 2) $N_{[0,t]}$: the component has been normal up to time t.

The probability during infinitesimal interval $[t, t + \mathrm{d}t]$ is calculated as $r(t)$ multiplied by $\mathrm{d}t$. Therefore, $r(t)$ is described as the "failure probability per unit time", given that the component is normal to time t.

Human failure rate is shown in Figure 6.4. The rate decreases after the birth, then remains constant between ages 10 and 20, and monotonically increases thereafter. A sharp increase is observed after age 40. This type of curve is known as a bathtub curve.

The decrease of the rate up to age 5 is an example of early failures, while the sharp increase after 40 is called a wearout failure. The failures with the relatively constant failure rate are called random failures. As we will see later, the constant rate means that the expected number of failures during unit time interval remains constant when the failed component is renewed instantly, thus the term random failure. The constant rate also implies a memoryless component that is as good as new when it is normal; such a component is not subject to accumulation of fatigue or memory.

The human early failure rate is magnified in Figure 6.5. Defects of production are major causes of early failures of industrial products. The wearout failures are due to deterioration by aging.

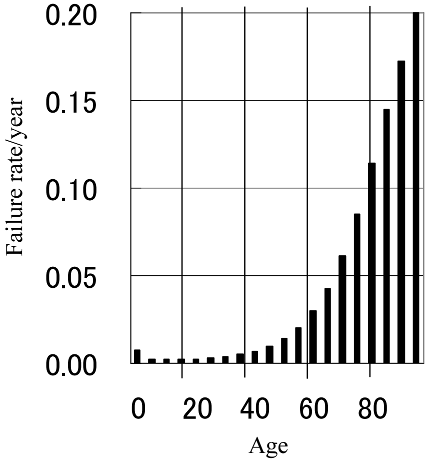


Fig. 6.4. Failure rate of human

Mean Time to Failure: MTTF

Denote by TTF (time to failure) a life span of a component, given that the component jumps into the normal state at time 0. This is a random variable. The expected value of TTF is called a mean time to failure, MTTF:

$$\mathrm{MTTF} = \int_0^\infty t f(t) \mathrm{d}t \tag{6.12}$$

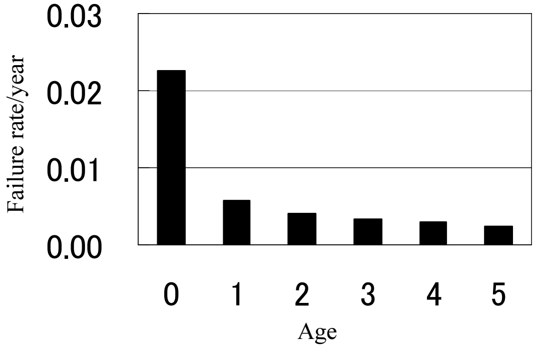


Fig. 6.5. Early failure rate of human

Term $f(t)\mathrm{d}t$ is the probability that the TTF falls in interval $[t, t+\mathrm{d}t]$, and hence the TTF can be regarded as t. The above integral yields the average of TTFs. It turns out that the average longevity of humans in Figure 6.3 is 62.4.

It is well known that the MTTF can be calculated as an integral of reliability $R(t)$:

$$\mathrm{MTTF} = \int_0^\infty R(t)\mathrm{d}t, \text{ if } tR(t) \to 0 \text{ as } t \to \infty \tag{6.13}$$

This can be shown by an integration by parts. Equation 6.13 is usually easier to use than Equation 6.12 that includes the additional variable t.

Suppose that the component has been normal up to time u. The remaining span of life is also a random variable, and its average is called a mean residual time to failure, MRTTF, which is calculated by:

$$\mathrm{MRTTF} = \int_u^\infty \frac{(t-u)f(t)}{R(u)}\mathrm{d}t \tag{6.14}$$

Here, denominator $R(u)$ is a normalization factor for $f(t)$, $u \le t < \infty$.

6.3.2 Failure-to-repair Process Parameters

Consider the process denoted by the broken line and the curve in Figure 6.1. The component stays at the failed state, and then returns to the normal state when the repair is completed. Shift the time axis so that the component jumps into the failed state at time $t = 0$.

Nonrepairability $\bar{G}(t)$

The nonrapairability is an uncommon terminology corresponding to the reverse side of reliability. Define event symbols by:

$$F_{[0,t]} = \text{the component continues to be failed up to time } t \tag{6.15}$$

$$F_0 = \text{the component fails at time zero} \tag{6.16}$$

Symbol “F” stands for failure, and suffix 0 the initial time. The nonrepairability $\bar{G}(t)$ can be written as:

$$\bar{G}(t) = \Pr\{F_{[0,t]}|F_0\} \tag{6.17}$$

Repairability $G(t)$

Repairability $G(t)$ is frequently called a repair distribution. This is the reverse side of unreliability or the failure distribution $F(t)$:

$$G(t) = \Pr\{\bar{F}_{[0,t]}|F_0\} = 1 - \bar{G}(t) \tag{6.18}$$

where complementary event $\bar{F}_{[0,t]}$ to $F_{[0,t]}$ is defined by:

$$\bar{F}_{[0,t]} = \text{the component is repaired during } [0,t] \tag{6.19}$$

Repair Density g(t)

This is the first derivative of the repair distribution:

$$g(t) = \frac{\mathrm{d}G(t)}{\mathrm{d}t} \tag{6.20}$$

or

$$g(t)\mathrm{d}t = G(t + \mathrm{d}t) - G(t) \equiv \mathrm{d}G(t) \tag{6.21}$$

On the contrary, the repair distribution can be obtained from the repair density:

$$G(t) = \int_0^t g(u)\mathrm{d}u \tag{6.22}$$

$$G(b) - G(a) = \int_a^b g(u)\mathrm{d}u,\ a < b \tag{6.23}$$

Difference $G(b) - G(a)$ is the probability of repair completion during interval $[a,b]$

Repair Rate $m(t)$

Quantity $m(t)\mathrm{d}t$ is defined by:

$$m(t)\mathrm{d}t = \Pr\{\bar{F}_{[t,t+\mathrm{d}t]}|F_0, F_{[0,t]}\} \tag{6.24}$$

where $\bar{F}_{[t,t+\mathrm{d}t]}$ is the probability of repair completion in interval $[t, t + \mathrm{d}t]$. Note that the condition $F_{[0,t]}$ indicates the continuation of the failed state up to time t. The repair rate $m(t)$ is described as the “repair probability per unit time”. The rate is zero when the component is nonrepairable, and is not subject to repair.

Mean Time to Repair: MTTR

Denote by TTR the time to repair. This consists of 1) time to detect the failure, 2) transport time to the repair shop, 3) time to repair the component, 4) transport time back to the plant, 5) assembly time into the plant, *etc.* (see also Section 3.7.2). A replacement is a repair. The TTR is a random variable, and its average is called the MTTR:

$$\text{MTTR} = \int_0^\infty t g(t)\mathrm{d}t \tag{6.25}$$

$$\text{MTTR} = \int_0^\infty \bar{G}(t)\mathrm{d}t, \text{ if } t\bar{G}(t) \to 0 \text{ as } t \to \infty \tag{6.26}$$

The MTTR is frequently used as a simplified measure of maintainability. Regular surveillance or diagnostic test of a component yields a smaller MTTR.

6.3.3 Combined Process Parameters

Consider a process obtained by combining the solid and broken line processes in Figure 6.1. Assume initial condition N_0, which means that the component jumps into the normal state at time zero. Failures and subsequent repairs are repeated when the component is repairable. The combined process reduces to the repair-to-failure process when the component is nonrepairable.

Availability $A(t)$

Define an index variable $x(t)$ by:

$$x(t) = \begin{cases} 1, & \text{if component is in normal state} \\ 0, & \text{if component is in failed state} \end{cases} \tag{6.27}$$

The availability is given by:

$$A(t) = \Pr\{x(t) = 0|N_0\} \tag{6.28}$$

This is the probability of a normal state at an instant of time, not over an interval. The next inequality holds because the failed component may be repaired:

$$A(t) \geq R(t) \tag{6.29}$$

The equality holds for the nonrepairable component.

The availability of the nonrepairable component monotonically decreases to zero as time goes to infinity. For the repairable component, the availability converges to a steady-state value.

Unavailability $Q(t)$

$$Q(t) = \Pr\{x(t) = 1|N_0\} = 1 - A(t) \tag{6.30}$$

Inequality

$$Q(t) \leq F(t) \tag{6.31}$$

holds, where equality holds for the nonrepairable component.

Failure Intensity $w(t)$

$$w(t)\mathrm{d}t = \Pr\{\bar{N}_{[t,t+\mathrm{d}t]}|N_0\} \tag{6.32}$$

Condition $N_{[0,t]}$ is removed from the definition of failure rate $r(t)$ of Equation 6.11. For the nonrepairable component, the failure intensity reduces to the failure density $f(t)$:

$$w(t) = f(t) \text{ for nonrepairable component} \tag{6.33}$$

Expected Number of Failures $W(a, b)$

Denote by $W(t, t+\mathrm{d}t)$ the expected number of failures (ENF) during interval $[t, t + \mathrm{d}t]$. Definition of the expected value yields:

$$W(t, t + \mathrm{d}t) = \sum_{i=1}^{\infty} i \times \Pr\{i \text{ failures in } [t, t + \mathrm{d}t]|N_0\} \tag{6.34}$$

At most one failure occurs in the infinitesimal interval $[t, t + \mathrm{d}t]$, and we set $i = 1$ in Equation 6.34:

$$W(t, t + \mathrm{d}t) = \Pr\{\text{one failure in } [t, t + \mathrm{d}t]|N_0\} \tag{6.35}$$

In other words, the ENF is equal to $w(t)\mathrm{d}t$ of Equation 6.32:

$$W(t, t + \mathrm{d}t) = w(t)\mathrm{d}t \tag{6.36}$$

Failure intensity $w(t)$ turns out to be the expected number of failures per unit time at time t.

The ENF over interval $[a, b]$ is denoted by $W(a, b)$:

$$W(a, b) = \int_a^b w(t)\mathrm{d}t \tag{6.37}$$

For the nonrepairable component, ENF $W(0, t)$ equals the failure distribution:

$$W(0, t) = F(t), \text{ for nonrepairable component} \tag{6.38}$$

The ENF monotonically increases for the repairable component.

Repair Intensity $v(t)$

$$v(t)\mathrm{d}t = \Pr\{\bar{F}_{[t,t+\mathrm{d}t]}|N_0\} \tag{6.39}$$

Condition N_0 replaces $F_{[0,t]}$ and F_0 in the definition of repair rate $m(t)$ of Equation 6.24. For the nonrepairable component, the repair intensity reduces to zero:

$$v(t) = 0 \text{ for nonrepairable component} \tag{6.40}$$

Expected Number of Repairs $V(a,b)$
Denote by $V(t,t+\mathrm{d}t)$ the expected number of repairs (ENR) during interval $[t,t+\mathrm{d}t]$:

$$V(t,t+\mathrm{d}t) = v(t)\mathrm{d}t \tag{6.41}$$

Repair intensity $v(t)$ turns out to be the expected number of repairs per unit time at time t.

The ENR over interval $[a,b]$ is denoted by $V(a,b)$:

$$V(a,b) = \int_a^b v(t)\mathrm{d}t \tag{6.42}$$

The ENR monotonically increases for the repairable component. We will see that the difference $W(0,t) - V(0,t)$ is equal to the unavailability $Q(t)$.

6.4 Relations between Reliability Parameters

6.4.1 Process up to Failure Occurrence

The following relations hold:

$$r(t) = \frac{f(t)}{1-F(t)} = \frac{f(t)}{R(t)} \tag{6.43}$$

$$F(t) = 1 - \exp\Big(-\int_0^t r(u)\mathrm{d}u\Big) \tag{6.44}$$

$$R(t) = \exp\Big(-\int_0^t r(u)\mathrm{d}u\Big) \tag{6.45}$$

$$f(t) = r(t)\exp\Big(-\int_0^t r(u)\mathrm{d}u\Big) \tag{6.46}$$

Equations 6.45 and 6.46 can easily be derived from Equation 6.44. Equation 6.43 is simply the definition of the conditional probability:

$$r(t)\mathrm{d}t = \Pr\{\bar{N}_{[t,t+\mathrm{d}t]}|N_0, N_{[0,t]}\} = \frac{\Pr\{\bar{N}_{[t,t+\mathrm{d}t]}, N_{[0,t]}|N_0\}}{\Pr\{N_{[0,t]}|N_0\}} = \frac{f(t)}{R(t)}\mathrm{d}t \tag{6.47}$$

The failure rate is sometimes called a hazard rate. The integral of hazard rate $r(t)$ is called a cumulative hazard function [35].

Equation 6.43 can be written as:

$$r(t) = \frac{\mathrm{d}F(t)/\mathrm{d}t}{1-F(t)} = -\frac{\mathrm{d}}{\mathrm{d}t}\ln[1-F(t)] \tag{6.48}$$

This yields Equation 6.44 by noting $F(0) = 0$.

The other three parameters can be determined from the remaining parameter. As an example, consider the following failure density:

$$f(t) = \begin{cases} t/2, & 0 \le t < 2 \\ 0, & 2 \le t \end{cases} \tag{6.49}$$

Failure distribution $F(t)$, reliability $R(t)$ and failure rate $r(t)$ are determined as:

$$F(t) = \begin{cases} t^2/4, & 0 \le t < 2 \\ 1, & 2 \le t \end{cases} \tag{6.50}$$

$$R(t) = 1 - F(t) = \begin{cases} 1 - (t^2/4), & 0 \le t < 2 \\ 0, & 2 \le t \end{cases} \tag{6.51}$$

$$r(t) = f(t)/R(t) = \begin{cases} \dfrac{t/2}{1 - (t^2/4)}, & 0 \le t < 2 \\ \text{not defined}, & 2 \le t \end{cases} \tag{6.52}$$

The MTTF is:

$$\text{MTTF} = \int_0^2 t f(t) \mathrm{d}t = \int_0^2 (t^2/2) \mathrm{d}t = 4/3 \tag{6.53}$$

This coincides with an alternative calculation:

$$\text{MTTF} = \int_0^2 R(t) \mathrm{d}t = \int_0^2 [1 - (t^2/4)] \mathrm{d}t = 4/3 \tag{6.54}$$

6.4.2 Process up to Repair Completion

Any set of three parameters can be calculated from the remaining parameter:

$$m(t) = \frac{g(t)}{1 - G(t)} = \frac{g(t)}{\bar{G}(t)} \tag{6.55}$$

$$G(t) = 1 - \exp\Big(- \int_0^t m(u) \mathrm{d}u \Big) \tag{6.56}$$

$$\bar{G}(t) = \exp\Big(- \int_0^t m(u) \mathrm{d}u \Big) \tag{6.57}$$

$$g(t) = m(t) \exp\Big(- \int_0^t m(u) \mathrm{d}u \Big) \tag{6.58}$$

6.4.3 Combined Process

Failure Intensity $w(t)$ and Repair Intensity $v(t)$
Consider a failure during the infinitesimal time interval $[t, t + \mathrm{d}t]$. Figure 6.6 yields the following equation:

$$w(t) \mathrm{d}t = f(t) \mathrm{d}t + \mathrm{d}t \int_0^t f(t - u) v(u) \mathrm{d}u \tag{6.59}$$

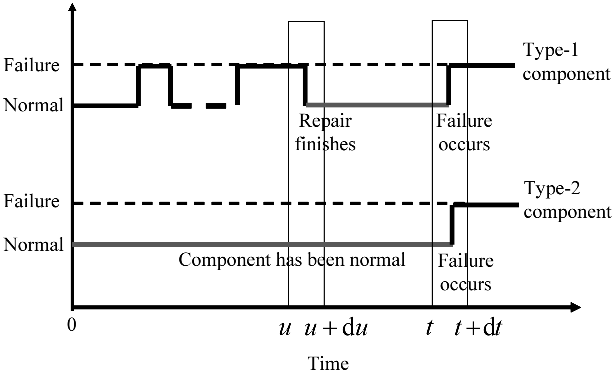


Fig. 6.6. Occurrence of failure during small time interval $[t, t + \mathrm{d}t]$

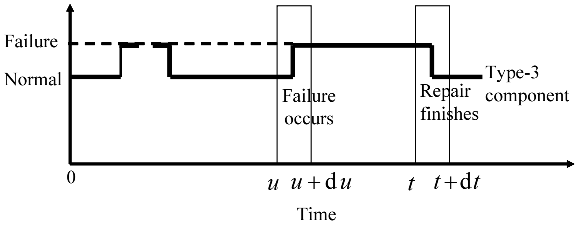


Fig. 6.7. Occurrence of repair completion during small time interval $[t, t + \mathrm{d}t]$

The first term on the rhs of this equation is the contribution to $w(t)\mathrm{d}t$ by the type-2 component, while the second integral is that of the type-1 component in Figure 6.6. Dividing both sides of the above equation by $\mathrm{d}t$ yields:

$$w(t) = f(t) + \int_0^t f(t-u)v(u)\mathrm{d}u \tag{6.60}$$

Consider next a repair completion during interval $[t, t + \mathrm{d}t]$. Only the type-3 component is feasible in Figure 6.7 because of the initial condition N_0. The component yields an equation similar to Equation 6.60, and these two equations can be written as:

$$\left.\begin{aligned} w(t) &= f(t) + \int_0^t f(t-u)v(u)\mathrm{d}u \\ v(t) &= \int_0^t g(t-u)w(u)\mathrm{d}u \end{aligned}\right\} \tag{6.61}$$

Failure intensity $w(t)$ and repair intensity $v(t)$ are obtained by solving the above integral equation, given failure density $f(t)$ and repair density $g(t)$.

Consider, for instance, a nonrepairable component. The identity $g(t) \equiv 0$ simplifies the integral equation into:

$$\left.\begin{aligned} w(t) &= f(t) \\ v(t) &= 0 \end{aligned}\right\} \tag{6.62}$$

Thus, we confirm that the failure intensity of the combined process equals the failure density of the repair-to-failure process.

Consider next an instantaneous repair. The repair distribution $g(t) = \delta(t)$, as a delta function rewrites the integral equation into:

$$\left.\begin{aligned} w(t) &= f(t) + \int_0^t f(t-u)v(u)\mathrm{d}u \\ v(t) &= w(t) \end{aligned}\right\} \tag{6.63}$$

Thus, only the failure intensity remains as an unknown function to be solved.

Unavailability $Q(t)$
Denote by $x_{0,1}$ and $x_{1,0}$ the number of failures and the number of repairs until time t, respectively. The variable $x(t)$ of Equation 6.27 can be expressed as:

$$x(t) = x_{0,1}(t) - x_{1,0}(t) \tag{6.64}$$

Consider, for instance, the case of 3 failures and 2 repairs. The component state is given by:

$$x(t) = 3 - 2 = 1 \tag{6.65}$$

The probability of the zero–one variable taking the value of unity is equal to the expected value of the variable. Thus, taking the expected value of both sides of Equation 6.64 gives:

$$Q(t) = W(0,t) - V(0,t) \tag{6.66}$$

In other words, the availability is the expected number of failures minus the expected number of repairs. These numbers are obtained from failure intensity and repair intensity:

$$Q(t) = \int_0^t [w(u) - v(u)]\mathrm{d}u \tag{6.67}$$

6.5 Constant Failure and Repair Rate Model

6.5.1 Process up to Failure Occurrence

The failure rate may be regarded as a constant after the early failure and before the wearout failure as shown by the human failure-rate data of Figure 6.4. Solid-state electronic components may fail with the constant failure rates, while analog or mechanical components fail with increasing failure rates because of deteriorations with time.

As a convention, the constant failure rate $r(t) = r$ is usually denoted by $r(t) = \lambda$. Equations 6.44 to 6.46 directly give the following formulas:

$$F(t) = 1 - \mathrm{e}^{-\lambda t} \tag{6.68}$$

$$R(t) = \mathrm{e}^{-\lambda t} \tag{6.69}$$

$$f(t) = \lambda \mathrm{e}^{-\lambda t} \tag{6.70}$$

Equation 6.68 is called an "exponential distribution". Its MTTF is the mean of the distribution and is given by the reciprocal of the constant failure rate λ:

$$\mathrm{MTTF} = \int_0^\infty t\lambda \mathrm{e}^{-\lambda t} \mathrm{d}t = \frac{1}{\lambda} \tag{6.71}$$

The MTTF can also be calculated by Equation 6.13:

$$\mathrm{MTTF} = \int_0^\infty \mathrm{e}^{-\lambda t} \mathrm{d}t = \frac{1}{\lambda} \tag{6.72}$$

Equation 6.14 yields the mean residual time to failure at age u:

$$\mathrm{MRTTF} = \int_u^\infty (t-u)\lambda \mathrm{e}^{-\lambda(t-u)} \mathrm{d}t = \int_0^\infty t\lambda \mathrm{e}^{-\lambda t} \mathrm{d}t = \frac{1}{\lambda} \tag{6.73}$$

The MRTTF becomes a constant $1/\lambda$ that does not depend on age u. The exponential distribution component is as good as new whenever it is normal. No accumulation of wear occurs for the constant-failure-rate component. The component is called memoryless.

The exponential distribution profile is shown in Figure 6.8. The tangential line at the origin horizontally moves by MTTF when it vertically moves by unity. The curve can be shaped by chamfering the corner "C" shown in the figure. About 63.2% and 86.5% of the components fail up to MTTF and 2×MTTF:

$$F(\mathrm{MTTF}) = 0.632,\ F(2 \times \mathrm{MTTF}) = 0.865 \tag{6.74}$$

6.5.2 Process up to Repair Completion

Constant repair rate $m(t) = m$ is denoted by μ by convention. Similarly to the failure occurrence, we have for repair completion the following equations:

$$G(t) = 1 - \mathrm{e}^{-\mu t} \tag{6.75}$$

$$\bar{G}(t) = \mathrm{e}^{-\mu t} \tag{6.76}$$

$$g(t) = \mu \mathrm{e}^{-\mu t} \tag{6.77}$$

$$\mathrm{MTTR} = \frac{1}{\mu} \tag{6.78}$$

$$G(\mathrm{MTTR}) = 0.632,\ G(2 \times \mathrm{MTTR}) = 0.865 \tag{6.79}$$

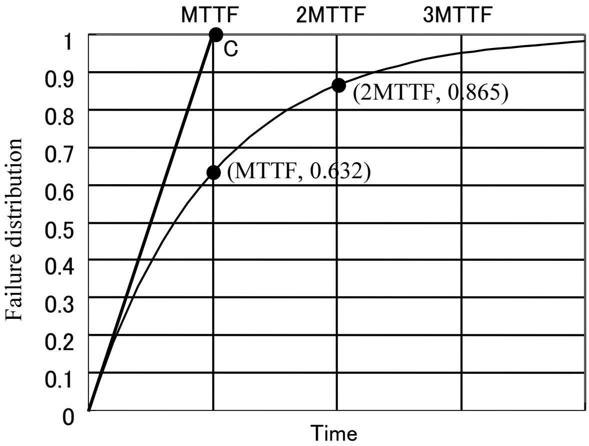


Fig. 6.8. Properties of exponential distribution

6.5.3 Combined Process

It turns out that the following failure intensity $w(t)$ and repair intensity $v(t)$ satisfy Equation 6.61:

$$w(t) = \frac{\lambda\mu}{\lambda+\mu} + \frac{\lambda^2}{\lambda+\mu}\mathrm{e}^{-(\lambda+\mu)t} \tag{6.80}$$

$$v(t) = \frac{\lambda\mu}{\lambda+\mu} - \frac{\lambda\mu}{\lambda+\mu}\mathrm{e}^{-(\lambda+\mu)t} \tag{6.81}$$

The ENF $W(0,t)$ and ENR $V(0,t)$ can be obtained as integrals of $w(t)$ and $v(t)$, respectively:

$$W(0,t) = \frac{\lambda\mu}{\lambda+\mu}t + \frac{\lambda^2}{(\lambda+\mu)^2}\left[1 - \mathrm{e}^{-(\lambda+\mu)t}\right] \tag{6.82}$$

$$V(0,t) = \frac{\lambda\mu}{\lambda+\mu}t - \frac{\lambda\mu}{(\lambda+\mu)^2}\left[1 - \mathrm{e}^{-(\lambda+\mu)t}\right] \tag{6.83}$$

Unavailability $Q(t)$ is a difference of $W(0,t)$ and $V(0,t)$:

$$Q(t) = W(0,t) - V(0,t) = \frac{\lambda}{\lambda+\mu}\left[1 - \mathrm{e}^{-(\lambda+\mu)t}\right] \tag{6.84}$$

$$A(t) = 1 - Q(t) = \frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu}\mathrm{e}^{-(\lambda+\mu)t} \tag{6.85}$$

Steady-state values of unavailability and availability become:

$$Q(\infty) = \frac{\lambda}{\lambda+\mu} = \frac{1/\mu}{(1/\lambda)+(1/\mu)} = \frac{\mathrm{MTTR}}{\mathrm{MTTF}+\mathrm{MTTR}} \tag{6.86}$$

$$A(\infty) = \frac{\mu}{\lambda+\mu} = \frac{1/\lambda}{(1/\lambda)+(1/\mu)} = \frac{\mathrm{MTTF}}{\mathrm{MTTF}+\mathrm{MTTR}} \tag{6.87}$$

The ratios of the value at time t to steady-state values are:

$$\frac{Q(t)}{Q(\infty)} = 1 - \mathrm{e}^{-t/T}, \ T \equiv \frac{1}{\lambda + \mu} \tag{6.88}$$

Therefore, 86.5% is attained at time $2T = 2/(\lambda + \mu)$. The MTTR is usually sufficiently smaller than MTTF. In other words, $\lambda \ll \mu$. Thus, time T can be approximated by MTTR:

$$T \simeq \frac{1}{\mu} = \mathrm{MTTR} \tag{6.89}$$

Repair rate μ is zero for the nonrepairable component. Thus, the failure intensity $w(t)$ of Equation 6.80 becomes equal to the failure density $f(t)$:

$$w(t) = \lambda \mathrm{e}^{-\lambda t} = f(t) \tag{6.90}$$

Example: Power-source Unreliability and Unavailability
Consider an electric power failure event. Assume MTTF = 0.5 (year) and MTTR = 30 min. Reliability $R(t)$ and unavailability $Q(t)$ at $t = 1$ year can be obtained in the following way:

$$\mathrm{MTTR} = \frac{30}{365 \times 24 \times 60} = 5.71 \times 10^{-5} \text{ year} \tag{6.91}$$

$$\lambda = 1/0.5 = 2/\text{year}, \ \ \mu = 1/\mathrm{MTTR} = 17\ 500/\text{year} \tag{6.92}$$

$$R(1) = \mathrm{e}^{-2\times 1} = 0.135 \tag{6.93}$$

$$Q(1) = \frac{2}{2 + 17\ 500}\left[1 - \mathrm{e}^{-(2+17\ 500)\times 1}\right] = 1.14 \times 10^{-4} \tag{6.94}$$

Note that the unavailability is far smaller than the unreliability of $F(t) = 1 - R(t) = 0.865$

Primary and Secondary Failures
Primary failure is the failure under normal conditions. Other failures due to exceptional factors such as earthquakes are called secondary failure.

Suppose that the earthquakes occur once per 60 years on average. A tank is destroyed with a probability of 50% by the earthquakes. The tank primary failures under normal conditions occur with a MTTF of 30 years. Assume a tank MTTR of 0.1 years. The reliability and unavailability of the tank after ten years of operation become:

$$\text{Primary failure rate } \lambda_{\mathrm{P}} = 1/30 = 3.33 \times 10^{-2}/\text{year} \tag{6.95}$$

$$\text{Secondary failure rate } \lambda_{\mathrm{S}} = 1/120 = 8.33 \times 10^{-3}/\text{year} \tag{6.96}$$

$$\text{Total failure rate } \lambda = \lambda_{\mathrm{P}} + \lambda_{\mathrm{S}} = 4.163 \times 10^{-2}/\text{year} \tag{6.97}$$

$$\text{Repair rate } \mu = 1/0.1 = 10/\text{year} \tag{6.98}$$

$$\text{Reliability } R(10) = \mathrm{e}^{-0.04163\times 10} = 0.659 \tag{6.99}$$

$$\text{Unavailability } Q(10) = \frac{0.04163}{0.04163 + 10}\left[1 - \mathrm{e}^{-(0.04163+10)\times 10}\right] = 4.15 \times 10^{-3} \tag{6.100}$$

6.5.4 Instantaneous Repair and Poisson Process

For the instantaneous repair, the repair rate is infinity. Thus, from $\mu = \infty$ in Equation 6.80, we have:

$$w(t) = \lambda, \ \ W(0,t) = \lambda t \tag{6.101}$$

In other words, the failure intensity equals to the failure rate. This is reasonable because the failure intensity $w(t)$ is the expected number of failures per unit time at time t. Suppose that the next failure occurs after $1/\lambda$ h in average. Then, the failures occur at the frequency of λ per h. The ENF is proportional to time t.

Figure 6.9 shows a transition diagram of a component subject to the instantaneous repair. Denote by $X(t)$ the state of the component. This is the number of failures during time interval [0,t], given that the component is at state 0 at time zero. The probability of x failures up to time t is given by a Poisson distribution.

$$\Pr\{X(t) = x\} = \frac{\mathrm{e}^{-\lambda t}(\lambda t)^x}{x!} \equiv \mathrm{Poisson}^*(x; \lambda, t), \ \ x = 0, 1, 2, \ldots, \tag{6.102}$$

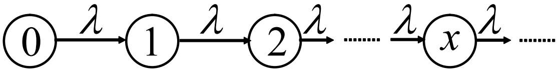


Fig. 6.9. Transition diagram of Poisson process

6.5.5 Fractional Time Availability

Availability $A(t)$ is the probability that a component is normal at time t. Assume a sufficiently large population. Then, the availability is the ratio of the number of normal components at time t divided by the total number of components. This can be regarded as a population average when 1 and 0 values are allocated to the normal and failed components, respectively.

Consider a particular component. Availability can also be defined as a time that the component is capable of performing its intended function divided by the total time that the intended function may be demanded. Consider a total of N pairs of TTF and TTR observed for the component:

$$(\mathrm{TTF}_i, \ \mathrm{TTR}_i), \ i = 1, \ldots, N \tag{6.103}$$

The fractional time availability can be written as:

$$\widetilde{A} = \frac{\sum_{i=1}^{N} \mathrm{TTF}_i}{\sum_{i=1}^{N} [\mathrm{TTF}_i + \mathrm{TTR}_i]} \tag{6.104}$$

Table 6.2. Time to failure data for germanium transistors

Time to failure (day)	Sum of failures
0	0
20	9
40	23
60	50
90	83
160	113
230	143
400	160
900	220
1200	235
2500	240
∞	250

Divide the numerator and the denominator of the above equation by sufficiently large N. Then, the numerator becomes MTTF and the denominator MTTF+MTTR:

$$\widetilde{A} = \frac{\mathrm{MTTF}}{\mathrm{MTTF} + \mathrm{MTTR}} \tag{6.105}$$

Suppose that the component is picked up randomly and thus it can represent the population. Then, MTTF and MTTR become those of the population and the availability of Equation 6.105 coincides with the steady-state availability $A(\infty)$ of Equation 6.87 for the exponential distribution. Such a coincidence of time average with the population average is observed for most distributions.

6.6 Estimation of Distribution Parameters

The TTF is a random variable. Figure 6.3 is based on about one million samples of the TTF values. It is impossible to depict an accurate failure density curve if the simple size is small. Fortunately, parameter estimation is possible for the small number of samples.

6.6.1 Exponential Distribution and Random Failure

Assume an exponential distribution. Reliability is given by:

$$R(t) = \mathrm{e}^{-\lambda t} \tag{6.106}$$

Taking logarithms of both sides of the above equation gives:

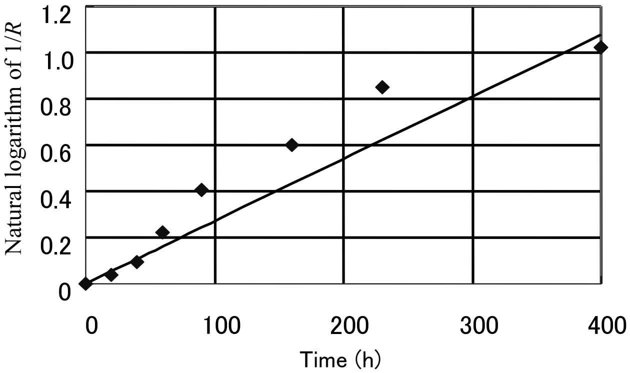


Fig. 6.10. Exponential distribution plot

$$\ln \frac{1}{R(t)} = \lambda t \tag{6.107}$$

Therefore, points $(t, \ln[1/R(t)])$ yield a straight line passing through the origin and having a slope of λ.

Consider the 250 TTF data for old-type transistors shown in Table 6.2. Reliability can easily be calculated by dividing the number of normal transistors by 250. The plotting result is shown in Figure 6.10, yielding a failure rate of $\lambda = 0.0027$.

Table 6.3. TTFs of first 7 failures among 20 devices

Failure Number i	TTF (h)	Median rank $F(t) \times 100$ $= \frac{i-0.5}{n} \times 100$
1	1	2.5
2	4	7.5
3	5	12.5
4	6	17.5
5	15	22.5
6	20	27.5
7	40	32.5

6.6.2 Weibull Distribution and Early Failure

A 2-parameter Weibull distribution is given by:

$$F(t) = 1 - \exp\left[- \left(\frac{t}{\sigma} \right)^{\beta} \right] \tag{6.108}$$

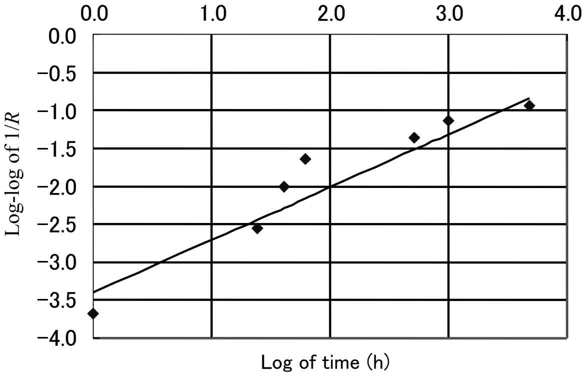


Fig. 6.11. Weibull distribution plot to identify early failures

The exponential distribution is a special case of the Weibull distribution with $\beta = 1$ and $\lambda = 1/\sigma$.

Take the logarithms twice for both sides of the above equation:

$$\ln \ln \frac{1}{1 - F(t)} = \beta \ln t - \beta \ln \sigma \tag{6.109}$$

Points $(\ln t, \ln \ln[1/(1 - F)])$ shape a straight line with slope β and the y intersection $\widetilde{y}$ of $-\beta \ln \sigma$. In other words, parameter β is obtained from the slope, while σ is determined by β and the y intersection $\widetilde{y}$:

$$\sigma = \exp \frac{-\widetilde{y}}{\beta} \tag{6.110}$$

Consider 20 devices of the same type [59]. The first 7 TTFs are shown in Table 6.3. The so-called median rank estimates unreliability on the basis of the number i of failures and finite number n of samples. Several formulas are available:

$$F(t) = \frac{i - 0.5}{n} \text{ or } \frac{i - 0.3}{n + 0.4} \tag{6.111}$$

The unreliability estimate is smaller than unity even if all samples fail, which is a reasonable requirement. See reference [60] for more detail.

Failures are concentrated during early times, which suggest early failures. An exponential distribution is too simple to fit the data. Figure 6.11 shows a result of a Weibull plot. The parameters are obtained as follows:

$$\beta = 0.70 \tag{6.112}$$

$$\sigma = \mathrm{e}^{3.4/0.70} = 129 \tag{6.113}$$

Unreliabilities at $t = 100$ and $t = 300$ are predicted on the basis of the parameter estimates:

$$F(100) = 1 - \exp\left[-\left(\frac{100}{129}\right)^{0.7}\right] = 0.56 \tag{6.114}$$

$$F(300) = 1 - \exp\left[-\left(\frac{300}{129}\right)^{0.7}\right] = 0.84 \tag{6.115}$$

The cumulative number of failures up to time $t = 100$ is predicted as $0.56 \times 20 = 11.2$, while the number up to time $t = 300$ is $0.84 \times 20 = 16.8$. In practice, 11 and 16 failures were observed up to $t = 100$ and $t = 300$, respectively, which indicated good performance of the Weibull distribution.

The Weibull distribution has the failure rate in an analytical form:

$$r(t) = \frac{\beta}{\sigma}\left(\frac{t}{\sigma}\right)^{\beta-1} \tag{6.116}$$

Figure 6.12 shows profiles of the failure density and failure rate for the Weibull distribution. The failure rate $r(t)$ is monotonically decreasing for $\beta < 1$, remains constant for $\beta = 1$, and monotonically increasing for $\beta > 1$. This example of early failures, of course, has the monotonically decreasing failure rate because parameter β equals 0.7.

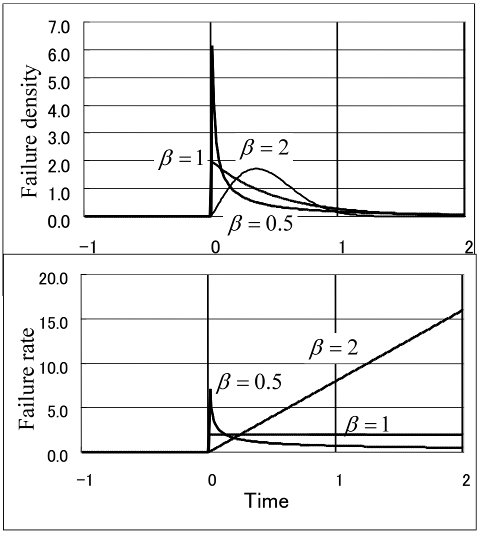


Fig. 6.12. Profiles of Weibull failure densities and failure rates

6.6.3 Weibull Distribution and Wearout Failure

This example concerns a retrospective Weibull analysis carried out on a furnace of a chemical company (page 316 of [53]). The furnace has 176 tubes. The

Table 6.4. TTF data for reactor pipes

Failure number i	Time to failure (day)	Percentile $F(t) \times 100 = \frac{i-0.3}{n+0.4} \times 100$
1	475	0.40
2	482	0.96
3	541	1.53
4	556	2.10

first tube failure occurs 475 days after the start of the furnace, thus suggesting a failure due to wearout mechanisms. A total of 4 failures are listed in Table 6.4. Points $(\ln t, \ln\ln[1/(1-F)])$ are plotted in Figure 6.13 in the same way

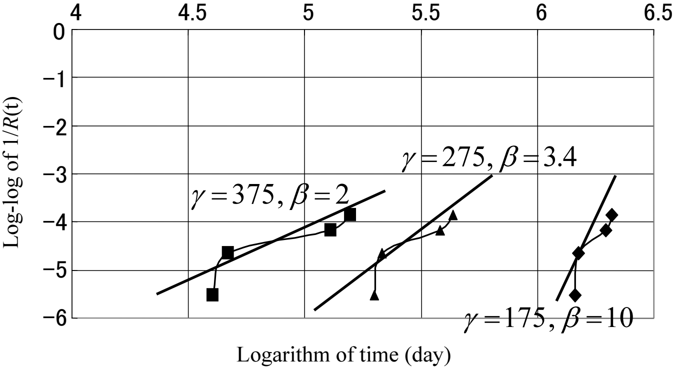


Fig. 6.13. Weibull distribution plot to identify wearout failures

as the early failures. A significantly steep slope with $\beta = 10$ is observed. Past experience indicates that parameter β takes a value in the interval $[2, 3.4]$ for wearout failures.

The following 3-parameter Weibull distribution is introduced to solve the problem of too large a value of β:

$$F(t) = \begin{cases} 0, & \text{for } 0 \le t < \gamma \\ 1 - \exp\left[-\left(\dfrac{t-\gamma}{\sigma}\right)^{\beta}\right], & \text{for } \gamma \le t \end{cases} \tag{6.117}$$

Similarly to the 2-parameter case, we have the equation by taking double logarithms:

$$\ln\ln\frac{1}{1-F(t)} = \beta\ln(t-\gamma) - \beta\ln\sigma \tag{6.118}$$

This indicates that the following points constitute a straight line with slope β and y intersection $-\beta \ln \sigma$:

$$\left(\ln(t-\gamma), \ln\ln\left[\frac{1}{1-F(t)}\right] \right) \tag{6.119}$$

Time t is replaced by $t - \gamma$ to plot points of Equation 6.118. Table 6.5 is created to explicitly perform the replacement by assuming two γs. The resultant plots are shown in Figure 6.13.

We have parameter $\beta = 2$ and $\beta = 3.4$ for $\gamma = 375$ and $\gamma = 275$, respectively. The two lines could be used to predict the residual number of failures up to 182 days after the fourth failure. The prediction was from 9 to 14 failures, while in practice 11 failures occurred.

Table 6.5. Shifting TTF data for reactor pipes

Failure number	TTF	$\gamma = 375$ days	$\gamma = 275$ days	Percentile $F(t) \times 100$
i	(day)	$\beta = 2.0$	$\beta = 3.4$	$= \dfrac{i-0.3}{n+0.4} \times 100$
1	475	100	200	0.40
2	482	107	207	0.96
3	541	166	266	1.53
4	556	181	281	2.10

6.7 Lognormal Distribution

The component unavailability Q (and failure rate λ) can be estimated with an uncertainty that includes statistical fluctuations and insufficient knowledge about the component.

The unavailability can be written as $Q = 10^x$, where variable x denotes the order of value Q. The uncertainty can be dealt with by noting that the order x of the unavailability follows a distribution. The lognormal distribution is a typical one to describe fluctuations of this order.

Assume that the order x follows a normal distribution. In other words, suppose that logarithm $\ln Q = x \ln 10$ follows a normal distribution:

$$\ln Q \sim \text{gau}^*(x; \mu, \beta^2) \tag{6.120}$$

Symbol gau* denotes the normal distribution probability density with mean μ and variance β^2. Note that quantity μ is not a mean of Q but $\ln Q$. Similarly, quantity $\beta > 0$ is not a standard variation of Q but $\ln Q$.

The range of unavailability Q is $[0,1]$, thus the logarithm $\ln Q$ is a negative value. However, mean $\mu < 0$ is usually sufficiently less than zero and standard variation β is also small. Thus, the contribution from the positive value regions of $\ln Q$ is negligible in Equation 6.120.

Let random variable Y be a function $Y = h(X)$ of another random variable X. The probability density $g(y)$ of Y is obtained from the density $f(x)$ of X [35].

$$g(y) = f(x)\left|\frac{\mathrm{d}x}{\mathrm{d}y}\right| \tag{6.121}$$

Special cases are given below:

$$g(y) = f(\ln y)\frac{1}{y} \text{ for } Y = \mathrm{e}^X \tag{6.122}$$

$$g(y) = f\left(\frac{1}{y}\right)\frac{1}{y^2} \text{ for } Y = \frac{1}{X} \tag{6.123}$$

$$g(y) = f\left(\ln\frac{Y}{1-Y}\right)\frac{1}{Y(1-Y)} \text{ for } Y = \frac{\mathrm{e}^X}{1+\mathrm{e}^X} \tag{6.124}$$

The lognormal distribution is uniquely determined from parameters μ and β. Equation 6.122 shows that the original variable Q follows the following probability density:

$$\mathrm{p}(Q) = \frac{1}{\sqrt{2\pi}\beta Q}\exp\left[-\frac{(\ln Q - \mu)^2}{2\beta^2}\right] \equiv \text{log-gau}^*(Q; \mu, \beta^2) \tag{6.125}$$

Here, the symbol log-gau$^*()$ denotes a lognormal density.

Denote by Q_{med}, Q_{mea}, and Q^* the median, mean, and mode of the lognormal variable Q. The following qualities can be shown with the inequalities (Figure 6.14):

$$Q_{\text{med}} = \exp(\mu) \tag{6.126}$$

$$Q_{\text{mod}} = Q_{\text{med}}\exp(-\beta^2) \tag{6.127}$$

$$Q_{\text{mea}} = Q_{\text{med}}\exp(0.5\beta^2) \tag{6.128}$$

$$Q_{\text{mod}} \leq Q_{\text{med}} \leq Q_{\text{mea}} \tag{6.129}$$

Variance of lognormal variable Q is given by

$$V(Q) = Q^2_{\text{med}}\exp(\sigma^2)[\exp(\sigma^2) - 1] \tag{6.130}$$

Equation 6.126 shows that mean μ of $\ln Q$ can be obtained from median Q_{med}. In the following, we will see that standard variation β is obtained from a positive constant K called an error factor.

The following confidence interval is considered for variable Q:

$$\left[\frac{Q_{\text{med}}}{K},\ Q_{\text{med}}K\right] \tag{6.131}$$

The order of Q follows a normal distribution. Thus, it is reasonable to introduce Q_{med}/K as a left boundary of the interval, and $Q_{\mathrm{med}}K$ a right boundary, given median Q_{med}. Constant K is defined as a coefficient such that variable Q falls in the interval of Equation 6.131 with probability $1-2\alpha>0$, and hence the name of the $1-2\alpha$ error factor K:

$$\Pr\{Q \in \Big[\frac{Q_{\mathrm{med}}}{K},\ Q_{\mathrm{med}}K\Big]\} = 1-2\alpha \tag{6.132}$$

We call K a 90% error factor for $\alpha = 0.05$.

Take a logarithm of expression $Q \in [Q_{\mathrm{med}}/K,\ Q_{\mathrm{med}}K]$, subtract $\mu = \ln Q_{\mathrm{med}}$, and then divide the result by β, yielding:

$$\Pr\Big\{\frac{\ln Q-\mu}{\beta} \in \Big[-\frac{\ln K}{\beta},\ \frac{\ln K}{\beta}\Big]\Big\} = 1-2\alpha \tag{6.133}$$

The variable $(\ln Q-\mu)/\beta$ follows a unit normal distribution with mean zero and variance unity. Thus, $(\ln K)/\beta$ is the $100(1-\alpha)$ percentile L of the unit normal distribution:

$$\Pr\{x \le L\} = 1-\alpha,\quad x \sim \mathrm{gau}^*(x;0,1) \tag{6.134}$$

In other words, parameter β can be determined from the percentile:

$$(\ln K)/\beta = L \Leftrightarrow \beta = (\ln K)/L \tag{6.135}$$

Factor K and parameter α are first specified. Then, percentile L is determined from α, and $\beta = (\ln K)/L$ is eventually obtained from K and L.

As an example, consider a case where median $Q_{\mathrm{med}} = 7.41\times10^{-2}$, error factor $K = 3.0$, and $\alpha = 0.05$. The 90% confidence interval becomes $[0.00247, 0.222]$. Parameter μ is obtained as $\mu = \ln Q_{\mathrm{med}} = -2.6$. A familiar normal distribution table gives the 95 percentile $L = 1.645$. Parameter β is obtained as $\beta = (\ln K)/L = 0.67$.

6.8 Stress and Response Model

The strength or resistance of equipment is the maximum stress that the equipment can withstand. Resistance C varies from one equipment to another even if the equipment type is the same. Thus variation can be represented by the probability density $p_C(c)$ in Figure 6.15. Capital C represents a random variable, while lower case c denotes an independent variable of the density function. The same convention will be used for other variables.

On the other hand, the stress is frequently called a response by borrowing the terminology of equipment response to earthquakes. The stress or the response vary depending on the equipment locations in the building and on the earthquakes. The variation is depicted by the probability density $p_R(r)$ in

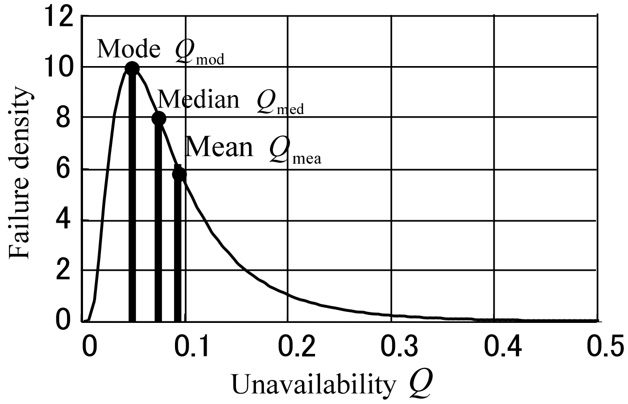


Fig. 6.14. Lognormal failure density

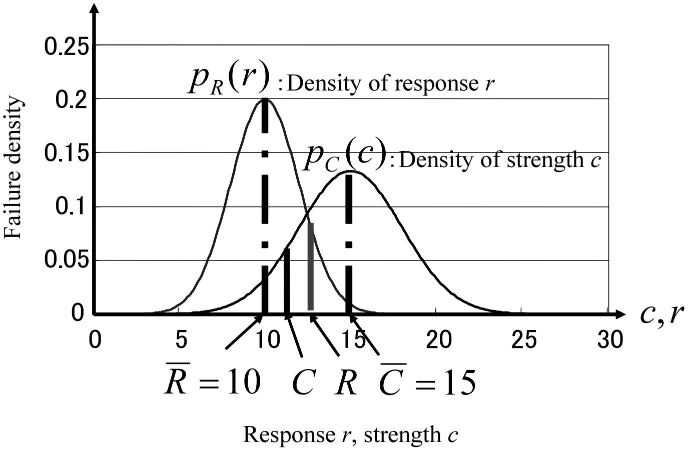


Fig. 6.15. Schematic representation of stress–response model

Figure 6.15. Equipment damage occurs when response R exceeds resistance C. An example of such an excess is shown explicitly in Figure 6.15. Assume that the response lies in the infinitesimal interval $[r, r + \mathrm{d}r]$. Then, the probability density $p_D(r)$ of the equipment damage becomes:

$$\mathrm{p}_D(r)\mathrm{d}r = \mathrm{p}_R(r)\mathrm{d}r \times \int_0^r \mathrm{p}_C(c)\mathrm{d}c \tag{6.136}$$

Thus, the equipment-damage probability P_D is the sum of $\mathrm{p}_D(r)\mathrm{d}r$ over all infinitesimal intervals:

$$P_D = \int_0^\infty \mathrm{p}_D(r)\mathrm{d}r = \int_0^\infty \mathrm{p}_R(r)\mathrm{d}r \times \int_0^r \mathrm{p}_C(c)\mathrm{d}c \tag{6.137}$$

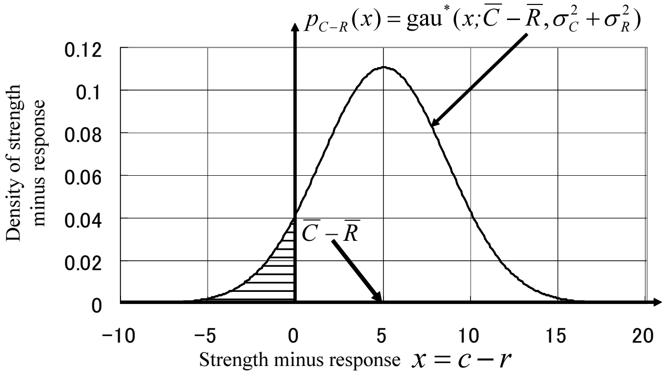


Fig. 6.16. Stress–response model described by normal distribution

6.8.1 Case of Normal Distribution

The simplest case is when both resistance and response follow normal distributions:

$$\mathrm{p}_C(c) = \frac{1}{\sqrt{2\pi}\sigma_C} \exp\left[-\frac{(c-\bar{C})^2}{2\sigma_C^2}\right] = \text{gau}^*(c; \bar{C}, \sigma_C^2) \tag{6.138}$$

$$\mathrm{p}_R(r) = \frac{1}{\sqrt{2\pi}\sigma_R} \exp\left[-\frac{(r-\bar{R})^2}{2\sigma_R^2}\right] = \text{gau}^*(r; \bar{R}, \sigma_R^2) \tag{6.139}$$

Figure 6.15 is the following case:

$$\bar{C} = 15, \quad \sigma_C = 3 \tag{6.140}$$

$$\bar{R} = 10, \quad \sigma_R = 2 \tag{6.141}$$

The normal distributions permit negative values, which can be neglected when the means are large and standard deviations are small. Another alternative is a normalization of the probability density after removing the probability of the negative portion.

It is obvious that damage occurs when the difference $C - R$ becomes negative. For the independent normal random variables C and R, the difference follows a normal distribution with mean $\bar{C} - \bar{R}$ and variance $\sigma_C^2 + \sigma_R^2$, as shown in Figure 6.16. The shaded area corresponds to the damage probability, which is about 0.08 in this case.

Denote by $\phi\text{gau}(x)$ the cumulative distribution function of the unit normal distribution with mean 0 and variance 1:

$$\phi\text{gau}(x) = \int_{-\infty}^{x} \text{gau}^*(x; 0, 1)\mathrm{d}x \tag{6.142}$$

Consider a new vertical axis crossing the horizontal coordinate at $\bar{C} - \bar{R}$ in Figure 6.16. It is easily seen that damage probability P_D is given by:

$$P_D = \phi\text{gau}\left(-\frac{\bar{C}-\bar{R}}{\sqrt{\sigma_C^2+\sigma_R^2}}\right) \tag{6.143}$$

The damage probability is influenced not only by the difference of means but also by the square root of the sum of variances: listpara

1) The damage probability becomes 0.5 when the resistance mean is equal to the response mean, $\bar{C}=\bar{R}$.
2) Consider a normal case $\bar{C}-\bar{R}>0$ where the resistance mean is larger than the response mean. The damage probability increases towards 0.5 when either or both the variances increase.
3) Assume another case $\bar{C}-\bar{R}<0$ the resistance mean is smaller than the response mean. The damage probability decreases towards 0.5 when either or both the variances increases.
4) There are two ways to decrease the damage probability. listpb
   4-1) Sufficiently large resistance mean $\bar{C}$.
   4-2) Sufficiently small variances, given that the resistance mean exceeds the response mean $\bar{C}>\bar{R}$.

6.8.2 Case of Lognormal Distribution

The lognormal cases are important in practice. Assume the following distributions:

$$\ln C \sim \text{gau}^*(x;\mu_C,\beta_C^2) \tag{6.144}$$

$$\ln R \sim \text{gau}^*(x;\mu_R,\beta_R^2) \tag{6.145}$$

The damage occurs when the difference $\ln C - \ln R = \ln(C/R)$ becomes negative because this is equivalent to $C-R \le 0$. The difference follows a normal distribution:

$$\ln C - \ln R \sim \text{gau}^*(x;\mu_C-\mu_R,\beta_C^2+\beta_R^2) \tag{6.146}$$

In the same way as Equation 6.143, the damage probability is given by:

$$P_D = \phi\text{gau}\left(-\frac{\mu_C-\mu_R}{\sqrt{\beta_C^2+\beta_R^2}}\right) \tag{6.147}$$

Parameters μ_C and μ_R are the means of normal random variables $\ln C$ and $\ln R$, respectively. Thus, parameters μ_C and μ_R are also the medians of $\ln C$ and $\ln R$, respectively. Denote, respectively, by C_{med} and R_{med} the median of variables C and R. Obviously, $\ln C_{\text{med}}$ and $\ln R_{\text{med}}$ become the medians of normal random variables $\ln C$ and $\ln R$, and the means can be expressed as:

$$\mu_C = \ln C_{\text{med}}, \quad \mu_R = \ln R_{\text{med}} \tag{6.148}$$

This is the same as Equation 6.126.

As a result, the damage probability is determined from medians C_{med} and R_{med}, and standard deviations β_C and β_R of the lognormal distributions:

$$P_D = \phi\mathrm{gau}\left(\frac{\ln(R_{\mathrm{med}}/C_{\mathrm{med}})}{\sqrt{\beta_C^2+\beta_R^2}}\right) \tag{6.149}$$

This equation is frequently used for calculating the equipment-damage probability by earthquakes.

6.9 Basic-event Parameters for PRA

The risk quantification process of PRA should be based on reliability databases that reflect objective facts and subjective assessments.

6.9.1 Types of Parameters

The PRA requires the following parameters concerning basic events [35].

1) initiating-event occurrence rate;
2) standby-failure rate;
3) duration parameters such as recovery rate;
4) unavailability;
5) demand failure probability

Data sources are surveyed in Section 4 of reference [35]

6.9.2 Data for Parameter Quantification

Two approaches are available for quantification of the basic event parameters: frequentist and Bayesian. Table 6.6 summarizes the Bayesian approach to constant parameters. Reference [35] describes confidence intervals as well as trends and aging.

Data required for the quantification are listed in the second row of the table. For the initiating event, x events are observed during exposure time t. For the standby failure, a total of n tests are performed at the end of test intervals, and x failures are observed; exact failure times before the tests are unknown; symbol t_i denotes the failed test interval. The remaining $n-x$ tests yield successful results; symbol s_j denotes the test interval.

For the failure-to-run, x failures occur at times t_i that are known, while $n-x$ successful operations continue up to mission completion times s_j.

Time-to-recovery data are examples of the duration data. For the unavailability, x pairs of up and down times are recorded. The demand failure assumes x failures per n demands.

Table 6.6. Bayesian approach for PRA-parameter quantification

Case	1 Initiating event	2 Standby failure	3 Failure to run	4 Duration	5 Unavailability	6 Demand failure
Data D	x events during exposure time t	1) x failures observed at the end of test intervals $t_1, \dots, t_x$ 2) $n-x$ successful results observed at the end of test intervals $s_1, \dots, s_{n-x}$	1) x failures observed at known times $t_1, \dots, t_x$ before mission completion 2) $n-x$ successful operations up to mission completion times $s_1, \dots, s_{n-x}$	Duration times $t_1, \dots, t_x$	x pairs of up and down times $(t_i, t_i^*),\ \ i = 1, \dots, x$	x failures per n demands
Unknown parameter	λ Occurrence rate	λ Standby failure rate	λ Failure rate	λ Recovery rate	$\lambda,\ \mu,\ Q$ Failure rate, repair rate, unavailability	Q Demand failure probability
a priori density ∝	$\lambda^{\alpha-1}\mathrm{e}^{-\lambda\beta}$ gamma$^*(\lambda; \alpha,\ \beta)$				$\lambda^{\alpha-1}\mathrm{e}^{-\lambda\beta}$ $\times\mu^{\alpha^*-1}\mathrm{e}^{-\mu\beta^*}$	$Q^{\alpha-1}(1-Q)^{\beta-1}$ beta$^*(Q; \alpha, \beta)$
Likelihood ∝	$\lambda^x\mathrm{e}^{-\lambda t}$ Poisson$^*(x; \lambda, t)$				$\lambda^x\mathrm{e}^{-\lambda t}\mu^x\mathrm{e}^{-\mu t^*}$	$Q^x(1-Q)^{n-x}$ binomial$^*()$
Exposure time	t: Given	$t \equiv \sum_{j=1}^{n-x} s_j$ $+\ (1/2)\sum_{i=1}^{x} t_i$	$t \equiv \sum_{j=1}^{n-x} s_j$ $+\ \sum_{i=1}^{x} t_i$	$t \equiv \sum_{i=1}^{x} t_i$	$t \equiv \sum_{i=1}^{x} t_i$ $t^* \equiv \sum_{i=1}^{x} t_i^*$	
a posteriori density ∝	$\lambda^{x+\alpha-1}\ \mathrm{e}^{-\lambda(t+\beta)}$ gamma$^*(\lambda; x+\alpha, t+\beta)$				$\lambda^{x+\alpha-1}\mathrm{e}^{-\lambda(t+\beta)}$ $\times\mu^{x+\alpha^*-1}\mathrm{e}^{-\mu(t^*+\beta^*)}$	$Q^{(x+\alpha)-1}$ $\times(1-Q)^{(n-x+\beta)-1}$ beta$*()$
a posteriori mean	$\hat{\lambda} = \dfrac{x+\alpha}{t+\beta},\ \ \hat{\mu} = \dfrac{x+\alpha^*}{t^*+\beta^*},\ \ \hat{Q} = \dfrac{\hat{\lambda}}{\hat{\lambda}+\hat{\mu}} \simeq \dfrac{\hat{\lambda}}{\hat{\mu}}$					$\hat{Q} = \dfrac{x+\alpha}{n+\alpha+\beta}$

6.9.3 Quantified Parameters

Parameters to be quantified are rates λ for the first four cases. The unavailability case estimates unavailability Q via failure rate λ and repair rate μ. The demand-failure case estimates the failure probability Q per demand.

6.9.4 Bayesian Approach

Rate Case
Denote by D the observed data. Consider the rate parameter λ for the first four cases.

The Bayes formula states that the *a posteriori* probability density $\mathrm{p}(\lambda|D)$ is proportional to the product of the *a priori* probability density $\mathrm{p}(\lambda)$ and likelihood $\mathrm{p}(D|\lambda)$:

$$\mathrm{p}(\lambda|D) \propto \mathrm{p}(D|\lambda)\mathrm{p}(\lambda) \tag{6.150}$$

The rhs could be divided by the normalizing factor $\mathrm{p}(D)$ to yield the unity integral of $\mathrm{p}(\lambda|D)$ over $\lambda \in [0, \infty)$. However, only factors related to λ can be retained in the rhs. The likelihood is regarded as a function of λ. This formula uses the fact that the conditional probability $\mathrm{p}(D|\lambda)$ is more easily obtained than the target conditional probability $\mathrm{p}(\lambda|D)$.

A typical *a priori* probability for the rate case is the gamma probability density:

$$\mathrm{p}(\lambda) = \mathrm{gamma}^*(\lambda; \alpha, \beta) \propto \lambda^{\alpha-1}\mathrm{e}^{-\lambda\beta}, \quad \alpha > 0, \quad \beta \geq 0 \tag{6.151}$$

This density has mean α/β and variance α/β^2. The *a priori* number of failures corresponds to α, while the *a priori* exposure time to β. A so-called Jeffreys noninformative prior is $\mathrm{gamma}^*(\lambda; 1/2, 0)$ with the infinite mean and the infinite variance.

The likelihood for the rate case becomes a Poisson type:

$$\mathrm{p}(D|\lambda) = \mathrm{Poisson}^*(x; \lambda, t) \propto \lambda^x \mathrm{e}^{-\lambda t} \tag{6.152}$$

The rhs includes only factors concerning λ in the same way as the rhs of Equation 6.150. Table 6.6 defines exposure time t for each case.

It turns out that the *a posteriori* density also becomes a gamma probability density:

$$\mathrm{p}(\lambda|D) = \mathrm{gamma}^*(\lambda; x + \alpha, t + \beta) \propto \lambda^{x+\alpha-1}\mathrm{e}^{-\lambda(t+\beta)} \tag{6.153}$$

The mean and variance are:

$$\hat{\lambda} \equiv E(\lambda|D) = \frac{x + \alpha}{t + \beta}, \ V(\lambda|D) = \frac{x + \alpha}{(t + \beta)^2} \tag{6.154}$$

The mean has a dimension of 1/time. The gamma *a priori* density is called a conjugate prior because the *a posteriori* density also becomes a gamma density.

Unavailability Case
The unavailability case considers as the *a priori* density the product of two gamma densities for λ and μ. The likelihood is the product of two Poisson distributions. The *a posteriori* density becomes a product of two gamma densities. The unavailability is estimated as:

$$\hat{Q} = \frac{\hat{\lambda}}{\hat{\lambda} + \hat{\mu}} \simeq \frac{\hat{\lambda}}{\hat{\mu}} \tag{6.155}$$

Demand-failure Case
A conjugate *a priori* density is a beta density:

$$\mathrm{p}(Q) = \mathrm{beta}^*(Q; \alpha, \beta) \propto Q^{\alpha-1}(1-Q)^{\beta-1}, \ \ \alpha > 0, \ \ \beta > 0 \tag{6.156}$$

The mean and variance are:

$$E(Q) = \frac{\alpha}{\alpha+\beta}, \ \ V(Q) = \frac{\alpha\beta}{(\alpha+\beta)^2(\alpha+\beta+1)} \tag{6.157}$$

The Jeffreys noninformative prior is:

$$\mathrm{beta}^*(Q; 1/2, 1/2) \propto \frac{1}{\sqrt{Q(1-Q)}} \tag{6.158}$$

The likelihood becomes a binomial type:

$$\mathrm{p}(D|Q) = \mathrm{binomial}^*(x; n, Q) \propto Q^x(1-Q)^{n-x} \tag{6.159}$$

This should be regarded as a function of Q.

The *a posteriori* density also becomes a beta density:

$$\mathrm{p}(Q|D) = \mathrm{beta}^*(Q; x+\alpha, n-x+\beta) \propto Q^{x+\alpha-1}(1-Q)^{n-x+\beta-1} \tag{6.160}$$

The dimensionless-mean and variance are:

$$\hat{Q} = E(Q|D) = \frac{x+\alpha}{n+\alpha+\beta}, \ V(Q|D) = \hat{Q}(1-\hat{Q})/(\alpha+\beta+1) \tag{6.161}$$

6.9.5 Demand Failure and Standby Failure

Consider frequentist maximum-likelihood estimators:

$$\lambda^* = \frac{x}{t}, \ \ Q^* = \frac{x}{n} \tag{6.162}$$

Denote by T a common test interval. We have $t \simeq nT$ by a rare-event approximation. Each test is regarded as a demand to obtain data x. Consider, on the other hand, that real demands are uniformly distributed over the test interval. A standby-channel demand-failure probability becomes:

$$\frac{1}{2}\lambda^* T = \frac{1}{2}\frac{x}{t}T \simeq \frac{x}{2n} = \frac{Q^*}{2} \tag{6.163}$$

The standby failure case results in one half of the failure probability as compared to the demand failure case.

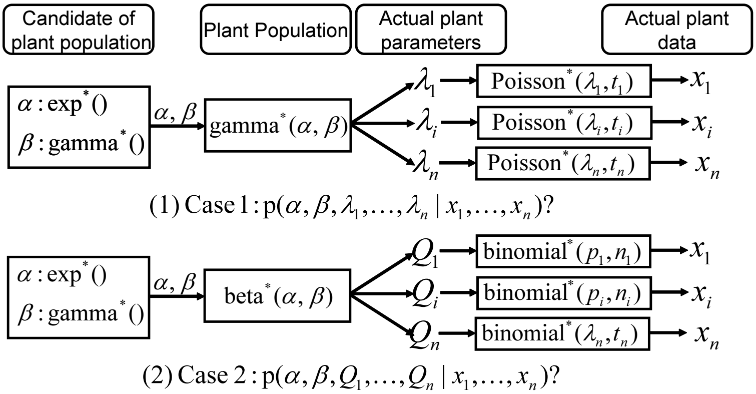


Fig. 6.17. Schematic of hierarchical Bayes approach

6.9.6 Hierarchical Bayes Approach

This approach uses a sophisticated Monte Carlo (*i.e.* Gibbs) sampling from the *a posteriori* distribution [35]. A window version called WinBUGS is currently available for free on WWW.

Variations of n different plants can be considered. Figure 6.17 shows the schematic. The *a priori* density for parameter α is exponential, while density for parameter β is gamma. These two densities are explicitly given to represent candidates of a distribution of n plants. Parameters α and β are sampled from these *a priori* densities, resulting in a unique distribution.

For the failure rate case, the unique distribution is gamma$^*(\lambda; \alpha, \beta)$. Plant-specific λ_i is sampled from this gamma density. The rate λ_i and exposure time t_i determine a plant-specific Poisson distribution from which the number x_i of events is observed for plant i. The *a posteriori* density of α, β, and λ_1 to λ_n are determined by the Monte Carlo, given observation x_1 to x_n.

The plant-specific demand failure probability Q_i is a sample from a beta distribution. The schematic can be modified into a case where the demand failure probability is sampled from a logistic-normal density. The probability Q has this distribution when $x = \ln[Q/(1-Q)]$ is normally distributed with mean μ and variance $\sigma^2 \equiv 1/\tau^2$. The conversion from x to Q is:

$$Q = \frac{\mathrm{e}^x}{1 + \mathrm{e}^x} \tag{6.164}$$

The logistic-normal density avoids concentration of Q around zero.

6.10 Concluding Remarks

Basic event parameters are defined. Their relations are clarified. Parameter quantification methods are demonstrated, including ordinary and hierarchical Bayes approaches for PRA.

7

System Event Quantification

7.1 Introduction

A top event is defined as an undesired state of a system (*e.g.*, a failure of the system to accomplish its function). The top event is the starting point (at the top) of the fault-tree model [5]. A basic event is defined as an event in a fault-tree model that requires no further development, because the appropriate limit of resolution has been reached [5]. This chapter focuses on the relationships between the top event and the basic events. The reliability parameters presented in Chapter 6 can be extended to the top event [53].

7.2 Simple Systems

7.2.1 Reliability Block Diagram

As was defined in Section 2.2.2, a function is an action that is required to achieve a desired goal [13]. The action is either performed by a machine or a human. The reliability block diagram represents the achievement of the function by a diagram consisting of blocks. Each block denotes a name or a lower-level function of a system component. Achievement of the system-level function is defined as a connectivity from the leftmost node to the rightmost node of the diagram.

Basic events corresponds to the component failure represented by the block. The connectivity is cut at blocks of component failures. The top event is a failure of achievement of the system-level function. A disconnection of the block diagram corresponds to the occurrence of the top event. The reliability block diagram is weak in dealing with repeated events defined as the same blocks showing up in different places of the diagram. The fault trees are superior in dealing with a variety of repeated events including a power failure shared by two or more devices.

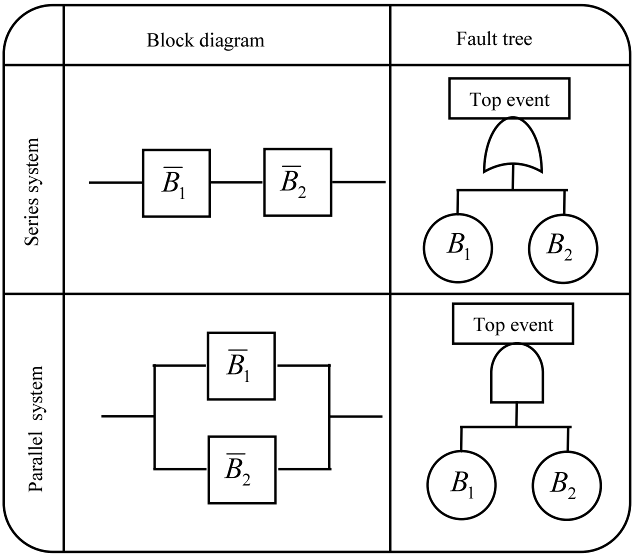


Fig. 7.1. Correspondence between block diagram and fault tree

Table 7.1. Truth table for series system

No	Basic event 1	Basic event 2	Top event	Probability
1	exist.	exist.	exist.	$\Pr\{B_1\}\Pr\{B_2\}$
2	exist.	nonexist.	exist.	$\Pr\{B_1\}\Pr\{\bar{B}_2\}$
3	nonexist.	exist.	exist.	$\Pr\{\bar{B}_1\}\Pr\{B_2\}$
4	nonexist.	nonexist.	nonexist.	$\Pr\{\bar{B}_1\}\Pr\{\bar{B}_2\}$

7.2.2 Series System

For the series system, the function at the system level is accomplished when all the functions at the component level are performed. Consider, as an example, the series system consisting of two components 1 and 2. Denote by complement $\bar{B}_i$ the achievement of function of component i, and by B_i the failure of component i. The series system can be represented by the block diagram or the OR gate in Figure 7.1. The curved baseline of the OR gate suggests "O". The system is also represented by the truth table of Table 7.1.

Denote by $Q_{\mathrm{S}}(t)$ the system unavailability where suffix "S" stands for "system". This is defined by the probability of the function being unavailable. This is also the probability of the top event when the function failure is represented by logic gates. The first three rows of Table 7.1 yields the unavailability of the series system by noting $\Pr\{\bar{B}_i\} = 1 - \Pr\{B_i\}$:

$$Q_{\mathrm{S}}(t) = \Pr\{B_1\} + \Pr\{B_2\} - \Pr\{B_1\}\Pr\{B_2\} \tag{7.1}$$

Table 7.2. Truth table for parallel system

No	Basic event 1	Basic event 2	Top event	Probability
1	exist.	exist.	exist.	$\Pr\{B_1\}\Pr\{B_2\}$
2	exist.	nonexist.	nonexist.	$\Pr\{B_1\}\Pr\{\bar{B}_2\}$
3	nonexist.	exist.	nonexist.	$\Pr\{\bar{B}_1\}\Pr\{B_2\}$
4	nonexist.	nonexist.	nonexist.	$\Pr\{\bar{B}_1\}\Pr\{\bar{B}_2\}$

7.2.3 Parallel System

For the parallel system, the function at the system level is accomplished when at least one of the functions at the component level is performed. The parallel system can be represented by the block diagram or the AND gate in Figure 7.1. The straight baseline of the AND gate suggests "simultaneous" occurrence of the input events. The system is also represented by the truth table of Table 7.2. The first row of this table yields the unavailability of the parallel system:

$$Q_S(t) = \Pr\{B_1\}\Pr\{B_2\} \tag{7.2}$$

7.2.4 Voting System

Assume that the top event occurs when m out of n basic events occur. Suppose that the occurrence probability of each input event is a common constant Q. Let $\Pr\{k; n, Q\}$ be the probability of the occurrence of k basic events and the nonoccurrence of the remaining $n - k$ events. This is given by the binomial probability as a function of k:

$$\Pr\{k; n, Q\} = \binom{n}{k} Q^k (1-Q)^{n-k}, \ \binom{n}{k} \equiv \frac{n!}{k!(n-k)!} \tag{7.3}$$

The top event occurs when m or more basic event occur. Thus, the system unavailability becomes the following sum:

$$Q_S(t) = \sum_{k=m}^{n} \binom{n}{k} Q^k (1-Q)^{n-k} \tag{7.4}$$

Consider, for instance, a 2/3 system or a 2-out-of-3 system. We have:

$$Q_S(t) \equiv Q_{2/3}(t) = \binom{3}{2} Q^2 (1-Q)^1 + \binom{3}{3} Q^3 = 3Q^2 - 2Q^3 \tag{7.5}$$

A rare-event approximation for small Q yields:

$$Q_{2/3} = 3Q^2 \tag{7.6}$$

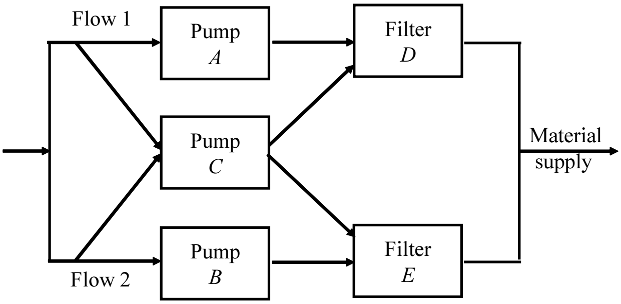


Fig. 7.2. Block diagram including bridge connection

Table 7.3. Truth table of nonseries-parallel system

No	*A*	*D*	*B*	*E*	*C*	Full	Half	No	*A*	*D*	*B*	*E*	*C*	Full	Half
1	W	W	W	W	W	W	W	17	F	W	W	W	W	W	W
2	W	W	W	W	F	W	W	18	F	W	W	W	F	F	W
3	W	W	W	F	W	F	W	19	F	W	W	F	W	F	W
4	W	W	W	F	F	F	W	20	F	W	W	F	F	F	F
5	W	W	F	W	W	W	W	21	F	W	F	W	W	F	W
6	W	W	F	W	F	F	W	22	F	W	F	W	F	F	F
7	W	W	F	F	W	F	W	23	F	W	F	F	W	F	W
8	W	W	F	F	F	F	W	24	F	W	F	F	F	F	F
9	W	F	W	W	W	F	W	25	F	F	W	W	W	F	W
10	W	F	W	W	F	F	W	26	F	F	W	W	F	F	W
11	W	F	W	F	W	F	F	27	F	F	W	F	W	F	F
12	W	F	W	F	F	F	F	28	F	F	W	F	F	F	F
13	W	F	F	W	W	F	W	29	F	F	F	W	W	F	W
14	W	F	F	W	F	F	F	30	F	F	F	W	F	F	F
15	W	F	F	F	W	F	F	31	F	F	F	F	W	F	F
16	W	F	F	F	F	F	F	32	F	F	F	F	F	F	F

Table 7.4. Numbers of functioning paths under event "Full" or "Half"

	A_{S}	Q_{S}
Full	2	0, 1
Half	1,2	0

Table 7.5. Cost comparison of 3 plant configurations

Configuration	A_{S}(Full)	A_{S}(Half)	Expected loss
Double	0.92	0.9984	\$323/day
Triple	0.9954	0.9994	\$239/day
Bridge	0.94	0.999	\$293/day

7.2.5 Nonseries-parallel System

Figure 7.2 is a block diagram of a raw-material supply system (page 375 of [53]). During the failure of pump A, pump C is used for flow path 1. A similar switchover occurs for the pump B failure. The block diagram has a bridge structure and can not reduce to a combination of series and/or parallel structures. A truth table can apply to nonseries-parallel systems as well as partial failures.

Table 7.3 enumerates all the states of the supply system. The "Full" indicates that the two flow paths are functioning, while "Half" shows that at least half the flow paths are functioning, *i.e.* that one or two paths are working. Symbols W and F, respectively, mean "working" and "failed". Table 7.4 lists the numbers of functioning paths under "Full" or "Half" event.

Assume a MTTF of 1/0.04 = 25 (days) and a MTTR of 5 (h) for each pump. The filter has the MTTF of 1/0.08 = 12.5 (days) and the MTTR of 10 (h). The availabilities of pumps and filters become:

$$\Pr\{\overline{A}\} = \Pr\{\overline{B}\} = \Pr\{\overline{C}\} = 0.99 \tag{7.7}$$

$$\Pr\{\overline{D}\} = \Pr\{\overline{E}\} = 0.97 \tag{7.8}$$

The probabilities of events "Full" and "Half" are denoted $A_{\mathrm{S}}(\text{Full})$ and $A_{\mathrm{S}}(\text{Half})$, respectively. Denote also by $Q_{\mathrm{S}}(\text{Half})$ the complement of $A_{\mathrm{S}}(\text{Half})$, *i.e.* the probability that the two flow paths are simultaneously failed.

The "Full" event probability is obtained as follows:

$$A_{\mathrm{S}}(\text{Full}) = \sum_{1,2,5,17} \Pr\{\text{row prob.}\} = 0.94 \tag{7.9}$$

The complement probability $Q_{\mathrm{S}}(\text{Half})$ is first calculated for event "Half" over the smaller number of rows than $A_{\mathrm{S}}(\text{Half})$:

$$Q_{\mathrm{S}}(\text{Half}) = \sum_{11,12,14,15,16,20,22,24,27,28,30,31,32} \Pr\{\text{row prob.}\} = 0.001 \tag{7.10}$$

The "Half" event probability, *i.e.* the probability of half or more supply becomes:

$$A_{\mathrm{S}}(\text{Half}) = 0.999 \tag{7.11}$$

Assume the following costs for pump, filter, full production loss, and half-production loss.

1) Pump: \$15 per day per pump including initial installation cost and others.
2) Filter: \$60 per day per filter including initial installation cost and others.
3) Full production loss: \$10 000 per day.
4) Half production loss: \$2000 per day.

Expected loss EL per day can be calculated as:

$$\begin{aligned}\mathrm{EL} = 3 \times 15 + 2 \times 60 + Q_{\mathrm{S}}(\mathrm{Half}) \times 10\ 000 \\ +[A_{\mathrm{S}}(\mathrm{Half}) - A_{\mathrm{S}}(\mathrm{Full})] \times 2000 = 293\end{aligned} \tag{7.12}$$

Parallel systems with two or three flow paths containing pairs of pump and filter can more easily be analyzed than the nonseries-parallel system. Table 7.5 shows the cost comparison. The full production is achieved in the triple-train system by a 2oo3 structure, while the half production is achieved by 1oo3. The triple-train system is the most cost effective.

7.3 Single Large Fault Tree

The pressure-tank example of Figure 2.3 showed an event tree coupled with fault trees, given an initiating event. This is the most familiar and effective application of event and fault trees.

Sometimes a single large fault tree is used without recourse to an event tree and without an initiating event. Figure 7.3 is such a fault tree where the relief-valve portion is removed from the ET–FT linkage for simplicity of description. On the contrary, the event tree become larger without the fault trees.

7.4 Minimal Cuts and Minimal Paths

7.4.1 Minimal Cut Sets

A minimal cut set is a collection of basic events and gives a system failure mode. A cut set consisting of a single event is dangerous and should be eliminated by design change.

Consider, for instance, the fault tree of Figure 7.3. The equivalent representation by a reliability block diagram is Figure 7.4. We see that the OR gate is replaced by a series arrangement of input events, and that the AND gate is given by a parallel arrangement.

A cut set is defined by:

1) It is a set of basic events.
2) Top event occurs when all the basic events occur in the cut set.

A minimal cut set is defined by:

1) It is a cut set.
2) It is no longer a cut set whenever an event is removed from the set.

The minimal cut set is a necessary and sufficient set of basic events that can cause the top event. The fault tree of Figure 7.3 has a total of 7 minimal cut sets:

$$\{1\}, \{2, 4\}, \{2, 5\}, \{2, 6\}, \{3, 4\}, \{3, 5\}, \{3, 6\} \tag{7.13}$$

Set $\{1, 2, 4\}$ is not minimal because it remains a cut set without event 1. The term "cut" means that the cut set disconnects signal transmission from the leftmost node to the rightmost one in the reliability block diagram of Figure 7.4. A large fault tree may have millions of minimal cut sets. Powerful computer codes to generate minimal cut sets are, for instance, SETS [61] and IRRAS [62].

7.4.2 Minimal Path Sets

A minimal path set is a collection of basic events and gives a system success mode in the sense that the top event does not occur. Similarly to our life, the

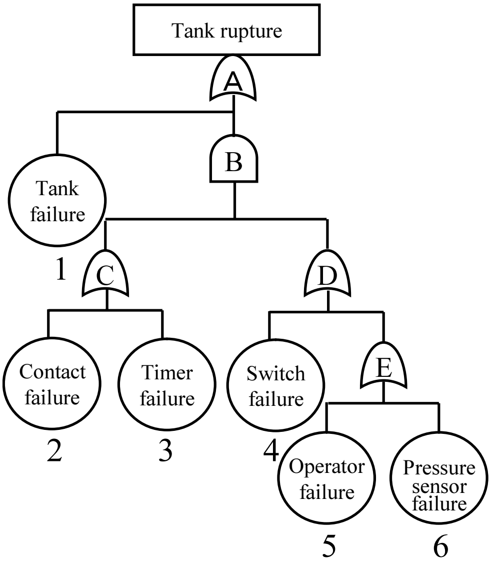


Fig. 7.3. Fault tree for rupture in pressure-tank system

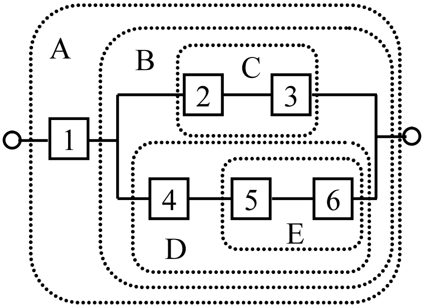


Fig. 7.4. Block diagram representation of cut and path sets

number of success modes (minimal path sets) are usually far smaller than the number of failure modes (minimal cut sets).

A path set is defined by:

1) It is a set of basic events.
2) Top event does not occur when none of the basic events in the set occurs.

A minimal path set is defined by:

1) It is a path set.
2) It is no longer a path set whenever an event is removed from the set.

The minimal path set is a necessary and sufficient set of basic events that ensure the nonoccurrence of the top event when none of the basic events occurs in the set. The fault tree of Figure 7.3 has 2 minimal path sets:

$$\{1, 2, 3\}, \{1, 4, 5, 6\} \tag{7.14}$$

The term "path" means that the path set gives a signal transmission route from the leftmost node to the rightmost one in Figure 7.4.

The nonoccurrences of all the basic events in a minimal path set ensure nonoccurrences of all the minimal cut sets. The occurrences of all the basic events in a minimal cut set ensure all the minimal path sets as system-success modes are nullified.

7.4.3 Minimal-cut Generation

MOCUS

One of most fundamental methods is called MOCUS (method of obtaining cut set) [63]. The method utilizes the fact that an OR gate increases cut sets, and that an AND gate increases the size of the cut sets. Eventually, a cut set is represented by a horizontal arrangement of basic events, while vertical arrangement of the cut sets enumerates the candidate of the minimal cut sets.

MOCUS proceeds as follows:

1) Repeat the following replacement downward of the fault tree.
   1-1) Replace an OR gate by a vertical arrangement of inputs.
   1-2) Replace an AND gate by a horizontal arrangement of inputs.
2) Remove nonminimal cut sets when all the gates are replaced.

A process of MOCUS is shown in Figure 7.5 for the fault tree of Figure 7.3. All the cut sets after the replacement are minimal because the fault tree has no repeated events, *i.e.* each basic event appears only once.

Horizontal arrangements such as (A, A, B) and $(1, 1, 2)$ can be simplified to (A, B) and $(1, 2)$, respectively.

Minimal path sets are generated when OR and AND gates are replaced by AND and OR gates before the start of the procedure. In other words, an OR gate of the original fault tree is replaced by a horizontal arrangement of inputs, while an AND gate by vertical arrangement.

A	1	1
1	2,4	2,4
B	2,E	2,5
1	3,4	2,6
C,D	3,E	3,4
1		3,5
2,D		3,6
3,D		

Fig. 7.5. Successive event development by MOCUS

Utilization of Module

A module is a portion independent of the remaining portions. Basic events in the module can be lumped together, thus simplifying minimal-cut generations and decreasing minimal cuts.

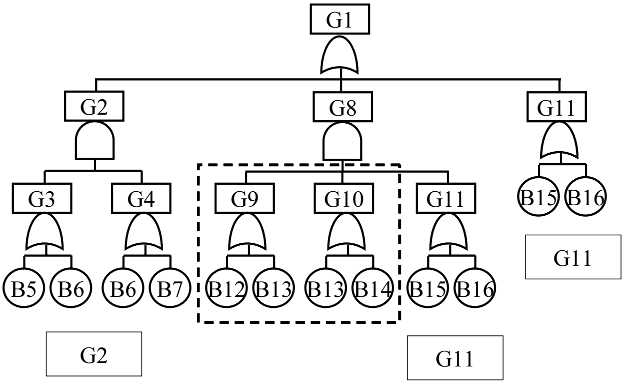


Fig. 7.6. Example of fault-tree modules

The fault tree of Figure 7.6 has two modules, 1) the portion below gate G11 inclusive, and 2) the portion below gate G2 inclusive, in the following sense:

1) It consists of a portion below a gate inclusive.
2) Basic events below the gate are confined there.

It is seen that the portion enclosed by the dotted-line square can be regarded as a module only after 1) AND gate G12 is introduced to combine gates G9 and G10, and 2) gate G12 is fed into gate G8. The modules depend on fault-tree representation. Minimal cut sets expressed in terms of modes are {G2} and {G11}. Cut set {G9, G10, G11} is not minimal and is removed.

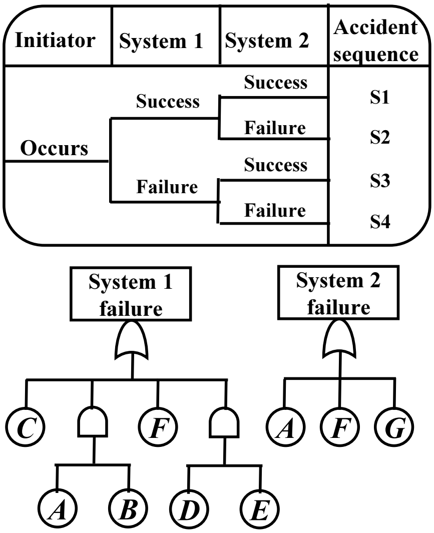


Fig. 7.7. Fault-tree linking along event tree

7.5 Fault-tree Linking along Event Tree

Consider an event tree coupled with two fault trees in Figure 7.7. Note that basic events A and F appear in both the fault trees.

The minimal path sets of system 1 failure fault tree are:

$$\{\bar{A},\bar{C},\bar{D},\bar{F}\},\ \{\bar{A},\bar{C},\bar{E},\bar{F}\},\ \{\bar{B},\bar{C},\bar{D},\bar{F}\},\ \{\bar{B},\bar{C},\bar{E},\bar{F}\} \tag{7.15}$$

Here, the nonoccurrence of basic event A is explicitly denoted by $\bar{A}$.

The minimal cut sets of the system 2 failure fault tree are:

$$\{A\},\ \{F\},\ \{G\} \tag{7.16}$$

These path sets and cut sets are combined to yield minimal cut sets of accident sequence 2:

$$\begin{aligned}&\{G,\bar{A},\bar{C},\bar{D},\bar{F}\},\ \{G,\bar{A},\bar{C},\bar{E},\bar{F}\},\ \{G,\bar{B},\bar{C},\bar{D},\bar{F}\},\ \{G,\bar{B},\bar{C},\bar{E},\bar{F}\}\\&\{A,\bar{B},\bar{C},\bar{D},\bar{F}\},\ \{A,\bar{B},\bar{C},\bar{E},\bar{F}\}\end{aligned} \tag{7.17}$$

Here, sets including pairs such as F and $\bar{F}$ are removed from the cut-set candidates.

We have an erroneous cut set $\{F\}$ when the cut set of sequence 2 is replaced by the cut set of system 2 by assuming that system 1 is always functioning.

Suppose that fault trees have no negations of basic events. Then minimal cut sets of an accident sequence are obtained by simply combining path sets and cut sets after removing inconsistent sets including both events and their negations. There is no need to use algorithms to generate so-called “prime implicants”.

7.6 Structure Functions

7.6.1 Definition

Define the 0–1 variable Y_i for basic event i:

$$Y_i = \begin{cases} 1, \text{basic event is occurring} \\ 0, \text{basic event is not occurring} \end{cases} \tag{7.18}$$

Suppose that there are a total of n basic events. Introduce vector variable $Y = (Y_1, \ldots, Y_n)$. The structure function ψ is an algebraic function that returns the value in the following way:

$$\psi(Y) = \begin{cases} 1, \text{top event is occurring} \\ 0, \text{top event is not occurring} \end{cases} \tag{7.19}$$

7.6.2 Simple Systems

AND Gate

We have the following structure function in *algebrac* form for the AND gate:

$$\psi(Y) = \prod_{i=1}^{n} Y_i = Y_1 Y_2 \times \cdots \times Y_n \tag{7.20}$$

OR Gate

The function takes the value of unity when some Y_i assumes zero. Thus, the structure function can be expressed as the algebraic form:

$$\psi(Y) = 1 - \prod_{i=1}^{n} [1 - Y_i] = 1 - [1 - Y_1][1 - Y_2] \times \cdots \times [1 - Y_n] \tag{7.21}$$

This form consists of 1) 1 minus Y_i terms, 2) multiplication of these terms, and 3) 1 minus the multiplication result. For the OR gate with two basic events, we have, after expansion:

$$\psi(Y) = Y_1 + Y_2 - Y_1 Y_2 \tag{7.22}$$

2/3 Gate

The function becomes unity when 2 or 3 basic events occurs:

$$\psi(Y) = 1 - [1 - Y_1 Y_2][1 - Y_2 Y_3][1 - Y_3 Y_1] \tag{7.23}$$

For the 0–1 variable, we note $Y_i^2 = Y_i$. The rhs of Equation 7.23 can be expanded and simplified into:

$$\psi(Y) = Y_1 Y_2 + Y_2 Y_3 + Y_3 Y_1 - 2Y_1 Y_2 Y_3 \tag{7.24}$$

7.6.3 Calculation of Unavailability

Denote by Q_{S} the probability of the top event. This is the probability of the structure function taking the value of unity, which in turn, is calculated by an expected value of the structure function:

$$\begin{aligned} Q_{\mathrm{S}} &= \Pr\{\text{Top event}\} = \Pr\{\psi(Y) = 1\} && (7.25)\\ &= \sum_{Y} \psi(Y)\Pr\{Y\} && (7.26)\\ &= E\{\psi(Y)\} && (7.27) \end{aligned}$$

The structure function is not a logic function but an algebraic function. This suggests that the expected-value operation of Equation 7.27 is relatively easier to carry out.

The expected value is a sum of all probabilities of $\psi(Y) = 1$ on a truth table. Each row of the table represents basic event state vector Y. We have $2^3 = 8$ rows for 3 basic events case. The rows increase exponentially with n and a large amount of calculation is required. The expected-value operation of Equation 7.27 reduces the calculation because it does not rely on the truth-table expression.

Consider, as an example, a 2/3 gate. Assume the occurrence probabilities for the basic events:

$$\Pr\{Y_i = 1\} = E\{Y_i\} = 0.6 \qquad (7.28)$$

The system unavailability $Q_{2/3}$ can be expanded into:

$$\begin{aligned} Q_{2/3} &= E\{\psi(Y)\} && (7.29)\\ &= E\{Y_1Y_2\} + E\{Y_2Y_3\} + E\{Y_3Y_1\} - 2E\{Y_1Y_2Y_3\} && (7.30) \end{aligned}$$

Note that the expected value of a sum of terms is a sum of expected values of the terms. In other words, the plus operation and expected-value operation are mutually interchangeable.

Assume here that the basic events are independent. Then, the expected value of the product of variables is the product of expected values of variables. The product operation and expected-value operation become mutually interchangeable for independent variables:

$$\begin{aligned} Q_{2/3} &= E\{\psi(Y)\} && (7.31)\\ &= E\{Y_1\}E\{Y_2\} + E\{Y_2\}E\{Y_3\} + E\{Y_3\}E\{Y_1\}\\ &\quad -2E\{Y_1\}E\{Y_2\}E\{Y_3\} && (7.32)\\ &= 3 \times 0.6^2 - 2 \times 0.6^3 = 0.648 && (7.33) \end{aligned}$$

The common variable Y_2 is included in terms $1 - Y_1Y_2$ and $1 - Y_2Y_3$ of Equation 7.23. Thus, these two terms are not statistically independent. We confirm the nonequality:

$$0.648 = Q_{2/3} \neq 1 - [1 - 0.6^2]^3 = 0.74 \tag{7.34}$$

We will see later in this chapter that the independent treatment of the dependent terms yields the upper bound of the true system unavailability.

7.6.4 Minimal-cut and Minimal-path Representations

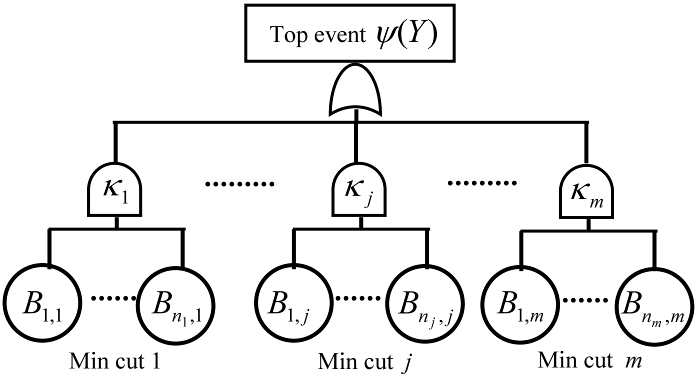


Fig. 7.8. Minimal-cut representation

Minimal-cut Representation

Suppose that the top event has m minimal cut sets:

$$\left.\begin{array}{ll} \{B_{1,1}, B_{2,1}, \ldots, B_{n_1,1}\} & \text{Min cut } 1 \\ \vdots & \\ \{B_{1,j}, B_{2,j}, \ldots, B_{n_j,j}\} & \text{Min cut } j \\ \vdots & \\ \{B_{1,m}, B_{2,m}, \ldots, B_{n_m,m}\} & \text{Min cut } m \end{array}\right\} \tag{7.35}$$

Minimal cut set j consists of n_j basic events. The top event can be represented by the fault tree of Figure 7.8 in terms of minimal cut sets.

Denote by 0–1 variable $Y_{i,j} = 1$ the occurrence of basic event $B_{i,j}$. The second suffix j denotes cut j. The structure function $\kappa_j(Y)$ of minimal cut set j becomes:

$$\kappa_j(Y) = \prod_{i=1}^{n_j} Y_{i,j} \tag{7.36}$$

Here, $\kappa_j = 1$ when the cut set is occurring.

Figure 7.8 yields the following structure function for the top event:

$$\psi(Y) = 1 - \prod_{j=1}^{m} [1 - \kappa_j(Y)] \tag{7.37}$$

This is called a minimal-cut-set representation of the structure function.

Consider, for instance, a 2/3 gate. There are 3 minimal cut sets:

$$\{B_1, B_2\}, \{B_2, B_3\}, \{B_3, B_1\} \tag{7.38}$$

The minimal-cut-set structure-functions are:

$$\kappa_1(Y) = Y_1Y_2,\ \kappa_2(Y) = Y_2Y_3,\ \kappa_3(Y) = Y_3Y_1 \tag{7.39}$$

The minimal-cut representation coincides with Equation 7.23.

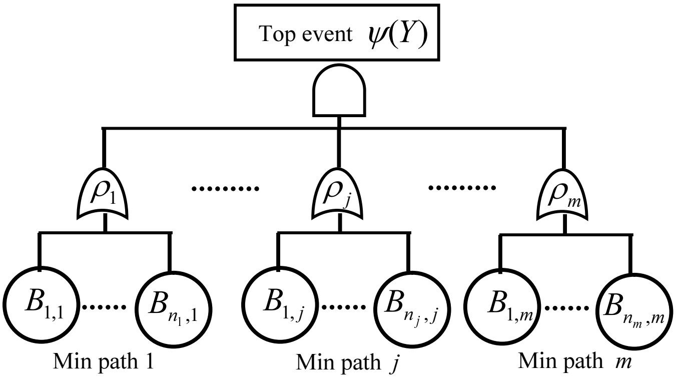


Fig. 7.9. Minimal-path representation

Minimal-path Representation

Suppose that the top event has m minimal path sets:

$$\left.\begin{array}{ll}\{B_{1,1}, B_{2,1}, \ldots, B_{n_1,1}\} & \text{Min path } 1\\ \vdots & \\ \{B_{1,j}, B_{2,j}, \ldots, B_{n_j,j}\} & \text{Min path } j\\ \vdots & \\ \{B_{1,m}, B_{2,m}, \ldots, B_{n_m,m}\} & \text{Min path } m\end{array}\right\} \tag{7.40}$$

Minimal path set j consists of n_j basic events. The top event can be represented by the fault tree of Figure 7.9 in terms of minimal path sets.

Denote by 0–1 variable $Y_{i,j} = 1$ the occurrence of basic event $B_{i,j}$. The second suffix j denotes path j. The structure function $\rho_j(Y)$ of minimal path set j becomes:

$$\rho_j(Y) = 1 - \prod_{i=1}^{n_j} [1 - Y_{i,j}] \tag{7.41}$$

Here, $\rho_j = 1$ when the path set is being nullified.

Figure 7.9 yields the following structure function for the top event:

$$\psi(Y) = \prod_{j=1}^{m} \rho_j(Y) \tag{7.42}$$

Consider, for instance, a 2/3 gate. There are 3 minimal path sets:

$$\{B_1, B_2\}, \{B_2, B_3\}, \{B_3, B_1\} \tag{7.43}$$

The minimal-path-set structure-functions are:

$$\begin{aligned} \rho_1(Y) &= 1 - [1 - Y_1][1 - Y_2] = Y_1 + Y_2 - Y_1Y_2 \\ \rho_2(Y) &= 1 - [1 - Y_2][1 - Y_3] = Y_2 + Y_3 - Y_2Y_3 \\ \rho_3(Y) &= 1 - [1 - Y_3][1 - Y_1] = Y_3 + Y_1 - Y_3Y_1 \end{aligned} \tag{7.44}$$

The minimal-path representation is given by:

$$\psi(Y) = [Y_1 + Y_2 - Y_1Y_2][Y_2 + Y_3 - Y_2Y_3][Y_3 + Y_1 - Y_3Y_1] \tag{7.45}$$

An expansion of this equation results in Equation 7.24.

Unavailability Calculation by Pivot Expansion

The product operation in the minimal-cut representation can not be interchanged by the expected-value operation because terms $[1 - \kappa_j(Y)]$ for different j are statistically dependent in general:

$$Q_S = E\{\psi_Y\} \neq 1 - \prod_{j=1}^{m} [1 - E\{\kappa_j(Y)\}] \tag{7.46}$$

The equality holds in this equation when each basic event appears in exactly one minimal cut set.

Similarly, the product operation in the minimal-path representation can not be interchanged by the expected-value operation:

$$Q_S = E\{\psi_Y\} \neq \prod_{j=1}^{m} E\{\rho_j(Y)\} \tag{7.47}$$

The equality holds when each basic event appears in exactly one minimal path set.

When a basic event appears in more than one minimal cut sets, the common variable Y_i can be made to appear alone in products by the following pivotal expansion:

$$\psi(Y) = Y_i\psi(1_i, Y) + (1 - Y_i)\psi(0_i, Y) \tag{7.48}$$

Symbol $(1_i, Y)$ denotes setting $Y_i = 1$ in vector Y, while $(0_i, Y)$ denotes setting $Y_i = 0$ in Y. When some factors in a product still have common variables, these are removed in a similar way.

Consider the minimal-path representation of Equation 7.45. A pivotal expansion with respect to Y_1 yields:

$$\psi(Y) = Y_1[Y_2 + Y_3 - Y_2Y_3] + [1 - Y_1]Y_2[Y_2 + Y_3 - Y_2Y_3]Y_3 \tag{7.49}$$

This equation still has Y_2 as a common variable in the second term. The expansion with respect to Y_2 gives:

$$\psi(Y) = Y_1[Y_2 + Y_3 - Y_2Y_3] + [1 - Y_1]Y_2Y_3 + [1 - Y_1][1 - Y_2] \times 0 \tag{7.50}$$

Assume a basic event probability of 0.6. The expected-value operation gives the following system unavailability:

$$\begin{aligned} Q_{2/3} &= E\{\psi(Y)\} = E\{Y_1\}[E\{Y_2\} + E\{Y_3\} - E\{Y_2\}E\{Y_3\}] \\ &+ [1 - E\{Y_1\}]E\{Y_2\}E\{Y_3\} && (7.51) \\ &= (0.6)[0.6 + 0.6 - 0.6^2] + [1 - 0.6](0.6)^2 = 0.648 && (7.52) \end{aligned}$$

This coincides with Equation 7.33.

Upper and Lower Bounds of System Unavailability

An upper bound of system unavailability is obtained when the product operation in a minimal-cut representation is interchanged by the expected-value operation. Similarly, a lower bound is obtained when product operation in a minimal-path-set representation is interchanged by the expected-value operation [64]:

$$Q_{\mathrm{S,min}} \equiv \prod_{j=1}^{m(P)} E\{\rho_j(Y)\} \leq Q_{\mathrm{S}} \leq 1 - \prod_{j=1}^{m(C)} [1 - E\{\kappa_j(Y)\}] \equiv Q_{\mathrm{S,max}} \tag{7.53}$$

where $m(C)$ is the total number of minimal cut sets, and $m(P)$ is the total number of minimal path sets.

The lhs of this equation is the unavailability when all paths fail independently. In practice, other paths are more likely to fail when a path fails. Thus, the lhs is an underestimation of the true unavailability.

Term $[1 - E\{\kappa_j(Y)\}]$ is the probability of nonoccurrence of cut j. The product on the rhs is the probability of no cut set failures when these failures are assumed independent. However, in practice, other cuts are less likely to occur when a cut does not occur. Thus, the product on the rhs is an underestimation of the probability of no cut set failures. Hence, the whole rhs is an upper bound of system unavailability.

Consider a 2/3 gate. Assume a basic event probability of $Q = 0.001$. The following results are obtained:

$$Q_{\mathrm{S}} = 3Q^2 - 2Q^3 = 2.998 \times 10^{-6} \tag{7.54}$$

$$Q_{\mathrm{S,min}} = [Q + Q - Q^2]^3 = 8 \times 10^{-9} \tag{7.55}$$

$$Q_{\mathrm{S,max}} = 1 - [1 - Q^2]^3 = 3 \times 10^{-6} \tag{7.56}$$

The upper bound is a good approximation of the true value, but the lower bound is too small.

Monotonically Increasing Structure Function
The bounds of Equation 7.53 hold for a coherent structure function satisfying:

1) $\psi(Y) \geq \psi(X)$ if $Y_i \geq X_i$ for all $i = 1, \ldots, n$,
2) $\psi(Y) = 1$ if $Y = (1, 1, \ldots, 1)$,
3) $\psi(Y) = 0$ if $Y = (0, 0, \ldots, 0)$, and
4) each basic event i appears in at least one minimal cut set.

The first condition is a monotonically increasing requirement where basic events occurring at variable X also occur at variable Y. This condition implies that the system never returns to a normal state by additional occurrences of basic events.

It can be shown that for the monotonically increasing structure function, Equation 7.48 can be simplified to:

$$\psi(Y) = Y_i \psi(1_i, Y) + \psi(0_i, Y) \tag{7.57}$$

In other words, the term $(1 - Y_i)$ can be omitted.

The second condition indicates that the top event occurs when all the basic events occur. A monotonically increasing function without this condition would identically equal zero.

The third condition indicates that the top event does not occur when none of the basic event occurs. A monotonically increasing function without this condition would identically equal one. The forth condition implies that basic events included in the structure function are all relevant. The most important condition of the coherent structure function is the first condition.

7.6.5 Inclusion-exclusion Formula

Exact Solution
Denote by d_j the occurrence of all basic events in minimal cut j. Top event T becomes a union event of cut set events d_js where m is the total number of cut sets:

$$T = \bigcup_{j=1}^{m} d_j \tag{7.58}$$

System unavailability is the probability of the union event. This probability can be expanded in the following way:

$$Q_\mathrm{S} = \Pr\{\bigcup_{j=1}^{m} d_j\} \tag{7.59}$$

$$\begin{aligned} &= \sum_{j=1}^{m} \Pr\{d_j\} - \sum_{1 \le j < k \le m} \Pr\{d_j \cap d_k\} \\ &+ \cdots + (-1)^{r-1} \sum_{1 \le j_1 < j_2 < \cdots < j_r \le m} \Pr\{d_{j_1} \cap d_{j_2} \cap \cdots \cap d_{j_r}\} \\ &+ \cdots + (-1)^{m-1} \Pr\{d_1 \cap d_2 \cap \cdots \cap d_m\} \end{aligned} \tag{7.60}$$

This expansion is called an inclusion-exclusion formula. The probability of a union event is expanded into the sum of more tractable probabilities of intersection events. Term r is a contribution by simultaneous occurrence of r minimal cut sets.

Consider a 2/3 system. Basic event probabilities are assumed to be 0.6. Cut set events d_js are:

$$d_1 = B_1 \cap B_2,\ d_2 = B_2 \cap B_3,\ d_3 = B_3 \cap B_1 \tag{7.61}$$

The inclusion-exclusion formula yields:

$$Q_\mathrm{S} = A - B + C \tag{7.62}$$

$$A \equiv \Pr\{d_1\} + \Pr\{d_2\} + \Pr\{d_3\} = Q^2 + Q^2 + Q^2 = 3Q^2 \tag{7.63}$$

$$\begin{aligned} B &\equiv \Pr\{d_1 \cap d_2\} + \Pr\{d_2 \cap d_3\} + \Pr\{d_3 \cap d_1\} \\ &= Q^3 + Q^3 + Q^3 = 3Q^3 \end{aligned} \tag{7.64}$$

$$C \equiv \Pr\{d_1 \cap d_2 \cap d_3\} = Q^3 \tag{7.65}$$

The basic event probability of 0.6 gives:

$$A = 1.08,\ \ B = 0.648,\ \ C = 0.216,\ \ Q_\mathrm{S} = 0.648. \tag{7.66}$$

Lower and Upper Bounds
The following inequalities hold:

$$\begin{aligned} Q_{\mathrm{S,min}} &\equiv \sum_{j=1}^{m} \Pr\{d_j\} - \sum_{1 \le j < k \le m} \Pr\{d_j \cap d_k\} \\ &\le Q_\mathrm{S} \le \sum_{j=1}^{m} \Pr\{d_j\} \equiv Q_{\mathrm{S,max}} \end{aligned} \tag{7.67}$$

Consider again the 2/3 system. Assume a relatively small probability $Q = 0.001$ for each basic event. The inequalities become:

$$A = 3 \times 10^{-6}, B = 3 \times 10^{-9}, C = 10^{-9} \tag{7.68}$$

$$Q_\mathrm{S} = A - B + C = 2.998 \times 10^{-6} \tag{7.69}$$

$$Q_{\mathrm{S,min}} = A - B = 2.997 \times 10^{-6} \tag{7.70}$$

$$Q_{\mathrm{S,max}} = A = 3 \times 10^{-6} \tag{7.71}$$

Note that the lower bound of Equation 7.70 is far more precise than that of Equation 7.55. The upper bound is a sum of cut set probabilities. This is called a rare-event approximation.

7.7 False and Inactive Alarms

Suppose that a plant is monitored by two or more sensors. The plant is shutdown when the sensor system as a whole detects an abnormal plant state and issues an alarm. One requirement for such a sensor system is to decrease false alarms as well as a lack of alarms when needed.

7.7.1 Alarm-generating Function

Consider a sensor system consisting of n sensors not necessarily identical. Denote by y_i the existence of an alarm from sensor i:

$$y_i = \begin{cases} 1, & \text{sensor } i \text{ is issuing alarm} \\ 0, & \text{otherwise} \end{cases} \tag{7.72}$$

Vector $y \equiv (y_1, \ldots, y_n)$ represents a state of n sensors. Introduce a coherent structure function $\psi(y)$ to represent the output from the sensor system as a whole:

$$\psi(y) = \begin{cases} 1, & \text{sensor system is issuing alarm} \\ 0, & \text{otherwise} \end{cases} \tag{7.73}$$

This function is called an alarm-generating function, specifying the alarm-generating logic based on the state of sensors. Examples of the alarm-generating function are:

1) Series system: $\psi(y_1, y_2) = y_1 y_2$. The system issues the alarm when both sensors generate the alarm simultaneously. The sensor alarm generation is regarded as a signal transmission, and hence the term series system.
2) Parallel system: $\psi(y_1, y_2) = 1 - (1 - y_1)(1 - y_2)$. The parallel system issues the alarm when either sensor (or both) issues the alarm.
3) 2/3 system: $\psi(y_1, y_2, y_3) = 1 - (1 - y_1 y_2)(1 - y_2 y_3)(1 - y_3 y_1)$. The system issues the alarm when two or more sensors generate the alarm.

The alarm-generating logic can be specified by a truth table that, in turn, is expressed as an equation:

$$\psi(y) = \sum_u \psi(u) \left[\prod_{i=1}^{n} y_i^{u_i} (1 - y_i)^{1-u_i} \right] \tag{7.74}$$

The 2/3 system gives the following expression:

$$\begin{aligned}\psi(y) &= y_1^0(1-y_1)^1 y_2^1(1-y_2)^0 y_3^1(1-y_3)^0 \\ &+ y_1^1(1-y_1)^0 y_2^0(1-y_2)^1 y_3^1(1-y_3)^0 \\ &+ y_1^1(1-y_1)^0 y_2^1(1-y_2)^0 y_3^0(1-y_3)^1 \\ &+ y_1^1(1-y_1)^0 y_2^1(1-y_2)^0 y_3^1(1-y_3)^0 \qquad (7.75) \\ &= (1-y_1)y_2y_3 + y_1(1-y_2)y_3 + y_1y_2(1-y_3) + y_1y_2y_3 \qquad (7.76)\end{aligned}$$

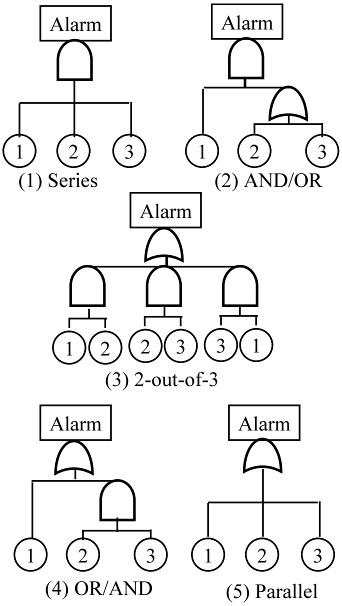


Fig. 7.10. Coherent alarm-generating functions

Consider systems consisting of 3 sensors. Figure 7.10 enumerates all the structures of alarm-generating functions that are coherent. A permutation of sensor IDs results in a different function with the same structure as cases (2) and (4).

7.7.2 False-alarm Function

Consider a normal plant state. Sensor i is subject to a false-alarm failure if it is generating an alarm. Thus, variable y_i can be interpreted as:

$$y_i = \begin{cases} 1, & \text{if sensor } i \text{ is generating a false alarm} \\ 0, & \text{otherwise} \end{cases} \qquad (7.77)$$

The false-alarm function ψ_{FA} of the sensor system describes the generation of a system false alarm in terms of a sensor false-alarm state y:

$$\psi_{\mathrm{FA}}(y) = \begin{cases} 1, & \text{if sensor system is generating a false alarm} \\ 0, & \text{otherwise} \end{cases} \tag{7.78}$$

Here, suffix FA stands for "false alarm". Since the system alarm is generated according to the alarm-generating function, the false-alarm function ψ_{FA} coincides with ψ when the interpretation of y_i is changed to the one in Equation 7.77:

$$\psi_{\mathrm{FA}}(y) = \psi(y) \tag{7.79}$$

Consider the alarm function $\psi(y) = y_1 y_2$ for a two-sensor series system. The false-alarm function is also given by:

$$\psi_{\mathrm{FA}}(y) = y_1 y_2 \tag{7.80}$$

In other words, the series system is subject to a false-alarm failure when both sensors 1 and 2 generate the false alarm.

7.7.3 Inactive-alarm Function

Consider an abnormal plant state. The sensor is normal when it is generating an alarm. Otherwise, the sensor is subject to an inactive-alarm failure. Define complementary variable $\bar{y}_i \equiv 1 - y_i$ of y_i. Since the plant state is abnormal, this variable can be interpreted as:

$$\bar{y}_i \equiv 1 - y_i = \begin{cases} 1, & \text{if sensor } i \text{ is inactive} \\ 0, & \text{otherwise} \end{cases} \tag{7.81}$$

The inactive-alarm function ψ_{IA} of the sensor system describes the lack of a system alarm in terms of inactive failure state $\bar{y}$ at the sensor level:

$$\psi_{\mathrm{IA}}(\bar{y}) = \begin{cases} 1, & \text{if sensor system is inactive} \\ 0, & \text{otherwise} \end{cases} \tag{7.82}$$

Here, suffix IA stands for "inactive alarm".

The inactive-alarm function takes the value of zero if and only if the alarm-generating function ψ generates the alarm under state $y = 1 - \bar{y}$. Thus,

$$\psi_{\mathrm{IA}}(\bar{y}) = 1 - \psi(1 - \bar{y}) \tag{7.83}$$

Consider the series system $\psi(y) = y_1 y_2$. The inactive-alarm function becomes:

$$\psi_{\mathrm{IA}}(\bar{y}) = 1 - (1 - \bar{y}_1)(1 - \bar{y}_2) = \bar{y}_1 + \bar{y}_2 - \bar{y}_1 \bar{y}_2 \tag{7.84}$$

In other words, the sensor system becomes inactive when sensor 1 or 2 becomes inactive.

7.7.4 False-alarm and Inactive-alarm Probabilities

Suppose that the plant state is either normal or abnormal. For simplicity, consider a single monitoring trial since continuous monitoring becomes more complicated because of the time-average treatment.

Demand Probability
The plant state is denoted by variable x:

$$x = \begin{cases} 1, & \text{if plant state is abnormal} \\ 0, & \text{otherwise} \end{cases} \tag{7.85}$$

Demand probability p is the probability of the abnormal plant state at the monitoring trial instant:

$$p \equiv \Pr\{x = 1\} \tag{7.86}$$

False-alarm Probability
The false-alarm probability of sensor i is defined by:

$$a_i \equiv \Pr\{y_i = 1 | x = 0\} \tag{7.87}$$

This is the probability of an alarm, given the normal plant state at the trial instant.

The false-alarm probability of the sensor system is defined similarly by a conditional probability:

$$a_{\mathrm{S}} \equiv \Pr\{\psi_{\mathrm{FA}}(y) = 1 | x = 0\} = E\{\psi(y) | x = 0\} \tag{7.88}$$

Assume independent failures of sensors. The expected-value operation can be applied to Equation 7.74:

$$a_{\mathrm{S}} = \sum_u \psi(u) \left[\prod_{i=1}^{n} a_i^{u_i} (1 - a_i)^{1-u_i} \right] \equiv h(a) \tag{7.89}$$

$$a \equiv (a_1, a_2, \ldots, a_n) \tag{7.90}$$

Function h is called a reliability function.

Inactive-alarm Probability
The inactive-alarm probability of sensor i is defined by:

$$b_i \equiv \Pr\{y_i = 0 | x = 1\} \tag{7.91}$$

The inactive alarm probability of the sensor system is defined similarly by a conditional probability:

$$b_{\mathrm{S}} = E\{1 - \psi(1 - \bar{y}) | x = 1\} \tag{7.92}$$

For independent sensor failures, this probability can be calculated from the reliability function:

$$b_{\mathrm{S}} = 1 - h(1 - b), \quad b \equiv (b_1, b_2, \ldots, b_n) \tag{7.93}$$

The reliability function for the series system is:

Table 7.6. False-alarm and inactive-alarm probabilities for a 3-sensor system

(a) Different sensors

Type	(1) Series	(2) AND-OR	(3) 2/3	(4) OR-AND	(5) Parallel
a_S	$a_1a_2a_3$	$a_1a_2 + a_1a_3$ $-a_1a_2a_3$	$a_1a_2 + a_1a_3$ $+a_2a_3$ $-2a_1a_2a_3$	$a_1 + a_2a_3$ $-a_1a_2a_3$	$a_1 + a_2 + a_3$ $-a_1a_2 - a_1a_3$ $-a_2a_3$ $+a_1a_2a_3$
b_S	$b_1 + b_2 + b_3$ $-b_1b_2 - b_1b_3$ $-b_2b_3$ $b_1b_2b_3$	$b_1 + b_2b_3$ $-b_1b_2b_3$	$b_1b_2 + b_1b_3$ $+b_2b_3$ $-2b_1b_2b_3$	$b_1b_2 + b_1b_3$ $-b_1b_2b_3$	$b_1b_2b_3$

(b) Identical sensors

Type	(1) Series	(2) AND-OR	(3) 2/3	(4) OR-AND	(5) Parallel
a_S	a^3	$2a^2 - a^3$	$3a^2 - 2a^3$	$a + a^2 - a^3$	$3a - 3a^2 + a^3$
b_S	$3b - 3b^2 + b^3$	$b + b^2 - b^3$	$3b^2 - 2b^3$	$2b^2 - b^3$	b^3

$$h(y) = y_1y_2, \text{ for series system} \tag{7.94}$$

The false-alarm and inactive-alarm probabilities are:

$$a_\mathrm{S} = a_1a_2 \tag{7.95}$$

$$b_\mathrm{S} = 1 - (1 - b_1)(1 - b_2) = b_1 + b_2 - b_1b_2 \tag{7.96}$$

Table 7.6 lists the false-alarm and inactive-alarm probabilities for the coherent 3-sensor systems in Figure 7.10. The following inequalities hold when the 3 sensors are identical:

$$a_\mathrm{S}^{(1)} \leq a_\mathrm{S}^{(2)} \leq a_\mathrm{S}^{(3)} \leq a_\mathrm{S}^{(4)} \leq a_\mathrm{S}^{(5)} \tag{7.97}$$

$$b_\mathrm{S}^{(1)} \geq b_\mathrm{S}^{(2)} \geq b_\mathrm{S}^{(3)} \geq b_\mathrm{S}^{(4)} \geq b_\mathrm{S}^{(5)} \tag{7.98}$$

We see that both types of the probabilities can be reduced by the 2/3 structure.

7.8 Concluding Remarks

The system-level analyses described in this chapter have been computerized by PRA codes. Proper understanding of the concept and analysis is important to use the computer codes. For instance, rare-event cut sets or accident sequences are truncated to make computation feasible. However, the truncation can not be justified when a component ensuring the rare event is a target of design modification.

8

Dependent Failure Quantification

8.1 Introduction

Risk reduction almost always would succeed if there were no dependent failures. The dependent failure is a source of a collapse of dependable risk reduction. Some dependencies are modeled explicitly in PRA, while others are dealt with by common-cause failure analysis. This chapter first describes a relatively recent methodology called the alpha-factor model for common-cause quantification. The well-known beta-factor model can be regarded as a variant of the alpha-factor model. The second dependency described in this chapter is a graceful degradation process where changes to inferior states occur in a gradual manner. The graceful or gradual degradation is a key approach to problems with risks because time is available to correct the current inferior situation.

8.2 Common-cause Failures

The redundancy does not necessarily lead to substantial improvement if common-cause failures exist. There are several models for quantifying systems subject to common-cause failures [34]. The beta-factor model is the most basic. A generalization of the beta-factor model is the multiple-Greek letter (MGL) model. A basic parameter (BP) model is equivalent to the MGL model.

In this section we focus on an alpha-factor model because 1) this has a direct relation to the failure data, 2) the parameter-estimator distribution is available in a Bayes framework, and 3) the model is simple, more understandable, and is becoming a standard.

In the following description, we assume that explicit relations such as functional and common-unit dependencies are expressed by logic models such as fault and event trees, and component-level minimal cut sets are available.

Candidates for common-cause failures include [5]: 1) motor-operated valves, 2) pumps, 3) safety-relief valves, 4) air-operated valves, 5) solenoid-operated valves, 6) check valves, 7) diesel generators, 8) batteries, 9) inverters and battery charger, and 10) circuit breakers.

In the common-cause analysis models, a redundant system failure is classified as either of the following:

1) Failure on demand: A redundant configuration fails to start operating due to a latent or random defect.
2) Failure during operation, that is, failure to continue to run.

This section mainly deals with the first case because the second case can be dealt with similarly.

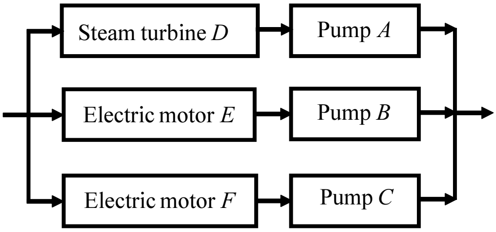


Fig. 8.1. Triple-train system with diversity of actuator

8.2.1 Cause-level Analysis

Figure 8.1 shows a triplex system consisting of pumps and actuators. The 3 pumps A, B and C are the same type but the actuators are different: the actuator of pump A is a steam turbine D, while pump B and C are actuated by electric motors E and F. The success criterion requires one or more functioning trains, *i.e.* 1/3 structure. The top event is expressed by the following logic:

$$\text{Top} = (A \vee D) \wedge (B \vee E) \wedge (C \vee F) \tag{8.1}$$

Symbol A is a failure of pump A, D is a failure of turbine D, and E a failure of motor E, *etc.* Symbol $\vee$ is logic OR, and $\wedge$ is logic AND. Ordinary multiplication is frequently used for $\wedge$.

Consider causes of the pump failure.

1) C_A, C_B, C_C:Independent failures of pump A, B, and C, respectively. These are causes of single-component failures.
2) C_{AB}, C_{AC}, C_{BC}:Simultaneous failures of pumps (A, B), (A, C), and (B, C), respectively. These are causes of double-component failures.
3) C_{ABC}:A simultaneous failure of the all three pumps. This is a cause of the triplet-component failure.

Causes C_E, C_F and C_{EF} can be defined in a similar way for the electric motors. The turbine failure is denoted by C_D.

The top event can be rewritten in terms of causes:

$$\begin{aligned}\text{Top} = &(C_A \vee C_{AB} \vee C_{AC} \vee C_{ABC} \vee C_D)\\ &\wedge (C_B \vee C_{AB} \vee C_{BC} \vee C_{ABC} \vee C_E \vee C_{EF})\\ &\wedge (C_C \vee C_{AC} \vee C_{BC} \vee C_{ABC} \vee C_F \vee C_{EF})\end{aligned} \tag{8.2}$$

It should be noted that common causes are considered only for groups of the same type of components, *i.e.* 1) pumps or 2) motors. These groups are called common-cause component groups. Common causes between different types of components can be dealt with similarly.

As noted earlier in Equation 7.57, the following equation is easily verified for a monotonically increasing function $\psi(Y)$:

$$\psi(Y) = Y_i\psi(1_i, Y) \vee \psi(0_i, Y) \tag{8.3}$$

In other words, negation $(1 - Y_i)$ disappears for pivot variable Y_i.

Consider a sequence of pivot variables: C_{ABC}, C_{AB}, C_{BC}, C_{AC}, and C_{EF}. The top event of Equation 8.2 can eventually be written as:

$$\begin{aligned}\text{Top} = &C_{ABC} \vee (C_{AB}C_{AC} \vee C_{AB}C_{BC} \vee C_{AC}C_{BC})\\ &\vee (C_{AB}C_C \vee C_{BC}C_A \vee C_{AC}C_B)\\ &\vee (C_{AB}C_{EF} \vee C_{AC}C_{EF}) \vee (C_{AB}C_F \vee C_{AC}C_E)\\ &\vee C_{BC}C_D \vee C_{EF}C_D \vee C_{EF}C_A\\ &\vee (C_A \vee C_D)(C_B \vee C_E)(C_C \vee C_F)\end{aligned} \tag{8.4}$$

where the logic AND is expressed by algebraic product. Logic OR is sometimes expressed by albraic sum. The last term on the rhs is a contribution by independent causes.

Suppose that the microscopic causes producing these failures occur independently. Approximate the probability of a union event by a sum of probabilities of elementary events in the union. The symmetry yields the following expression for the top-event probability:

$$\begin{aligned}\Pr\{\text{Top}\} \simeq &Q_{P,3} + 3Q_{P,2}^2 + 3Q_{P,2}Q_{P,1} + 2Q_{P,2}Q_{M,2} + 2Q_{P,2}Q_{M,1}\\ &+ Q_{P,2}Q_{T,1} + Q_{M,2}Q_{T,1} + Q_{M,2}Q_{P,1}\\ &+ (Q_{P,1} + Q_{T,1})(Q_{P,1} + Q_{M,1})^2\end{aligned} \tag{8.5}$$

Term $Q_{P,3}$ is the probability that the 3 pumps fail simultaneously. $Q_{P,2}$ is the probability that pump A and B fail but pump C does not. By symmetry, this equals the probability that pump A and C fail without pump B failure.

Consider a subset consisting of k pumps. In general, $Q_{P,k}$ is the probability that all the pumps in the specific subset fail without a failure of the remaining pumps outside the subset.

Remove simultaneous occurrences of overlapping causes such as $C_{AB}C_{AC}$ [34]. Then, $3Q_{P,2}^2$ can be removed from Equation 8.5:

$$\begin{aligned}\Pr\{\text{Top}\} \simeq\ & Q_{P,3} + 3Q_{P,2}Q_{P,1} + 2Q_{P,2}Q_{M,2} + 2Q_{P,2}Q_{M,1} \\ & + Q_{P,2}Q_{T,1} + Q_{M,2}Q_{T,1} + Q_{M,2}Q_{P,1} \\ & + (Q_{P,1} + Q_{T,1})(Q_{P,1} + Q_{M,1})^2 \end{aligned} \tag{8.6}$$

The top-event probability can be calculated from the following probabilities.

1) $Q_{P,3}$, $Q_{P,2}$, $Q_{P,1}$: for the pumps.
2) $Q_{M,2}$, $Q_{M,1}$: for the electric motors.
3) $Q_{T,1}$: for the steam turbine.

These are typically probabilities of failure to start. Other cases include failure rates to describe failure to continue the operation.

Past failure data yield a total failure-probability for a pump due to independent and common causes. This total probability is available from a generic plant database or a plant-specific database. The probability varies from plant to plant. The common-cause parameters are introduced to determine ratios of common causes. These ratios represent different degrees of simultaneity of failures, given a component type, and frequently remain constant for different plants. Common-cause failure probabilities $Q_{P,3}$, $Q_{P,2}$ and independent failure probability $Q_{P,1}$, for instance, are determined from the total failure-probability and ratio parameters.

In the following sections we describe two approaches to modeling the ratio parameters; the alpha-factor model and the beta-factor model.

8.2.2 Alpha-factor Model

This section briefly describes the alpha-factor model of NUREG/CR-5485 [34].

Common-cause Component Group (CCCG)

This is defined as a group of components that are considered to have a high potential for failure due to the same cause or causes. These components are usually similar in mission, manufacturer, maintenance, environment, *etc.* (see Section 3.4.2).

The triple-train system of Figure 8.1 consists of three CCCGs: 1) pump A, B, and C; 2) electric motor E, and F; 3) steam turbine D. The third group consists of only one component.

Common-cause Basic Event (CCBE) Probability

A definition of a basic event is now extended to an event in a reliability logic model that represents the state in which a component or a *group* of components is unavailable [34]. As before, the basic event does not require further development.

m=1			m=2				m=3					m=4					
k		A	k		A	B	k		A	B	C	k		A	B	C	D
1	1	▨	1	1	▨		1	1	▨			1	1	▨			
				2		▨		2		▨			2		▨		
			2	1	▨	▨		3			▨		3			▨	
							2	1	▨	▨			4				▨
								2	▨		▨	2	1	▨	▨		
								3		▨	▨		2	▨		▨	
							3	1	▨	▨	▨		3	▨			▨
													4		▨	▨	
													5		▨		▨
													6			▨	▨
												3	1	▨	▨	▨	
													2	▨	▨		▨
													3	▨		▨	▨
													4		▨	▨	▨
												4	1	▨	▨	▨	▨

Fig. 8.2. Simultaneous failures of k components out of a common-cause component group of size m

Consider a CCCG consisting of m components. Introduce the following symbol:

$$Q_k^{(m)} \equiv \text{probability of a basic event involving a \textit{specific} set of } k \text{ components } (1 \leq k \leq m) \text{ in a CCCG of size } m \qquad (8.7)$$

In general, this probability is a function of size m and k:

$$Q_k^{(m)} \neq Q_k^{(l)}, \;\; m \neq l \qquad (8.8)$$

A common-cause basic event (CCBE) is defined as a basic event that represents the unavailability of a *specific* set of components. The CCBE is caused by shared causes that are not explicitly represented in the system logic model as other basic events. Thus, $Q_k^{(m)}$ is the probability of CCBE of size k in CCCG of size m.

Note that a symmetry assumption is used to make the probability of each CCBE independent of the specific combination of components affected; it is only dependent on the number k of components being failed [34].

Start Failure and Run Failure

A run failure is when the component fails to continue its operation when the operation starts successfully. The symbol $Q_k^{(m)}$ then represents a failure rate $\lambda_k^{(m)}$ per unit time, not a probability.

The run-failure probability after the time span T of continuous operation is approximated by $\lambda_k^{(m)}T$. Similar relations to the start failure case hold for the run failures.

Example: CCCG up to Four Components
Figure 8.2 enumerates CCBEs for CCCG with size from 1 to 4. For the CCCG with size 4, we have the following CCBEs.

1) Independent cause impacting one component: C_A, C_B, C_C, and C_D. Each has probability $Q_1^{(4)}$.
2) Common cause impacting two components: C_{AB}, C_{AC}, C_{AD}, C_{BC}, C_{BD}, and C_{CD}. Each has probability $Q_2^{(4)}$.
3) Common cause impacting three components: C_{ABC}, C_{ABD}, C_{ACD}, and C_{BCD}. Each has probability $Q_3^{(4)}$.
4) Common cause impacting four components: C_{ABCD}. This has probability $Q_4^{(4)}$.

Note that a CCBE is caused by a specific common cause:

Number of CCBEs
The total number of CCBEs with fixed size k is:

$$\binom{m}{k} \equiv \frac{m!}{k!(m-k)!} \tag{8.9}$$

The total number of CCBEs for size $1 \le k \le m$ is:

$$\sum_{k=1}^{m} \binom{m}{k} = 2^m - 1 \tag{8.10}$$

The total number of CCBEs with size k including component A is:

$$\binom{m-1}{k-1} \equiv \frac{(m-1)!}{(k-1)!(m-k)!} \tag{8.11}$$

Probability of Simultaneous Failure of k Components
Denote by q_k^m the following probability:

$$\begin{aligned} q_k^{(m)} \equiv\ & \text{probability of event involving } k \text{ component failures} \\ & (1 \le k \le m) \text{ in a CCCG of size } m \end{aligned} \tag{8.12}$$

This probability should not be confused with Q_k^m. Probability $q_3^{(4)}$, for instance, is:

$$q_3^{(4)} = \Pr\{C_{ABC} \vee C_{ABD} \vee C_{ACD} \vee C_{BCD}\} \tag{8.13}$$

while $Q_3^{(4)}$ is:

$$Q_3^{(4)} = \Pr\{C_{ABC}\} = \Pr\{C_{ABD}\} = \Pr\{C_{ACD}\} = \Pr\{C_{BCD}\} \tag{8.14}$$

A rare-event approximation yields the first term of the inclusion-exclusion formula for $q_3^{(4)}$:

$$q_3^{(4)} = \Pr\{C_{ABC}\} + \Pr\{C_{ABD}\} + \Pr\{C_{ACD}\} + \Pr\{C_{BCD}\} = 4Q_3^{(4)} \quad (8.15)$$

In general, we have the equality:

$$q_k^{(m)} = \binom{m}{k} Q_k^{(m)} \tag{8.16}$$

Component Total Failure-probability

A total failure-probability Q_{T} of component A in a CCCG with $m = 4$ under the rare-event approximation becomes:

$$\begin{aligned} Q_{\mathrm{T}} = \Pr\{C_A\} + {} & \Pr\{C_{AB}\} + \Pr\{C_{AC}\} + \Pr\{C_{AD}\} \\ + {} & \Pr\{C_{ABC}\} + \Pr\{C_{ABD}\} + \Pr\{C_{ACD}\} \\ + {} & \Pr\{C_{ABCD}\} \qquad (8.17) \\ = {} & Q_1^{(4)} + 3Q_2^{(4)} + 3Q_3^{(4)} + Q_4^{(4)} \qquad (8.18) \end{aligned}$$

Equation 8.11 yields a general expression of the total failure-probability of a component in a CCCG with size m:

$$Q_{\mathrm{T}} = \sum_{k=1}^{m} \binom{m-1}{k-1} Q_k^{(m)} \tag{8.19}$$

Definition of Parameter Alpha

Probability of occurrence of CCBE is:

$$\sum_{k=1}^{m} q_k^{(m)} = \sum_{k=1}^{m} \binom{m}{k} Q_k^{(m)} \tag{8.20}$$

The alpha-factor parameters are defined as ratio parameters:

$$\alpha_k^{(m)} = \frac{q_k^{(m)}}{\sum_{k=1}^{m} q_k^{(m)}} = \frac{\binom{m}{k} Q_k^{(m)}}{\sum_{k=1}^{m} \binom{m}{k} Q_k^{(m)}} \tag{8.21}$$

The denominator is the probability of CCBE, while the numerator is the probability of events involving k component failures in a CCCG of m components. In other words:

$$\begin{aligned} \alpha_k^{(m)} \equiv {} & \text{probability that the CCBE involves failure of } k \text{ components,} \\ & \text{given that a CCBE occurs in a CCCG of size } m. \end{aligned} \tag{8.22}$$

This is a conditional probability. Obviously,

$$\sum_{k=1}^{m} \alpha_k^{(m)} = 1 \tag{8.23}$$

For example, for a group of four similar components we have:

$$\begin{aligned}
\alpha_1^{(4)} &= \frac{4Q_1^{(4)}}{4Q_1^{(4)} + 6Q_2^{(4)} + 4Q_3^{(4)} + Q_4^{(4)}} \\
\alpha_2^{(4)} &= \frac{6Q_2^{(4)}}{4Q_1^{(4)} + 6Q_2^{(4)} + 4Q_3^{(4)} + Q_4^{(4)}} \\
\alpha_3^{(4)} &= \frac{4Q_3^{(4)}}{4Q_1^{(4)} + 6Q_2^{(4)} + 4Q_3^{(4)} + Q_4^{(4)}} \\
\alpha_4^{(4)} &= \frac{Q_4^{(4)}}{4Q_1^{(4)} + 6Q_2^{(4)} + 4Q_3^{(4)} + Q_4^{(4)}} \qquad (8.24)
\end{aligned}$$

CCBE Probability in Parametric Form
Equations 8.19 and 8.21 yield an expression of CCBE probability $Q_k^{(m)}$ in terms of total component-failure-probability Q_{T} and alpha-factor parameters [34]:

$$Q_k^{(m)} = \frac{m}{\binom{m}{k}} \frac{\alpha_k^{(m)}}{\alpha_{\mathrm{T}}} Q_{\mathrm{T}} \tag{8.25}$$

where

$$\alpha_{\mathrm{T}} \equiv \sum_{k=1}^{m} k\alpha_k^{(m)} \tag{8.26}$$

Table 8.1 shows the expressions up to $m = 4$.

2-Component CCCG
Consider a 2-component CCCG consisting of component A and B. The top event of a 1-out-of-2 system becomes:

$$\begin{aligned}
T_{1/2} &= (C_A \vee C_{AB})(C_B \vee C_{AB}) && (8.27) \\
&= C_A C_B \vee C_{AB} && (8.28)
\end{aligned}$$

A rare-event approximation yields the following expression for the top-event probability $Q_{1/2}$:

$$Q_{1/2} = Q_1^2 + Q_2 \tag{8.29}$$

where the superscript (2) representing m is omitted.

Similarly, the top event of a 2oo2 system becomes:

$$\begin{aligned}
T_{2/2} &= (C_A \vee C_{AB}) \vee (C_B \vee C_{AB}) && (8.30) \\
&= C_A \vee C_B \vee C_{AB} && (8.31)
\end{aligned}$$

A rare-event approximation yields the following expression:

$$Q_{2/2} = 2Q_1 + Q_2 \tag{8.32}$$

Table 8.1. Parametric representation of CCBE probability

m	k	CCBE prob. $Q_k^{(m)}$
2	1	$Q_1^{(2)} = \frac{\alpha_1}{\alpha_\mathrm{T}} Q_\mathrm{T}$
2	2	$Q_2^{(2)} = \frac{2\alpha_2}{\alpha_\mathrm{T}} Q_\mathrm{T}$
3	1	$Q_1^{(3)} = \frac{\alpha_1}{\alpha_\mathrm{T}} Q_\mathrm{T}$
3	2	$Q_2^{(3)} = \frac{\alpha_2}{\alpha_\mathrm{T}} Q_\mathrm{T}$
3	3	$Q_3^{(3)} = \frac{3\alpha_3}{\alpha_\mathrm{T}} Q_\mathrm{T}$
4	1	$Q_1^{(4)} = \frac{\alpha_1}{\alpha_\mathrm{T}} Q_\mathrm{T}$
4	2	$Q_2^{(4)} = \frac{2\alpha_2}{3\alpha_\mathrm{T}} Q_\mathrm{T}$
4	3	$Q_3^{(4)} = \frac{\alpha_3}{\alpha_\mathrm{T}} Q_\mathrm{T}$
4	4	$Q_4^{(4)} = \frac{4\alpha_4}{\alpha_\mathrm{T}} Q_\mathrm{T}$

3-Component CCCG
The top event of a 1oo3 consisting of A, B, and C becomes:

$$\begin{aligned} T_{1/3} &= (C_A \vee C_{AB} \vee C_{AC} \vee C_{ABC})(C_B \vee C_{AB} \vee C_{BC} \vee C_{ABC}) \\ &\quad \wedge (C_C \vee C_{AC} \vee C_{BC} \vee C_{ABC}) \qquad (8.33) \\ &= C_A C_B C_C \vee C_A C_{BC} \vee C_B C_{AC} \vee C_C C_{AB} \vee C_{ABC} \qquad (8.34) \end{aligned}$$

Note that overlapping CCBEs such as $C_{AB}C_{BC}$ are removed for simplicity and because of past data that these contributions are relatively smaller than the nonoverlapping (*i.e.* exclusive) CCBEs.

The rare-event approximation yields:

$$Q_{1/3} = Q_1^3 + 3Q_1Q_2 + Q_3 \qquad (8.35)$$

Minimal Cut Sets of Voting Systems
Minimal cut sets can be obtained in a similar way for other k-out-of-n systems. These are summarized in Table 8.2. Refer to [34] for more expressions. Only nonoverlapping combinations are considered.

Failure Probabilities of Voting Systems
Table 8.3 lists algebraic equations for the failure of the voting systems obtained as the first term of the inclusion-exclusion formula using the minimal cut sets in Table 8.2. First-order approximations neglecting the second- and higher-order terms are also given. The corresponding table in Reference [34] does not contain the first-order independent failure contributions such as $2Q_1$ to 2oo2.

Table 8.2. Minimal cut sets of voting systems

Case	Minimal cut sets. Overlapping ones are excluded.
1oo2	$\{C_A, C_B\}, \{C_{AB}\}$
2oo2	$\{C_A\}, \{C_B\}, \{C_{AB}\}$
1oo3	$\{C_A, C_B, C_C\}, \{C_A, C_{BC}\}, \{C_B, C_{AC}\}, \{C_C, C_{AB}\}, \{C_{ABC}\}$
2oo3	$\{C_A, C_B\}, \{C_A, C_C\}, \{C_B, C_C\}, \{C_{AB}\}, \{C_{AC}\}, \{C_{BC}\}, \{C_{ABC}\}$
3oo3	$\{C_A\}, \{C_B\}, \{C_C\}, \{C_{AB}\}, \{C_{AC}\}, \{C_{BC}\}, \{C_{ABC}\}$
1oo4	$\{C_A, C_B, C_C, C_D\}, \{C_{AB}, C_{CD}\}, \{C_{AC}, C_{BD}\}, \{C_{AD}, C_{BC}\},$ $\{C_A, C_{BCD}\}, \{C_B, C_{ACD}\}, \{C_C, C_{ABD}\}, \{C_D, C_{ABC}\},$ $\{C_A, C_B, C_{CD}\}, \{C_A, C_C, C_{BD}\}, \{C_A, C_D, C_{BC}\},$ $\{C_B, C_C, C_{AD}\}, \{C_B, C_D, C_{AC}\}, \{C_C, C_D, C_{AB}\}, \{C_{ABCD}\}$
2oo4	$\{C_A, C_B, C_C\}, \{C_A, C_B, C_D\}, \{C_A, C_C, C_D\}, \{C_B, C_C, C_D\},$ $\{C_A, C_{BC}\}, \{C_A, C_{BD}\}, \{C_A, C_{CD}\}, \{C_B, C_{AC}\}, \{C_B, C_{AD}\}, \{C_B, C_{CD}\},$ $\{C_C, C_{AB}\}, \{C_C, C_{AD}\}, \{C_C, C_{BD}\}, \{C_D, C_{AB}\}, \{C_D, C_{AC}\}, \{C_D, C_{BC}\},$ $\{C_{AB}, C_{CD}\}, \{C_{AC}, C_{BD}\}, \{C_{AD}, C_{BC}\},$ $\{C_{ABC}\}, \{C_{ABD}\}, \{C_{ACD}\}, \{C_{BCD}\}, \{C_{ABCD}\}$
3oo4	$\{C_A, C_B\}, \{C_A, C_C\}, \{C_A, C_D\}, \{C_B, C_C\}, \{C_B, C_D\}, \{C_C, C_D\},$ $\{C_{AB}\}, \{C_{AC}\}, \{C_{AD}\}, \{C_{BC}\}, \{C_{BD}\}, \{C_{CD}\},$ $\{C_{ABC}\}, \{C_{ABD}\}, \{C_{ACD}\}, \{C_{BCD}\}, \{C_{ABCD}\}$
4oo4	$\{C_A\}, \{C_B\}, \{C_C\}, \{C_D\},$ $\{C_{AB}\}, \{C_{AC}\}, \{C_{AD}\}, \{C_{BC}\}, \{C_{BD}\}, \{C_{CD}\},$ $\{C_{ABC}\}, \{C_{ABD}\}, \{C_{ACD}\}, \{C_{BCD}\}, \{C_{ABCD}\}$

Table 8.3. Failure probabilities of voting systems

Case	Failure probabilities	First-order approx.
1oo2	$Q_1^2 + Q_2$	Q_2
2oo2	$2Q_1 + Q_2$	$2Q_1 + Q_2$
1oo3	$Q_1^3 + 3Q_1Q_2 + Q_3$	Q_3
2oo3	$3Q_1^2 + 3Q_2 + Q_3$	$3Q_2 + Q_3$
3oo3	$3Q_1 + 3Q_2 + Q_3$	$3Q_1 + 3Q_2 + Q_3$
1oo4	$Q_1^4 + 3Q_2^2 + 4Q_1Q_3 + 6Q_1^2Q_2 + Q_4$	Q_4
2oo4	$4Q_1^3 + 12Q_1Q_2 + 3Q_2^2 + 4Q_3 + Q_4$	$4Q_3 + Q_4$
3oo4	$6Q_1^2 + 6Q_2 + 4Q_3 + Q_4$	$6Q_2 + 4Q_3 + Q_4$
4oo4	$4Q_1 + 6Q_2 + 4Q_3 + Q_4$	$4Q_1 + 6Q_2 + 4Q_3 + Q_4$

Parameter Expression of First-order Failure Probabilities

Consider the first-order probabilities in Table 8.3. The CCBE probabilities can be rewritten by the parametric expressions in Table 8.1. A result is shown in Table 8.4. The staggered testing column is described shortly.

8.2.3 Distribution of Alpha-factor Parameters

Assume the following set of data to estimate $\alpha_k^{(m)}, k = 1, \ldots, m$:

Table 8.4. Alpha-factor expression of voting-system failure-probabilities (first order)

Case	Nonstaggered testing
1oo2	$\frac{2\alpha_2}{\alpha_\mathrm{T}}Q_\mathrm{T}$
2oo2	$\frac{2(\alpha_1+\alpha_2)}{\alpha_\mathrm{T}}Q_\mathrm{T}$
1oo3	$\frac{3\alpha_3}{\alpha_\mathrm{T}}Q_\mathrm{T}$
2oo3	$\frac{3(\alpha_2+\alpha_3)}{\alpha_\mathrm{T}}Q_\mathrm{T}$
3oo3	$\frac{3(\alpha_1+\alpha_2+\alpha_3)}{\alpha_\mathrm{T}}Q_\mathrm{T}$
1oo4	$\frac{4\alpha_4}{\alpha_\mathrm{T}}Q_\mathrm{T}$
2oo4	$\frac{4(\alpha_3+\alpha_4)}{\alpha_\mathrm{T}}Q_\mathrm{T}$
3oo4	$\frac{4(\alpha_2+\alpha_3+\alpha_4)}{\alpha_\mathrm{T}}Q_\mathrm{T}$
4oo4	$\frac{4(\alpha_1+\alpha_2+\alpha_3+\alpha_4)}{\alpha_\mathrm{T}}Q_\mathrm{T}$

$$E = \{n_1, \ldots, n_k, \ldots, n_m\} \tag{8.36}$$

Here, n_k is the number of events involving exactly k component failures in CCCGs of fixed size m. The superscript (m) is omitted.

Restrict probabilistic sampling situations to the case where some CCBE occurs. Then, the probability of involving exactly k component failures is α_k with the constraint of:

$$\sum_{k=1}^{m} \alpha_k = 1 \tag{8.37}$$

The likelihood of observing evidence E, given a set of α_k is a well-known multinomial distribution:

$$L(n_1, \ldots, n_m | \alpha_1, \ldots, \alpha_m) \propto \prod_{k=1}^{m} \alpha_k^{n_k} \tag{8.38}$$

Assume the *a priori* density of α_k as a Dirichlet distribution:

$$\mathrm{p}(\alpha_1, \ldots, \alpha_m) \propto \prod_{k=1}^{m} \alpha_k^{A_{0k}}, \quad A_{0,k} \geq 0 \tag{8.39}$$

The Bayes theorem yields the following *a posteriori* density of α_k:

$$\mathrm{p}(\alpha_1, \ldots, \alpha_m | n_1, \ldots, n_m) \propto \prod_{k=1}^{m} \alpha_k^{A_k}, \quad A_k = A_{0k} + n_k \tag{8.40}$$

The maximum likelihood estimator of α_k is obtained by maximizing the *a posteriori* density with the constraint of Equation 8.37 through a Lagrange multiplier method:

$$\hat{\alpha}_k = \frac{A_k}{A_\mathrm{T}}, \quad A_\mathrm{T} \equiv \sum_{k=1}^{m} A_k = \sum_{k=1}^{m} (A_{0k} + n_k) \tag{8.41}$$

For a uniform prior, we have $A_{0,k} = 0, k = 1, \ldots, m$. The estimator becomes:

$$\hat{\alpha}_k = \frac{n_k}{\sum_{k=1}^{m} n_k} \tag{8.42}$$

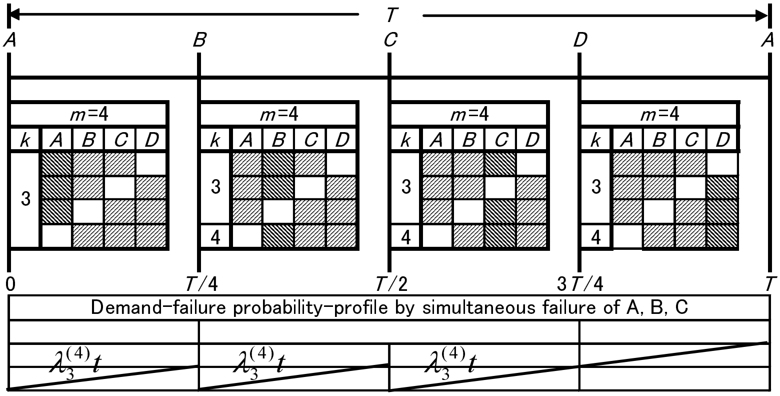


Fig. 8.3. Set of 3 component CCBE checked by a staggered test time

8.2.4 Alpha Factor with Staggered Testing

In the nonstaggered test, all the components in a CCCG are tested, and any occurrence of CCBE is corrected. The periodic test interval is T. Assume that the CCBE occurs with a constant failure rate. The CCBE probability $Q_k^{(m)}$ takes the maximum value immediately before the next test.

Consider, on the other hand, a staggered test where each component is tested in sequence uniformly with test interval T. Figure 8.3 shows a situation with $k = 3$ and $m = 4$. Consider a 3-component CCBE C_{ABC} including component A. This event or cause is tested when component A is tested because:

1) If component A is normal, then the nonoccurrence of event C_{ABC} is confirmed. Since the event occurs with constant failure rate $\lambda_3^{(4)}$, the CCBE is as good as new after the component A test.

2) If component A is failed, then all the CCBE including A is checked. If event C_{ABC} is occurring, then the three components are renewed, and hence the CCBE becomes as good as new.

For the event C_{ABC}, the situation is the same as above, when component B is tested. Component C test also yields the same result. The only exception is a component D test where event C_{ABC} is not affected when component D is normal.

When component D is failed, C_{ABC} is affected through a check of B or C, but the probability of component D failure is small and this case is neglected when compared to the normal case of component D.

Unavailability profiles of C_{ABC} is depicted in Figure 8.3. The average availability for the staggered test is:

$$Q_3^{(4)\mathrm{S}} = \frac{3\lambda_3^{(4)}T}{16} \tag{8.43}$$

while the availability for the nonstaggered test is:

$$Q_3^{(4)} = \frac{\lambda_3^{(4)}T}{2} \tag{8.44}$$

These availabilities lead to a different result from reference [35]:

$$Q_k^{(m)\mathrm{S}} \neq \frac{1}{k} Q_k^{(m)} \tag{8.45}$$

Notice that the system being analyzed generally differs from the system from which failure data were collected. For instance, a three-train system may have to be analyzed using data from four-train systems. The CCBE C_{AD} in the four-train system is regarded as CCBE C_A in the three-train system without component D. Readers can refer to NUREG/CR-5485 [34] for details of such a downward (or upward) mapping.

8.2.5 Beta-factor Model

The beta-factor model assumes that all components within the CCCG fail whenever a multiple failure CCBE occurs [65]. Thus, only probabilities $Q_1^{(m)}$ and $Q_m^{(m)}$ are nonzero, and others are zero. It was the first model that was applied to common-cause quantifications. The total component-failure-probability of Equation 8.19 reduces to:

$$Q_{\mathrm{T}} = Q_1^{(m)} + Q_m^{(m)} \tag{8.46}$$

The beta-factor parameter $\beta^{(m)}$ is defined as:

$$\beta^{(m)} \equiv \frac{Q_m^{(m)}}{Q_{\mathrm{T}}} = \frac{Q_m^{(m)}}{Q_1^{(m)} + Q_m^{(m)}} \tag{8.47}$$

In other words:

$$\beta^{(m)} \equiv \text{probability that when a } \textit{component} \text{ failure occurs in a CCCG of size } m\text{, it involves failure of } m \text{ components.} \tag{8.48}$$

Equations 8.46 and 8.47 yield expressions of CCBE probabilities $Q_1^{(m)}$ and $Q_m^{(m)}$ in terms of component-failure probability Q_{T} and beta-factor parameters:

$$Q_1^{(m)} = (1 - \beta^{(m)})Q_{\mathrm{T}} \tag{8.49}$$

$$Q_m^{(m)} = \beta^{(m)} Q_{\mathrm{T}} \tag{8.50}$$

A comparison of Equations 8.50 and 8.25 with $k = m$ yields a conversion from the alpha- to beta-factor model:

$$\beta^{(m)} = \frac{m\alpha_m^{(m)}}{\alpha_1^{(m)} + m\alpha_m^{(m)}} \tag{8.51}$$

The beta- to alpha-factor conversion is:

$$\alpha_m^{(m)} = \frac{\beta^{(m)}}{m + (1-m)\beta^{(m)}}, \quad \alpha_1^{(m)} = 1 - \alpha_m^{(m)} \tag{8.52}$$

Other αs are all zero.

For instance:

$$\beta^{(2)} = \frac{2\alpha_2^{(2)}}{\alpha_1^{(2)} + 2\alpha_2^{(2)}} \tag{8.53}$$

$$\beta^{(3)} = \frac{3\alpha_3^{(3)}}{\alpha_1^{(3)} + 3\alpha_3^{(3)}} \tag{8.54}$$

$$\beta^{(4)} = \frac{4\alpha_4^{(4)}}{\alpha_1^{(4)} + 4\alpha_4^{(4)}} \tag{8.55}$$

Alternatively,

$$\alpha_2^{(2)} = \frac{\beta^{(2)}}{2 - \beta^{(2)}}, \quad \alpha_1^{(2)} = 1 - \alpha_2^{(2)} \tag{8.56}$$

$$\alpha_3^{(3)} = \frac{\beta^{(3)}}{3 - 2\beta^{(3)}}, \ \alpha_1^{(3)} = 1 - \alpha_3^{(3)}, \ \alpha_2^{(3)} = 0 \tag{8.57}$$

$$\alpha_4^{(4)} = \frac{\beta^{(4)}}{4 - 3\beta^{(4)}}, \ \alpha_1^{(4)} = 1 - \alpha_4^{(4)}, \ \alpha_2^{(4)} = \alpha_3^{(4)} = 0 \tag{8.58}$$

Equation 8.5 reduces to the following equation by removing partial simultaneous failures $Q_{P,2}$:

$$\Pr\{\text{Top}\} \simeq Q_{P,3} + Q_{M,2}Q_{T,1} + Q_{M,2}Q_{P,1} + (Q_{P,1} + Q_{T,1})(Q_{P,1} + Q_{M,1})^2 \tag{8.59}$$

The top-event probability of the 1oo3 system of Equation 8.35 reduces to:

$$Q_{1/3} = Q_1^3 + Q_3 = (1 - \beta^{(3)})^3 Q_{\mathrm{T}}^3 + \beta^{(3)} Q_{\mathrm{T}} \tag{8.60}$$

A single-component system has the unavailability of Q_{T}. Thus, the unavailability of the 1/3 system is reduced only by $\beta^{(3)}$ when the independent portion is neglected. The unavailability without the common causes is $Q_{1/m} = Q_{\mathrm{T}}^3$, which is often an underestimated value.

As a special case of the alpha-factor model, let n_m be the number of times that all the m components were failed on demand, and n_1 be the number that only a single component was failed on demand. Alpha-parameter estimates $\hat{\alpha}_1 = n_1/(n_1 + n_m)$ and $\hat{\alpha}_m = n_m/(n_1 + n_m)$ and the conversion equation of Equation 8.51 yield the $\beta^{(m)}$ estimate:

$$\hat{\beta}^{(m)} = \frac{n_m}{n_m + (n_1/m)} = \frac{mn_m}{n_1 + mn_m} \tag{8.61}$$

This estimator does not include the total number n of demands.

Component-failure probability on demand can be estimated by:

$$\hat{Q}_{\mathrm{T}} = \hat{Q}_1 + \hat{Q}_m = \frac{n_1}{nm} + \frac{n_m}{n} = \frac{n_m + (n_1/m)}{n} \tag{8.62}$$

The number n is frequently unavailable. Component-failure probabilities from databases are used instead of Equation 8.62.

Other methods of determining $\beta^{(m)}$ include a scoring approach [66].

8.3 Markov Analysis of Graceful Degradation

A graceful degradation gives us time to cope with system degradations. This section presents a quantification method based on Markov transition diagram.

8.3.1 Steer-by-wire System Reliability

A steer-by-wire (SBW), in its literal sense, has no mechanical connection composing conventional power-steering systems. A complete loss of steering may occur when important components such as the electronic control unit (ECU) fail. A prudent automated operation procedure is required to cope with partial system degradations, together with a fault-tolerant hardware design for prevention and mitigation of the partial as well as complete system failures.

This section quantifies the SBW with the mechanical backup [67]. An operation procedure is presented and converted into a Markov transition diagram where each state represents either a normal SBW, or a partially degraded, or a completely failed SBW. The system reliability is quantified in terms of the state probabilities calculated by a numerical integration of the Markov diagram specified by component failure rates.

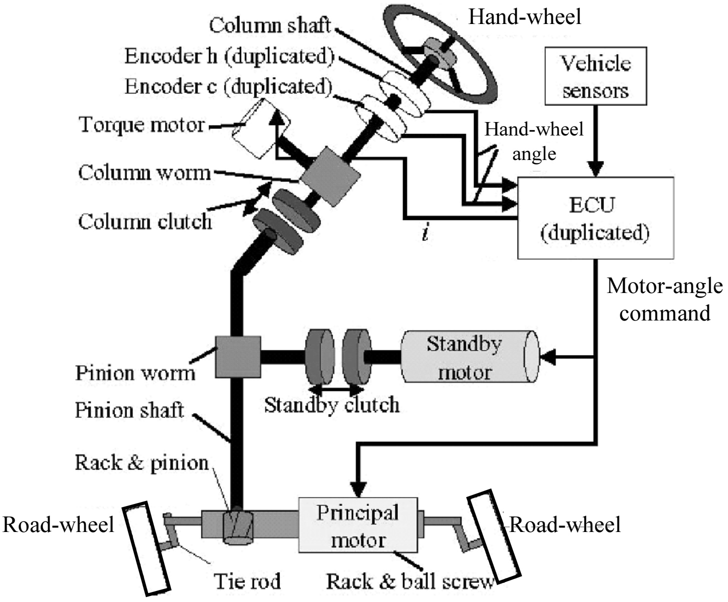


Fig. 8.4. Fault-tolerant steer-by-wire system with a mechanical backup

8.3.2 Fault-tolerant Design

A principal motor functions as a steering actuator, as shown in Figure 8.4. A standby motor is a backup actuator. The reaction torque is acted on the hand-wheel by a torque motor. The three motors are commanded by duplicated ECUs. When both principal and standby motors fail, the road-wheel and hand-wheel are mechanically connected via a column clutch, thus reducing to a conventional "manual" steering. The torque motor, in turn, is used to generate an assist torque for the manual steering to function as a power steering.

The hand-wheel torque is detected by a pair of upside and downside encoders to measure a twist angle in between, and the hand-wheel angle is measured by either one of the encoders in the pair. The upside encoder itself is duplicated as well as the downside one to facilitate failure detection.

The angle command to the principal or standby motor is determined from encoders measuring the hand-wheel torque and angle, and from vehicle sensors measuring vehicle speed, lateral acceleration, and yaw rate.

In the simplest case the angle command is made proportional to the hand-wheel angle measured by either one of the encoders.

8.3.3 Operation Procedure during Partial Failures

The operation procedure can be represented by a state-transition diagram shown in Figure 8.5. A transition from one state to another is shown by a

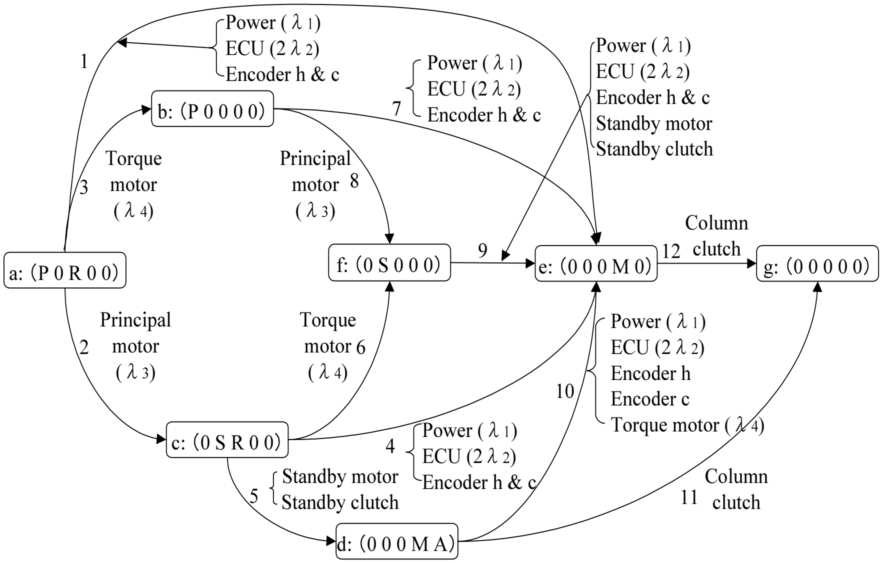


Fig. 8.5. Degradation diagram for steer-by-wire system

numbered arrow. Each of the 7 states a to g consists of five elements enclosed by parentheses.

1) The 1st element is a principal SBW (PSBW) index. Symbol P (principal) denotes a normal PSBW where the road-wheels are actuated by the principal motor, while 0 denotes a failed PSBW.
2) The 2nd is a standby SBW (SSBW) index. Symbol S (standby) denotes a normal SSBW with the road-wheels actuated by the standby motor, while 0 denotes a failed SSBW.
3) The 3rd is a reaction-torque index. Symbol R (reaction) represents the existence of the reaction torque, while 0 represents the nonexistence.
4) The 4th is a manual-steering index. Symbol M (manual) denotes that the manual steering is functioning through the mechanical coupling, while 0 denotes manual-steering failure.
5) The 5th is an assist-torque index. Symbol A (assist) denotes availability of the assist torque, while 0 denotes unavailability.

Some combinations of the five elements are infeasible. The total number of feasible states turns out to be 7. There are 12 feasible transitions.

State a thus denotes principal SBW with reaction torque, b principal SBW without reaction torque, c standby SBW with reaction torque, f standby SBW without reaction torque, d manual steering with assist torque, e manual steering without assist torque, and g denotes a complete loss of steering.

The state transitions are denoted by arrows labeled by component failures: “power” denotes power failure, “ECU” failure of either one of the two

ECUs, “encoder h” failure of either one of the two upside encoders, “encoder c” failure of either one of the two downside encoders, “encoder h&c” both failures of upside and downside encoders, “torque motor” torque-motor failure, “principal motor” principal-motor failure, “standby motor or standby clutch” failure of either standby motor or standby clutch, and “column clutch” denotes column-clutch failure.

The duplicated ECU detects its failure by output comparison; the ECU failure is thus defined as a failure of either one of the two ECUs; the same is true for the duplicated upside encoders or the downside encoders.

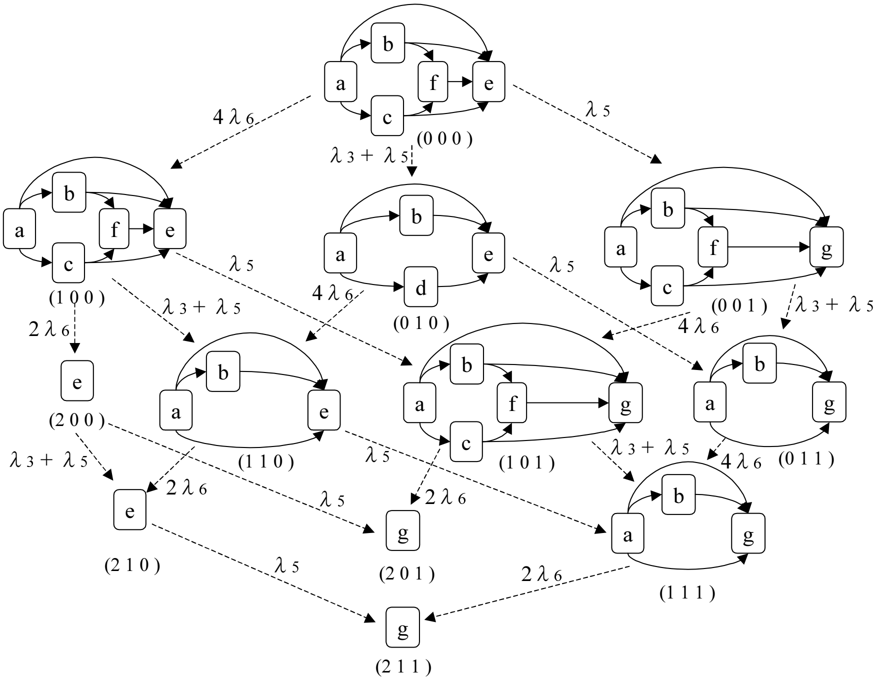


Fig. 8.6. Markov transition diagram for steer-by-wire system

8.3.4 Markov Transition Diagram

Unfortunately, the diagram of Figure 8.5 lacks the Markov property. In other words, some nodes in the diagram can not be regarded as states. This is explained below.

A transition to d (manual with assist torque) from state c (standby SBW with reaction torque) occurs by the sum of failure rates of standby motor and standby clutch, given that these two components were normal when state c was visited. However, this transition occurs instantly when the standby motor was already failed before the visit to state c. The transition rate from state c to d changes according to standby-motor and clutch failures at the visit to parent state c, which indicates that the Markov property of the transition diagram is lost.

Similarly, column clutch and encoder h&c are shown to be factors influencing transition rates.

The original diagram is reconfigured into a layer structure to yield a Markov state-transition diagram. The 7 states in Figure 8.5 are called main states, while the states in Equation 8.63 are substates:

$$\begin{gathered}\text{(encoder h\&c, standby motor \& standby clutch,}\\ \text{column clutch)}\end{gathered} \tag{8.63}$$

Encoder h&c has three component states: full inservice (upside and downside) denoted by 0, half inservice (upside or downside but not both) by 1, and both out-of-service by 2.

The standby motor & standby clutch has two states: both inservice denoted by 0, and one or two out-of-service denoted by 1.

The column clutch has two states: 0 means inservice, 1 means in-failure. The component states of Equation 8.63 are enumerated below:

$$\left(\begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right) \tag{8.64}$$

For example, $(2, 1, 0)$ means that both the upside and downside encoders are failed, the standby motor and/or the standby clutch is failed, and that the column clutch is normal. It is clear that the number of substates is $3 \times 2 \times 2 = 12$. The number of main states is 7. Thus, the maximum number of augmented states is $12 \times 7 = 84$.

A number of combinations turn out to be infeasible because some substates cause state transitions in the original diagram of Figure 8.5; these transitions immediately occur when the substates are realized by relevant component failures. For example, augmented state $a(2, 1, 0)$ is infeasible, and is replaced by state $e(2, 1, 0)$.

Consider transitions between the substates denoted by dotted arrows in Figure 8.6. Three paths from $a(0, 0, 0)$ to $e(2, 1, 0)$ are observed along the dotted arrows. These transitions yield a layer structure classified by the sum of three elements of each substate. The maximum number of the sum is $4 = 2+1+1$, and the 12 substates can be arranged by 5 layers. Figure 8.6 becomes the augmented state-transition diagram with the Markov property where each main state is conditioned by a relevant substate shown below in parentheses.

1) Main state transitions initiated by a substate transition can be identified easily. For example, augmented state $c(0, 0, 0)$ on the first layer transits to $d(0, 1, 0)$ on the second layer when the substate moves from $(0, 0, 0)$ to $(0, 1, 0)$.

2) The transitions among main states without a substate transition can be identified easily from Figure 8.5.
3) An augmented state implying a complete loss of steering denoted by g is treated as an absorption state from the viewpoint of main states as well as substates. No further transition occurs once this absorption state is reached. For example, the transition from $g(0,0,1)$ to $g(0,1,1)$ need not be considered.
4) The total number of feasible, augmented states is 37, less than the 84.

8.3.5 Markov Differential Equation

A Markov differential equation is used for a quantitative reliability analysis. Denote by $P_i(t)$ the probability that the SBW system is in state i at time t. Parameter γ_{ji} is a transition rate from state j to i, and γ_{ij} from i to j. The total number of states is denoted by n:

$$\dot{P}_i(t) = \sum_{j=1,\ j\neq i}^{n} \gamma_{ji} P_j(t) - P_i(t) \sum_{j=1,\ j\neq i}^{n} \gamma_{ij} \tag{8.65}$$

The probability of each state at time t can be calculated from Equation 8.65. The transition rates are determined from component failure rates.

8.3.6 Reliability Quantification

Consider a continuous operation up to 8 h for a nonrepairable SBW system. The state probabilities are shown in Figure 8.7. Assume that the SBW system is renewed at the start of each driving. This means that the driving can not be initiated until system degradations during the last driving have been repaired. Two time spans are considered for the continuous driving: 2 h and 8 h.

The probability of "state c: standby SBW with reaction torque" is about one failure per 10^8 vehicles after 2 h of continuous driving. A similar probability to c is obtained for "state e: manual steering without assist torque". Even if the continuous driving increases to 8 h, the probability of these system degradation states remains at once per 10^7 vehicles.

On the other hand, the probability of "state g: complete loss of steering" is once per 10^{16} for 2 h of continuous driving. For 8 h driving, it still remains at a small value, *i.e.* once per 10^{15} vehicles. The actual probability of complete loss of steering is further decreased because the SBW system can be repaired when system-degradation states are detected. Note that the assist torque is less available for the manual steering; this is observed from the probabilities of state e and state d. The designer's intention to provide a power-steering feature at the manual state is not achieved.

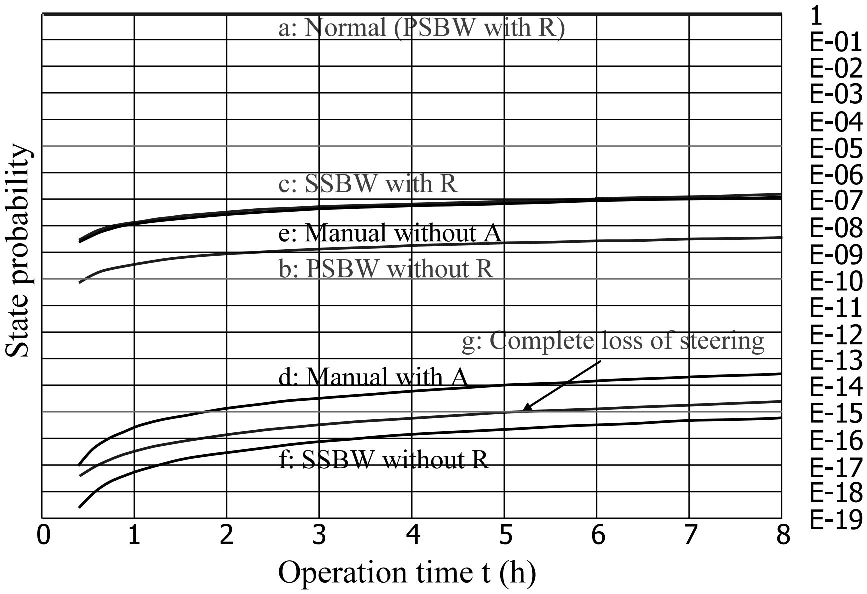


Fig. 8.7. Time-dependent state probability for a mechanical backup SBW

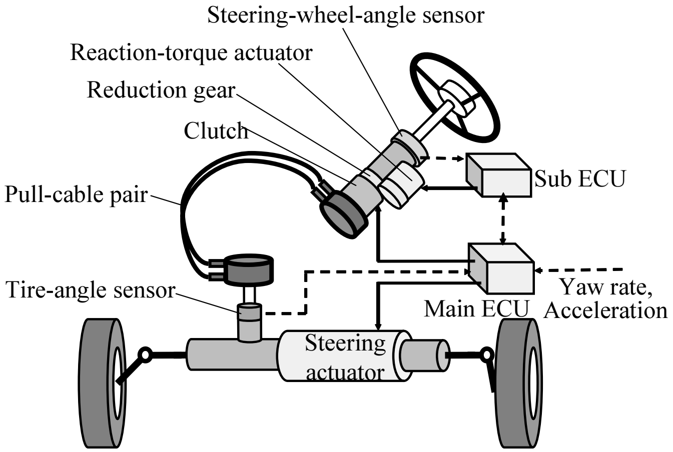


Fig. 8.8. Steer-by-cable without column shaft as a final backup of the steer-by-wire system

8.3.7 Design Alternative for Collision Safety

Figure 8.4 has a column shaft to implement the mechanical clutch. This shaft is hazardous at a collision. A complete SBW without the mechanical clutch violates the principle of defense-in-depth. The column shaft can be replaced by a cable-based clutch mechanism to improve collision safety, as shown in Figure 8.8 [68].

8.4 Concluding Remarks

Common causes are routinely quantified in the nuclear field because of the maturity of the PRA. The graceful degradation analysis of the automobile device can be extended to consider common causes. Without these dependent failure analyses, the PRA departures from realism would be significant.

9

Human-error Quantification

9.1 Introduction

To quote Alexander Pope (1688–1744), “to err is human”. Human errors in thinking and rote tasks occur, and these errors can destroy aircraft, chemical plants, and nuclear power plants. Our behavior is both beneficial and detrimental to modern engineering systems. The reliability and safety analyst must consider the human element; otherwise, the analysis is not creditable [53]. This chapter briefly discuss the human-error quantification. Refer to references [56],[69]–[73] for more detail. There is a software version called HRA Calculator [74]. The ASME PRA Standard recommends the use of THERP [56] and ASEP [69].

The term “unsafe act” is sometimes preferred to “error” because the latter sometimes suggests responsibility on the human who erred. We use the term “error” with an agreement that the term does not necessarily imply responsibility.

As compared with hardware or machine [53, 75], human beings are characterized by:

1) We are less reliable, less precise, less consistent, and slower, but more flexible than hardware.
2) We are weak in computation, negation logic, normative treatment, and concurrent processing but strong in pattern recognition and heuristics.
3) We are flexible in manipulation, data sensing, and data processing where the same purpose can be accomplished by different approaches.
4) We are unpredictable; we can commit all types of misdiagnoses and wrong actions.
5) We frequently lie to absolve ourselves from blame.
6) We are far superior in self-correction capability to machines.
7) We are purposeful; we form a solution and act accordingly, searching for relevant information and performing necessary actions along the way. This

goal-oriented behavior is good as long as the goal is correct; otherwise, the wrong solution becomes a dominant source of common-cause failures.

8) We can anticipate.
9) We have strong intuitive survival instincts.

We don't like to think. Let us briefly list how this brain bottleneck manifests itself.

1) Shortcut: We tend to simplify things to minimize work loads. This tendency is dangerous when protection devices are nullified and safety-related procedures are neglected.
2) Perseverance: There is a tendency to believe that an explanation first fitting the current situation is the only one that is correct.
3) Task fixation: We become preoccupied with one particular task to the exclusion of other tasks that are more important.
4) Alternation: This occurs when we constantly change a decision while basic information is not changing.
5) Dependence: Excessive dependence on other personnel, written procedures, automatic controllers, and indicators is sometimes harmful.
6) Naivety: Once trained, we tend to perform tasks by rote. Simple stimulus–response manipulations that yield unsafe results occur.
7) Queuing and escape: This phenomenon typically occurs when the work load is too high.
8) Gross discrimination: Details are neglected. Qualitative rather than quantitative information is collected.
9) Cheating and lying: When the human thinks it is to its advantage, it will lie and cheat.

9.2 Classification of Human Error for PRA

Event trees and fault trees should include human-error events before and after initiating events. The ASME PRA Standard uses the same classification [5].

9.2.1 Preinitiator Error

These occur under controlled conditions (*e.g.*, no accident, little or no time pressure).

Test and Maintenance Errors
A typical example is failure to return safety equipment to its working state after a test, thus causing a latent failure of the safety system when an initiator occurs.

Initiating-event Causation
An initiating event may be caused by human error. A railroad example is a train departure neglecting a red signal (Section 5.2.2).

9.2.2 Postinitiator Error

This is a postinitiator error containing accident-procedure errors and recovery errors. Wakefield [76] gives typical human-response activities during accidents.

1) Manual backup to automatic plant response. Emergency diesel generators automatically start when an electrical power failure occurs. The generators are manually started when the automatic activation failed.
2) Change of normal plant-safety response. Cooling system is terminated when an excessive cooling causes a blockage by solidification of metal fluid.
3) Recovery and repair of failed system. Repair of component or other manual actions, such as manually forcing stuck valves to open [9]. Recovery of cooling before vessel failure is also an example.
4) Total shift to manual operation.

The following errors are typical.

1) Procedural error: Deviations from 1) emergency operating procedure (EOP) such as isolating a leak, given a water level drop, or 2) abnormal operating procedure (AOP) such as manually starting backup turbine generator [77].
2) Recovery error: An example is an AC recovery failure in station blackout accident sequences. Quantification of recovery actions typically depends on the time available to diagnose the situation and perform the action, as well as the adequacy of the training, procedures, and operator knowledge. Estimating the success probability for the recovery actions involves a certain degree of subjectivity.

   Recovery probabilities are realistically quantified. The apparently low risk significance of certain items may be dependent on credit for restoration of component function [9]. Crew interactions affect recovery from human errors.

   PRAs typically model recovery actions especially for dominant accident sequences. Sensitivity analyses can assume cases when recovery actions are removed. Some SSCs support procedural or recovery actions. Time to recover a component is a typical parameter of success criteria.

9.3 Slip, Lapse, Mistake, and No Detection

An extension of the original operator action tree (OAT) [78] is shown in Figure 9.1 as a typical operator model. Consider, for example, that a safety system fails to start, requiring a manual start. The OAT extension consists of six phases.

1) A – Occurrence: An event such as an automatic safety system failing to start occurs.

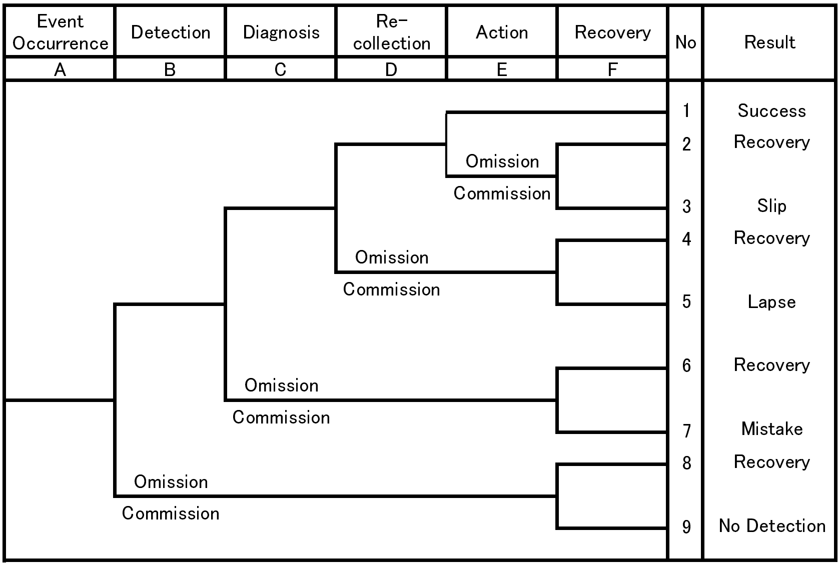


Fig. 9.1. Operator action tree. Extended version

2) B – Detection: This is a trigger to make the operator more aware about the situation. After the detection, the operator tries to identify causes and necessary actions. Similar to human the disease case, some failure modes are difficult to detect. The target of detection includes not only event occurrences but also reliability degradation before failures.
3) C – Diagnosis: Engineers identify causes, assess the situation, predict plant response, and determine actions. A medical prescription instructs an action.
4) D – Recollection: The operator must first recollect the necessary action before execution.
5) E – Action: Execution of actions determined in the diagnostic phase. Valves are opened or operators are instructed.
6) F – Recovery: Previous errors and failures are corrected.

Everything is OK in sequence 1 of Figure 9.1. Errors in action, recollection, diagnosis, or detection phases are recovered in sequences 2, 4, 6, and 8, respectively. Other sequences involve uncorrected human errors.

1) Slip: This occurs in sequence 3. The necessary action is recollected correctly, but the action is not performed in time (omission), or is performed incorrectly (commission). For instance, the operator may close a valve instead of opening it.
2) Lapse: The necessary action is determined by the diagnosis correctly, but the action is not recalled at all (omission), or recalled incorrectly (com-

mission). The operator may forget to manipulate a valve (omission), or may close a wrong valve because of a failure of recollection (commission). Forgetting a name is an omission type of lapse, while recalling an incorrect name is a commission type.

3) Mistake: This is sequence 7. If a doctor misdiagnoses a patient, no drug is prescribed (omission), or a hazardous drug is prescribed (commission). When the diagnosis does not finish in time, this can be regarded as omission if nothing is done.
4) No detection: This is sequence 9. Nothing is done because of a lack of detection (omission), or irrelevant things are performed because of a false detection (commission).

The term “no response” typically refers to an omission type of “no detection”. However, “no response” in a broader sense means omissions in slip, lapse, mistake, and detection.

9.4 Stress and Performance-shaping Factors

NUREG-1764 considers, for instance, the following four changes to human actions [79]:

1) Changes in teamwork: Has the requested change significantly changed the team aspects of performing an action. For example, is one operator now performing the tasks accomplished by two or more operators in the past?
2) Changes in skill level: Has the requested change made it necessary for an individual who is less trained and has lower qualifications to take the action than was the case before the modification?
3) Change in communication demands: Has the requested change significantly increased the level of communication needed to perform the task? For example, must an operator now communicate with other personnel to perform actions that previously could be taken at a local panel?
4) Change in environmental conditions: Has the requested change significantly increased the environmental challenges (such as radiation, or noise) that could negatively affect task performance?

These typical factors such as teamwork, skill level, communication demands, and environmental conditions influence human performance, and are called performance-shaping factors [56]. NUREG-1764 defines performance-shaping factors (PSFs) as factors that influence human reliability through their effects on performance. PSFs include factors such as environmental conditions, HSI (human–system interface) design, procedures, training, and supervision.

Tables 9.1 and 9.2 list performance-shaping factors in the handbook [56]. The “changes in teamwork” and “change in communication demand” correspond to “3.15 team structure and communication” in the “3 Task and equipment characteristics” of external PSFs. The “change in environmental

Table 9.1. Performance-shaping factors – External PSFs

External PSFs	
1	Situational characteristics: Those PSFs general to one or more jobs in a work situation.
1.1	Architectural features
1.2	Quality of environment (temperature, humidity, air, quality, radiation, lighting, noise, vibration, degree of general cleanliness
1.3	Work hours/work breaks
1.4	Shift rotation
1.5	Availability/adequacy of special equipment, tools, and supplies
1.6	Staffing parameters
1.7	Organizational structure (*e.g.* authority, responsibility, communication channels)
1.8	Actions by supervisors, coworkers, union representatives, and regulatory personnel
1.9	Rewards, recognition, benefits
2	Job and task instructions: Single most important tool for most tasks
2.1	Procedures required (written/not written)
2.2	Written or oral communications
2.3	Cautions and warning
2.4	Work methods
2.5	Plant policies (shop practices)
3	Task and equipment characteristics: Those PSFs specific to tasks in a job
3.1	Perceptual requirements
3.2	Motor requirements (speed, strength, precision)
3.3	Control–display relationship
3.4	Anticipatory requirements
3.5	Interpretation requirements
3.6	Decision-making requirements
3.7	Complexity (information load)
3.8	Narrowness of task
3.9	Frequency and repetitiveness
3.10	Task criticality
3.11	Long- and short-term memory
3.12	Calculational requirements
3.14	Dynamic vs. step-by-step activities
3.15	Team structure and communication
3.16	Human–machine interface (design of prime equipment, test equipment, manufacturing equipment, job aids, tools, fixtures)

Table 9.2. Performance-shaping factors – Stressor and internal PSFs

	Stressor PSFs
4	Psychological stressors: PSFs that directly affect mental stress
4.1	Suddenness of onset
4.2	Duration of stress
4.3	Task speed
4.4	Task load
4.5	High jeopardy risk
4.6	Threats (of failure, loss of job)
4.7	Monotonous/degrading/meaningless work
4.8	Long, uneventful vigilance periods
4.9	Conflicts of motives about job performance
4.10	Reinforcement absent or negative
4.11	Sensory deprivation
4.12	Distractions (noise, glare, movement, flicker, color)
4.13	Inconsistent cueing
5	Physical stressors: PSFs that directly affect physical stress
5.1	Duration of stress
5.2	Fatigue
5.3	Pain or discomfort
5.4	Hunger or thirst
5.5	Temperature extremes
5.6	Radiation
5.7	G-force extremes
5.8	Atmospheric pressure extremes
5.9	Oxygen insufficiency
5.10	Vibration
5.11	Movement constriction
5.12	Lack of physical exercise
5.13	Disruption of circadian rhythm
	Internal PSFs
6	Organismic factors
6.1	Previous training experience
6.2	State of current practice or skill
6.3	Personality and intelligence variables
6.4	Motivation and attitudes
6.5	Emotional state
6.6	Stress (mental or bodily tension)
6.7	Knowledge of required performance standards
6.8	Sex differences
6.9	Physical condition
6.10	Attitudes based on influence of family or other outside persons or agencies
6.11	Group identifications

conditions” to “1.2 Quality of environment” in the “1 Situational characteristics”, while the “changes in the skill level” to “6.2 State of current practice” in “6 Organismic factors” of “Internal PSFs”.

Some PSFs can be viewed as how well the human is supported by a proposed change to human actions (HAs) [79].

1) Change in HSIs (human–system interfaces): Has the requested change significantly changed the HSIs used by personnel to perform the task? For example, are personnel now performing their tasks at a computer terminal where previously they were performed at a control board with analog displays and controls? This is related to the “3.16 Human–machine interface” in “3 Task and equipment characteristics”.
2) Change in procedures: Has the requested change significantly changed the procedures that personnel use to perform the task, or is the task not supported by procedures? This is related to “2.1 Procedures required (written/not written)“ in “2 Job and task instructions”.
3) Change in training: Has the requested change significantly modified the training, or is the task not addressed in training? This is related to “6.1 Previous training experience” in “6 Organismic factors”.

NUREG-1764 gives two other examples where the PSFs are varied significantly.

1) Change in Automation: Has the requested change given personnel a new functional responsibility that they previously did not have and that differs from their normal responsibilities? For example, are operators now required to take an action in place of a previously automated one?

   Consider the example of simply being required to open a valve that previously was automatically operated, and where the action required to do so is similar to other valve-opening operations with which the operators are familiar. This would not be a sufficient change (in and of itself) to warrant a “yes” to this question when considering task complexity. However, there may be increased workload if the aggregate of added actions is judged to be excessive; this may warrant a yes.”
2) Change in tasks: Has the requested change significantly modified the way in which personnel perform their tasks (*e.g.*, making them more complex, significantly reducing the time available to perform the action, increasing the operator workload, changing the operator role from primarily “verifier” to primarily “actor”)?

   In this case, operators do not have a new functional responsibility; instead, the way that they perform their current functional responsibilities has significantly changed and is different from what they usually do.

The stressor in Table 9.2 is defined as a source of a stress. Figure 9.2 indicates that both extremes are not preferable for human performance, and there is an optimal level in between.

The factors “5.1 Previous training experience”, “5.2 State of current practice or skill”, “5.3 Personality and intelligence variables”, and “5.7 Knowledge

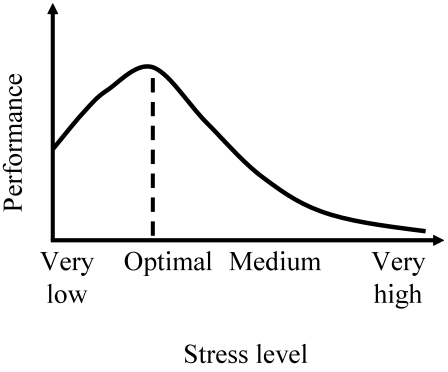


Fig. 9.2. Human performance and stress level

of required performance standards" are related to types of mental processes considered in the HCR model [80].

1) Skill-based behavior: This behavior is characterized by a very close coupling between sensory input and response action. Skill-based behavior does not depend directly on the complexity of the task, but rather on the level of training and the degree of practice in performing the task. A highly trained worker performs skill-based tasks swiftly or even mechanically with a minimum of errors.
2) Rule-based behavior: Actions are governed by a set of rules or associations that are known and followed. A major difference between rule-based and skill-based behaviors stems from the degree of practice. If the rules are not well practiced, the human being has to recall consciously or check each rule to be followed. Under these conditions the human response is less timely and more prone to errors because additional cognitive processes must be called upon. The potential for error results from problems with memory, the lack of willingness to check each step in a procedure, or failure to perform each and every step in the procedure in the proper sequence. The rule-based behavior tends to approach the skill-based behavior after a sufficient amount of practice.
3) Knowledge-based behavior: Suppose that symptoms are ambiguous or complex, the plant state is complicated by multiple failures or unusual events, or instruments give only indirect readings of the plant state. Then the engineer has to rely on personal knowledge, and behavior is determined by more complex cognitive processes. Rasmussen calls this knowledge-based behavior [81]. Human performance in this type of behavior depends on knowledge of the plant and an ability to use that knowledge. This type of behavior is more prone to error and requires more time.

The ASME Standard requires that for each human-error-probability evaluation the following plant-specific information be included as supporting requirements (HR-D3) [5]:

1) the quality of written procedures (for performing tasks) and administrative controls (for independent review);
2) the quality of the human–machine interface, including both the equipment configuration, and instrumentation and control layout.

The recovery of preinitiator errors should be assessed by using the following information (HR-D4):

1) postmaintenance or postcalibration tests required and performed by procedure;
2) independent verification, using a written check list, which verifies the component status following maintenance or testing;
3) original operator, using a written check list, makes a separate check of component status at a later time;
4) work shift or daily checks of component status, using a written check list.

The uncertainty of HEP is assessed. Mean values are used as point estimates.

The postinitiator HEPs should be estimated by the following plant-specific and scenario-specific performance-shaping factors (HR-G3).

1) quality and frequency of the operator training or experience;
2) quality of the written procedures and administrative controls;
3) availability of instrumentation needed to take corrective actions;
4) degree of clarity of the cues and/or indicators;
5) human–machine interface;
6) time available and time required to complete the response;
7) complexity of the required response;
8) environment such as lighting, heat and radiation under which the operator is working;
9) accessibility of the equipment requiring manipulation;
10) necessity, adequacy, and availability of special tools, parts, clothing, *etc.*

9.5 Calculation of Nonresponse Probability

9.5.1 Median Response Time

From the point of view of changes to human actions, the following types are considered as the changes [79].

1) New actions: An action that was not previously performed by personnel, such as when an action previously performed by automation is allocated to the operators.

2) Modified actions: A change in the way actions were previously performed, such as through introducing new task steps (*e.g.*, due to new system components, a modification to a component, or failed components), or new control and display devices for performing the action.
3) Modified task demands: Rather than affecting the task steps themselves, a change in the plant may affect the task demands, such as the amount of time available or the overall environment for the task.

This section deals with a specific type of demand. The amount of time available is focused [82]. Consider a case where a safety system is supposed to start automatically to cope with an initiating event. The system must be started manually when the automatic action fails. The nonresponse probability means the probability that the operator fails to detect the automatic-action failure. More precisely, this is the nodetection plus omission type of diagnosis error in Figure 9.1.

9.5.2 Median of Operator-detection Time

The time for the operator to detect the failure can be regarded as a random variable. Denote by $\bar{T}_{1/2}$ the median of the task time, *i.e.* the time to detection. This median varies due to the following factors.

1) Operator experience: Experienced operator detects the failure more quickly.
2) Stress level: The median takes its minimum at the optimal stress level.
3) Human–system interface: The better the interface, the shorter the median time.

The task time can be divided into detection time and diagnosis time. The median detection time to notice something is wrong is $T'_{1/2} = 10$ s. The diagnosis time to identify the failure of automatic activation is $T''_{1/2} = 15$ s.

The skill level, stress level, and interface quality are quantified by coefficients K_1, K_2, and K_3, respectively. A new median time $T_{1/2}$ reflecting the current situation is calculated by modifying the nominal median time $\bar{T}_{1/2} = 10 + 15$:

$$T_{1/2} = (1 + K_1)(1 + K_2)(1 + K_3)\bar{T}_{1/2} \tag{9.1}$$

Assume for the current example the average operator ($K_1 = 0$), a high stress level ($K_2 = 0.28$), and a good interface ($K_3 = 0$). The median time after the modification is:

$$T_{1/2} = (1 + 0)(1 + 0.28)(1 + 0) \times (10 + 15) = 32 \text{ s} \tag{9.2}$$

9.5.3 Available Time and Nonresponse Probability

Another factor affecting the nonresponse probability is the time available denoted by t. Normalize this time by the median response time:

Table 9.3. Typical PSFs influencing nonresponse probability

PSF	Coef.	Criteria
P1 Operator experience	K_1	
1 Expert	-0.22	Trained with more than five years experience
2 Average	0.00	Trained with more than six months experience
3 Novice	0.44	Trained with less than six months experience
P2 Stress level	K_2	
1 Grave emergency	0.44	High stress situation, Emergency with operator feeling threatened
2 High workload	0.28	High stress situation, Partway through accident with high workload or equivalent
3 Optimal condition	0.00	Optimal situation, Crew carrying out small load adjustments
4 Low stress (vigilance)	0.28	Problem with vigilance, Unexpected transient with no precursors
P3 Interface	K_3	
1 Excellent	-0.22	Advanced operator aids are available to help in accident situation
2 Good	0.00	Displays human engineered with information integration
3 Fair	0.44	Displays human engineered, but without information integration
4 Poor	0.78	Displays are available, but not human engineered
5 Extremely poor	0.92	Displays are not directly visible to operator

$$\hat{t} \equiv t/T_{1/2} \tag{9.3}$$

This shows how much time is available as compared with the median time.

Suppose that the operator must complete the plant shutdown within 79 s from the start of the initiating event, *i.e.* failure of automatic safety system actuation. Manipulation of a shutdown switch belongs to an execution phase. It is assumed that the manipulation time is short enough to be neglected. It is also assumed that the switch is identified easily without selection error and without reverse manipulation error. There is no lapse-type error of recollection.

A 3-parameter Weibull reliability in Figure 9.3 is used to represent the nonresponse probability $\Pr\{\hat{t}\}$ as a function of the normalized time available:

$$\Pr\{\hat{t}\} = \exp\left[-\left\{\frac{\hat{t}-B}{A}\right\}^{C}\right] \tag{9.4}$$

Here, parameters A, B, and C are correlation coefficients associated with the type of mental processing, *i.e.* skill, rule, or knowledge. Table 9.4 lists the parameters. The current example assumes a skill-based processing of the

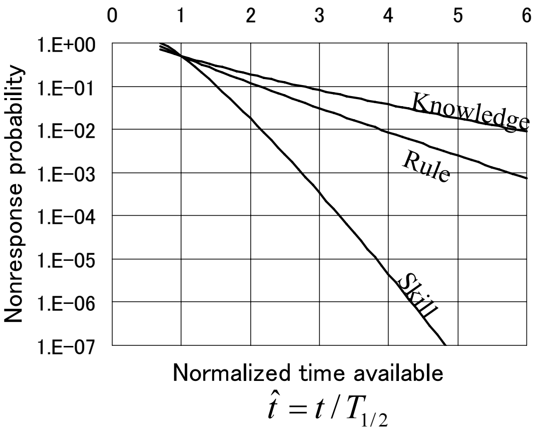


Fig. 9.3. Nonresponse probability as functions of available time

Table 9.4. Mental-processing type affecting nonresponse error

Mental processing	A	B	C
Skill	0.407	0.7	1.2
Rule	0.601	0.6	0.9
Knowledge	0.791	0.5	0.8

sufficiently experienced operator. The nonresponse probability becomes:

$$\Pr\{\hat{t}\} = \exp\left[-\left\{\frac{(79/32) - 0.7}{0.407}\right\}^{1.2}\right] = 0.0029 \tag{9.5}$$

If the stress is changed to its optimal level (K_2=0), the nonresponse probability decreases to 0.00017. If knowledge-based mental processing is required and the corresponding constants are taken from Table 9.4, the probability increases to 0.028. If lapse/slip errors during the response phase cannot be neglected in Figure 9.1, these should also be quantified by an appropriate method such as THERP, described in the next section.

9.6 THERP

The technique for human-error rate prediction (THERP) is regarded as the most powerful and systematic methodology for the quantification of human reliability. This technique, which was first developed and publicized by Swain, Rook, and coworkers at the Sandia Laboratory in 1962 for weapons-assembly tasks, was later used in the WASH-1400 study, and since then it has been improved.

THERP is most effective when a human task is divided into a sequence of unit tasks. Human errors are defined as deviations from each unit task. THERP is relatively weak in analyzing time-stressed thought processes such as diagnosis during an accident where a step-by-step analysis into unit tasks is infeasible. The PSFs remain relevant to the thought process. THERP is best suited for skill-based routine activities, and rule-based procedures-following activities.

9.6.1 Task Analysis

A task is defined as a group of activities that have a common purpose, often occurring in temporal proximity, and that utilize the same displays and controls [13]. An important element of task analysis is a decomposition of the task into unit tasks. Each unit task is not necessarily a step of a procedure. Rather, the unit task is a more microscopic one, for instance:

1) Recollection of action: An action to be performed is recalled. As shown in Figure 9.1, an omission error occurs when the operator recollects nothing.
2) Selection: A suitable display, a control, a procedure manual, or a procedural step is selected. A commission error occurs when the operator selects wrong items.
3) Interpretation: Errors in this phase include a reading error of a temperature display, or a confirmation error of a pump-operating status.
4) Execution: Errors include reversal manipulation error of a control. This is a commission error.

Suppose, for example, that the control in question is large and the only one in the neighborhood. Then, the selection phase can be neglected. When immediate feedback of results of manipulation is available, then the reversal manipulation error can be removed from the task analysis.

The task analysis clarifies the following aspects in addition to the task decomposition [13].

1) The information that is required to inform personnel that each human action (HA) is necessary, that the HA has been correctly performed, and that the HA can be terminated.
2) Plant personnel who are affected by the HAs should be identified including licensed control-room operators up to engineering support personnel.
3) Task analyses should provide detailed descriptions of what the personnel must do.
4) The task analysis should address the full range of plant conditions and situational factors, and performance-shaping factors anticipated to influence human performance. The range of plant-operating modes relevant to the HAs (*e.g.*, abnormal and emergency operations, transient conditions, and low-power and shutdown conditions) should be included in the task analysis.

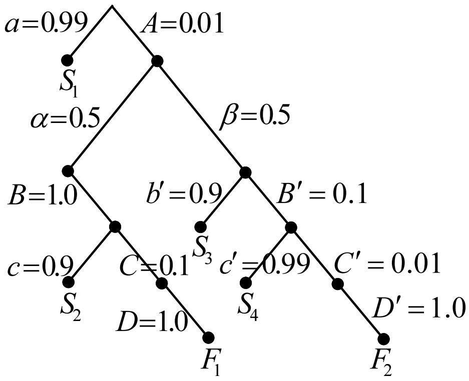


Fig. 9.4. Human-reliability analysis event tree

5) The human-task requirements should be assessed to determine whether they are compatible with each individual's responsibilities (*i.e.* will not interfere with or be disrupted by the cognitive and physical demands of other tasks and responsibilities).
6) The task analysis should identify reasonable or credible, potential errors.

9.6.2 HRA Event Tree

Deviations from a sequence of unit tasks are represented by a HRA ET (human-reliability analysis event tree). An example is given in Figure 9.4.

Assume that a technician is assigned the task of calibrating set points of three comparators that use OR logic to detect abnormal pressure [56]. The basic event in the fault tree is that OR detection logic fails due to a calibration error. The detection failure occurs when all three comparators are miscalibrated.

The worker must first assemble the test equipment. If he sets up the equipment incorrectly, the three comparators are likely to be miscalibrated. The calibration task consists of four unit activities:

1) Set up test equipment.
2) Calibrate comparator 1.
3) Calibrate comparator 2.
4) Calibrate comparator 3.

Figure 9.4 shows the HRA event tree. We observe the following conventions.

1) A capital letter represents a unit-task failure or its probability. The corresponding lowercase letter represents a unit-task success or probability.
2) Greek letters represent nonhuman events such as abnormal hardware-failure states caused by preceding human errors. In Figure 9.4 the hard-

Table 9.5. Unit-task failures and hardware states

Label	Description	P	Label	Description	P
A	Set-up error of test equip.	0.01			
α	Test equip. with small error	0.5	β	Test equip. with large error	0.5
B	Set-up error of comparator 1	1.0	B'	Set-up error of comparator 1	0.1
C	Set-up error of comparator 2	0.1	C'	Set-up error of comparator 2	0.01
D	Set-up error of comparator 3	1.0	D'	Set-up error of comparator 3	1.0

ware states are a small setup error α of test equipment and a large setup error β.

3) The letters S and F are exceptions to the above rule in that they represent, respectively, human-task success and failure. Failure is the simultaneous miscalibration of the three comparators.
4) The two-limb branch represents unit-task success and failure; each left limb expresses success and each right limb, failure. For hardware states, limbs are arranged from left to right in ascending order of severity of failure.
5) Limbs with zero or negligibly small probability of occurrence are removed from the event tree.

As shown in Table 9.5, the technician fails to correctly set up the test equipment with probability 0.01. If she succeeds in the setup, she will correctly calibrate at least one comparator. Assume that miscalibration of each of the three comparators occurs independently with probability 0.01; then simultaneous miscalibration occurs with probability $(0.01)^3 = 10^{-6}$, which is negligibly small. A common-cause failure is not considered here. The success limb $a = 0.99$ can therefore be truncated by success node S_1, which implies that one or more comparators are calibrated correctly.

Set-up error A results in a small or a large test equipment error with equal probability, 0.5 for each. We assume that the technician sets up comparator 1 without noticing a small set-up error. This is shown by the unit failure probability $B = 1.0$. While calibrating the second comparator, however, she would probably notice the small set-up error because it would seem strange that the two comparators happen to require identical adjustment simultaneously. Probability $c = 0.9$ is assigned to the successful discovery of a small set-up error. Success node S_2 results because the technician would almost certainly correct the set-up error and calibrate at least one comparator correctly. If the technician neglects the small set-up error during the first two calibrations, a third calibration error is almost certain. This is shown by unit probability $D = 1.0$. Failure node F_1 implies sequential miscalibration of three comparators.

A large test equipment set-up error would probably be noticed during the first calibration because it would seem strange that the first comparator required such a large adjustment. This is indicated by success probability $b' = 0.9$ of finding the set-up error. Success node S_3 implies the same event

Table 9.6. Modification of error probabilities by stress and skill levels

A Experienced personnel		
Stress level	Error probability modified	Uncertainty bounds modified
1 Very low	2 × Table BHEP	2 × Table BHEP
2 Optimum	Table BHEP	Table BHEP
3 Moderately high		
1) Step-by-step tasks	2 × Table BHEP	2 × Table BHEP
2) Dynamic tasks	5 × Table BHEP	5 × Table BHEP
4 Extremely high	0.25	$[0.03, 0.75]$

B Novices		
Stress level	Error probability modified	Uncertainty bounds modified
1 Very low	2 × Table BHEP	2 × Table BHEP
2 Optimum		
1) Step-by-step tasks	Table BHEP	Table BHEP
2) Dynamic tasks	2 × Table BHEP	2 × Table BHEP
3 Moderately high		
1) Step-by-step tasks	4 × Table BHEP	4 × Table BHEP
2) Dynamic tasks	10 × Table BHEP	10 × Table BHEP
4 Extremely high	0.25	$[0.03, 0.75]$

as S_2. Even if the large set-up error at the first calibration is neglected, it would almost certainly be noticed during the second calibration, thus yielding success node S_4 with probability $c' = 0.99$. The technician would assuredly fail to find the set-up error at the third calibration if the error was neglected during the first and second calibrations. This is evidenced by unit failure probability $D' = 1.0$. Failure node F_2 also implies sequential miscalibration (simultaneous failure) of the three comparators.

The probability of a success or failure node can be calculated by multiplying the appropriate probabilities along the path to the node. For example:

$$\Pr\{S_2\} = 0.01 \times 0.5 \times 1.0 \times 0.9 = 0.0045 \tag{9.6}$$

$$\Pr\{F_2\} = 0.01 \times 0.5 \times 0.1 \times 0.01 \times 1.0 = 0.000005 \tag{9.7}$$

Probability $\Pr\{F\}$ of occurrence of the basic event is the sum of failure-node probabilities:

$$\Pr\{F\} = \Pr\{F_1\} + \Pr\{F_2\} = 0.0005 + 0.000005 = 0.000505 \tag{9.8}$$

Insignificant numbers are carried simply for identification purposes.

9.6.3 Stress and Skill Level

The stress level is a global PSF because it influences the majority of unit tasks extracted by the task analysis. Figure 9.2 showed four stress levels: very low, optimal, moderately high, and extremely high. Human-error probabilities at the optimal level are called basic human-error probabilities (BHEPs) and are listed in the THERP Handbook [56]. Table 9.6 shows how BHEPs can be modified to reflect other nonoptimal stresses. Novices are more susceptible to the stress than experienced personnel at the moderately high stress level and for dynamic tasks at the optimal stress level.

A step-by-step task is one completed by a single action such as closing a valve. Dynamic tasks refer to those having correlations in space and time. Dynamic multivariable problems are more difficult to solve than static, single-variable ones. The former are typified by the following.

1) Some variables are not directly observable and must be estimated.
2) Variables are correlated.
3) The controlled process has a large time lag.
4) Humans tend to rely on short-term memory because various display indicators should be interpreted collectively.
5) Each unit process is complicated and difficult to visualize as a mental image.

Consider a selection-error probability (SEP) for an experienced worker. The value at the optimal stress level is 0.003 with the 90% confidence interval of $[0.001, 0.01]$. The SEP can be modified as:

1) Very low: $2 \times 0.003 = 0.006, \quad [0.002, 0.02]$
2) Moderately high: $2 \times 0.003 = 0.006, \quad [0.002, 0.02]$
3) Extremely high: $0.25, \quad [0.03, 0.75]$

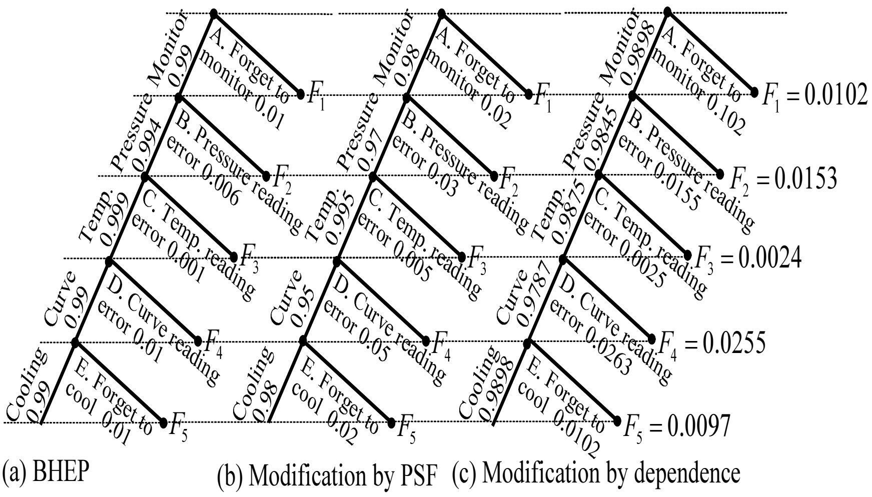
9.6.4 General THERP Procedure

First, the following three points are clarified.

1) human-error events in the fault or event trees;
2) human activities related to the event;
3) boundary conditions under which the activities are performed.

Second, the task analysis is performed and HRA event trees are developed by noting the following points:

1) Combining dependent events by context: For instance, omission failure to close the first valve usually leads to omission failures for the remaining valves if the valves are perceived as a group.
2) Neglecting small probabilities: If the occurrence probability in a limb is negligibly small, that limb and all successors can be removed from the tree as nondominant sequences.
3) Failure or success node: Further development of the event tree from a success or a failure node is not required.
4) Neglecting recovery factors: Estimated failure probability for a given sequence in an HRA event tree may be so low, without considering the effects of recovery factors, that the sequence will not be a dominant failure mode. In this case recovery factors can be dropped from further consideration.



(a) BHEP (b) Modification by PSF (c) Modification by dependence

Fig. 9.5. HRA event tree for cooldown operation

Third, probabilities are assigned to the event-tree limbs. The THERP Handbook BHEPs are usually based on the following limiting assumptions [42].

1) The plant is operating under normal conditions.
2) The operator need not wear protective clothing.
3) A level of administrative control roughly equal to industry-wide averages.
4) The tasks are performed by licensed, qualified plant personnel.
5) The working environment is adequate to optimal.

Suitable BHEPs are assigned to HRA event trees. Relevant PSFs are considered and the BHEPs are modified accordingly.

Dependencies among unit tasks and operators are evaluated. THERP considers 5 types of dependencies. Suppose task "A" is followed by task "B". Failure probability B of task B, given failure of task A, is determined according to the dependencies, where B_0 is the probability when task B is performed alone.

1) Complete dependence (CD): $B = 1$.
2) High-level dependence (HD): $B = (1 + B_0)/2$.
3) Moderate-level dependence (MD): $B = (1 + 6B_0)/7$.
4) Low-level dependence (LD): $B = (1 + 19B_0)/20$.
5) Zero dependence (ZD): $B = B_0$.

Finally, success and failure probabilities are calculated for the basic event of a fault tree. Recovery factors are considered for failure limbs that have relatively large probabilities. A sensitivity analysis is carried out. Results of the human-reliability analysis are then transmitted to fault-tree analysts.

Consider a control problem of water temperature and pressure of a reactor. The water starts boiling when the pressure becomes low as compared with the temperature. To prevent boiling, the temperature is lowered to keep the pressure above the saturation curve, where horizontal and vertical axes denote temperature and pressure, respectively. The task analysis yields the 5 unit tasks:

1) A: Start monitoring pressure and temperature.
2) B: Read pressure from pressure gauge.
3) C: Read temperature from temperature gauge.
4) D: Compare the saturation curve with the temperature and pressure point.
5) E: Start cooling the water when the point is below the curve.

An example of an HRA event tree is shown in Figure 9.5. Part (a) shows BHEPs, while part (b) results after modification by a moderately high stress level. Unit tasks B, C, and D are regarded as dynamic tasks, and the corresponding BHEPs are multiplied by 5. Tasks A and E are step-by-step tasks, and the BHEPs are doubled for modification.

Assume two operators in the control room. A standby operator may notice even if a principal operator fails. Assume the high-level dependence. Then the omission error, “forget monitoring pressure and temperature”, can be modified as follows:

$$(\text{new } A) = (\text{old } A) \times \frac{1 + (\text{old } A)}{2} = 0.02 \times \frac{1 + 0.02}{2} = 0.0102 \tag{9.9}$$

In other words, about 50% of the error can be recovered by the standby operator. The remaining HEPs are modified by the dependence, as shown in part (c). The failure probability of the control task is a sum of the five failure nodes.

9.7 Concluding Remarks

Human-error classification into pre- and postinitiator error is a distinctive feature of the PRA that is based on the concept of an initiating event. In spite of a large number of studies after the emergence of THERP, there has been little advancement in quantification of human error. The PRA may quantify partial aspects of human activities, although dependencies and uncertainties are considered. This lack of completeness should be complemented by qualitative, traditional, and deterministic approaches as described in Chapter 2.

References

1. IEC (1998) International standard. Functional safety of electrical/electronic/programmable electronic safety-related systems, IEC 61508, part 1-7.
2. USNRC (1986) Safety goals for the operations of nuclear power plants; Policy statement. Federal Register, Vol. 51 p. 30028 (51 FR 30028)
3. USNRC (1990) SECY-98-101 Modifications of the safety goal policy statement. See also Attachment 6: Staff analysis of issues associated with possible modification of the safety goal policy statement.
4. USNRC (1997) ACRS (Advisory Committee on Reactor Safeguards) letter to Chairman S.A. Jackson. Risk-based regulatory acceptance criteria for plant-specific application of safety goals.
5. ASME (2003) Standard for probabilistic risk assessment for nuclear power plant applications. ASME RA-Sa-2003. Addenda to ASME RA-S-2002.
6. USNRC (Sep. 12, 1997) Elevation of the core damage frequency objective to a fundamental commission safety goal. Staff Requirements Memorandum (SRM), SECY-97-208
7. Meserve RA (2001) The evolution of safety goals and their connection to safety culture. ANSJ/ANS Topical Meeting on Safety Goals and Safety Culture, Milwaukee, Wisconsin.
8. USNRC (1990) SECY-89-102 Implementation of the safety goals.
9. USNRC (2002) Use of probabilistic risk assessment in plant-specific, risk-informed decision-making: General Guidance. Revision 1 of standard review plan Chapter 19.
10. Memorandum from Chairman (July 2, 1997) The statement of core damage frequency of 10^{-4} as a fundamental commission goal.
11. IEC (2003) International standard. Functional safety – Safety instrumented systems for the process industry sector. IEC 61511, part 1-3, IEC.
12. USNRC (2002) Regulatory Guide 1.174 – An approach for using probabilistic risk assessment in risk-informed decisions on plant-specific changes to the licensing basis. Revision 1.
13. USNRC (2004) Guidance for the review of changes to human actions. Final report. NUREG-1764.
14. USNRC (1998) Regulatory Guide 1.177 – An approach for plant-specific, risk-informed decision-making: Technical specifications.

15. USNRC(1996) ACRS letter to Chairman S.A. Jackson. Risk-informed, performance-based regulation and related matters.
16. USNRC (1995) Use of probabilistic risk assessment methods in nuclear regulatory activities; Final policy statement. Federal Register, Vol. 60, p. 42622.
17. USNRC (1998) Regulatory Guide 1.175 – An approach for plant-specific, risk-informed decision-making: Inservice testing.
18. NEI (2004) 10 CFR 50.69 SSC Categorization Guideline. NEI 00-04.
19. HSE (1992) The tolerability of risk from nuclear power stations. UK HSE (Health and Safety Executive).
20. IAEA (1999) Basic safety principles for nuclear power plants. 75-INSAG-3 Rev. 1, INSAG-12. A report by the International Nuclear Safety Advisory Group.
21. HSE (2001) Reducing risks, protecting people. HSE's decision-making process, HSE Books.
22. Ball DJ, Floyd PJ (1998) Societal risks. Report available from the Risk Assessment Policy Unit, HSE.
23. Kleinbreuer W, Kreutzkampf F, Meffert K, Reinert D (1999) Categories for safety-related control systems in accordance with EN 954-1. HVBG
24. HSE (2002) Technical issues arising from the implementation of making paper safety. Sector Information Minute.
25. Schäbe H (2001) Different approaches for determination of tolerable hazard rates. ESREL 2001, Torino, Conference Proceedings, Vol. 1, pp. 435–442.
26. EN (March, 2000) EN 50126 railway applications. The specification and demonstration of dependability, reliability, availability, maintainability and safety (RAMS) issue. EN 50126.
27. EN (June, 1997) Final Draft prEN 50128 railway applications, Software for railway control and protection systems issue. EN 50128.
28. EN (April, 2000) EN 50129 railway applications, Safety related electronic systems for signaling issue.
29. Lambert HE (1991) Case study on the use of PSA methods: Determining safety importance of systems and components at nuclear power plants. IAEA IAEA-TECHDOC-590.
30. BS EN 954-1 (1997) Safety of machinery, Safety related parts of control systems, General principles for design. British Adopted European Standard.
31. Code of Federal Regulations. 10 CFR Part 50. Domestic licensing of production and utilization facilities.
32. USNRC (1998) Regulatory Guide 1.176 – An approach for plant-specific, risk-informed decision-making: Graded quality assurance.
33. Vesely WE, Davis TC, Denning RS, Saltos N (1983) Measures of risk importance and their applications. NUREG/CR-3385, BMI-2103, USNRC.
34. Mosleh A, Rasmuson DM, Marshall FM (1998) Guidelines on modeling common-cause failures in probabilistic risk assessment. NUREG/CR-5485, USNRC.
35. USNRC (2002) Handbook of parameter estimation for probabilistic risk assessment. NUREG/CR-6823, SAND2003-3348P.
36. USNRC (1998) Guidelines on modeling common-cause failures in probabilistic risk assessment. NUREG/CR-5485.
37. USNRC (2002) Human–system interface design review guidelines. NUREG-0700, Rev. 2.
38. USNRC (2004) Human factors engineering program review model. NUREG-0711, Rev. 2.

39. Johnson WG (1980) Mort Safety Assurance Systems. Marcel Dekker, New York.
40. Redmill F, Chudleigh M, Catmur J (1999) System Safety: HAZOP and Software HAZOP. John Wiley and Sons.
41. McDermott RE, Mikulak RJ, Beauregard M R (1996) The Basics of FMEA. Productivity, Inc.
42. USNRC (1983) PRA procedures guide: A guide to the performance of probabilistic risk assessments for nuclear power plants. USNRC, NUREG/CR-2300.
43. Papazoglou IA, Aneziris ON (2003) Master logic diagram: method for hazard and initiating event identification in process plants. J. Hazard. Mater. Vol. 97, No. 1: 11–30
44. HSE Home Page. Five steps to risk assessment.
45. NEI (1996) Industry guideline for monitoring the effectiveness of maintenance at nuclear power plants. Nuclear Energy Institute, NUMARC 93-1 01, Revision 2.
46. vonHerrmann JL, Wood PJ (1989) The practical application of PRA: An evaluation of utility experience and USNRC perspectives. Reliab. Eng. Syst. Saf., vol. 24, no. 2; 167–198
47. Papazoglou IA, Aneziris O, Christou M, Nivoliantou Z (1991) Probabilistic safety analysis of an ammonia storage plant. In Probabilistic Safety Assessment and Management, edited by G. Apostolakis, New York, Elsevier; 233–238.
48. USNRC (1975) Reactor safety study: An assessment of accident risk in U.S. Commercial nuclear power plants. WASH-1400, NUREG-75/014.
49. Apostolakis GE, Bickel JH, Kaplan S (1989) Editorial: Probabilistic risk assessment in the nuclear power utility industry. Reliab. Eng. Syst. Saf., vol. 24, no. 2; 91–94.
50. USNRC (1990) Severe accident risks: An assessment for five U.S. nuclear power plants. NUREG-1150, vol. 2.
51. Travers WD (2000) PRA scope and technical attributes. Attachment to SECY-00-0162. Addressing PRA quality in risk-informed activities. USNRC.
52. Hake TM, Whitehead DW (1991) Initiating event analysis for a BWR low power and shutdown accident frequency analysis. In Probabilistic Safety Assessment and Management, edited by G. Apostolakis, New York, Elsevier; 1251–1256.
53. Kumamoto H, Henley EJ (1996) Probabilistic Risk Assessment and Management for Engineers and Scientists. IEEE Press.
54. USNRC (1983) PRA procedures guide: A guide to the performance of probabilistic risk assessments for nuclear power plants. NUREG/CR-2300.
55. Arrieta LA, Lederman L (1987) Angra I probabilistic safety study. In Implications of Probabilistic Risk Assessment, edited by Cullingford M.C., Shah S.M., Gittus J.H., New York: Elsevier Applied Science: 45–63.
56. Swain AD , Guttman HE (1983) Handbook of human reliability analysis with emphasis on nuclear power plant applications. NUREG/CR-1278, USNRC.
57. American Nuclear Society (2003) American national standard external-events PRA methodology. ANSI/ANS-58.21-2003, ANS.
58. Reyes LA (2004) Action plant: Stabilizing the PRA quality expectations and requirements. Attachment to SECY-04-0118, Plan for the implementation of the commissions phased approach to probabilistic risk assessment quality. USNRC.
59. Hahn GJ, Shapiro SS (1967) Statistical Methods in Engineering. New York, John Wiley and Sons.
60. Kececioglu D(1993) Reliability and Life Testing Handbook, Volume 1. PTR Prentice Hall.

61. USNRC (1985) A SETS user's manual for accident sequence analysis. NUREG/CR-3547, SAND83-2238.
62. USNRC (1993) Integrated reliability and risk analysis system version 5.0 reference manual. NUREG/CR-6116.
63. Fussell JB, Henry EB, Marshall NH (1974) MOCUS: A computer program to obtain minimal cut sets from fault trees. Aerojet Nuclear Company, ANCR-1156.
64. Esary JD, Proschan F (1970) A reliability bound for systems of maintained and independent components. J. Am. Stat. Assoc., Vol. 65, pp. 329–338.
65. Fleming KN (1975) A reliability model for common mode failure in redundant safety systems. Proc. of the 6th Annual Pittsburgh Conference on Modeling and Simulation, General Atomic Report GA-A13284.
66. Smith D, Simpson K (2003) Functional Safety - A Straightforward Guide to Applying IEC 61508 and Related Standards. 2nd eds., Butterworth-Heinemann.
67. Zuo G, Kumamoto H, Nishihara O, Hayama R, Nakano R (2005) Quantitative reliability analysis of different design alternatives for steer-by-wire system. Reliab. Eng. Syst. Saf., Vol. 89: 241–247
68. Personal communication with Dr. Nakano S at JTEKT (2006).
69. Swain AD (1987) Accident sequence evaluation program: Human reliability analysis procedure. Sandia National Laboratories, NUREG/CR-4722, SAND86-1996.
70. EPRI (1984) Systematic human action reliability procedure (SHARP). EPRI NP-3583.
71. EPRI (1992) An approach to the analysis of operator actions in probabilistic risk assessment. EPRI TR-100259.
72. EPRI (1989) A human reliability analysis approach using measurements for individual plant examination. EPRI NP-65601.
73. Cooper SE, Ramey-Smith AM, Wreathall J *et al.* (1996) A technique for human error analysis (ATHEANA). NUREG/CR-6350, USNRC.
74. http://www.epri.com/hra/discuss.html
75. Hancock PA (1993) Modeling the basic error tendencies of human operators. Reliab. Eng. Syst. Saf., Vol. 22, pp. 137–153.
76. Wakefield DJ (1988) Application of the human cognitive reliability model and confusion matrix approach in a probabilistic risk assessment. Reliab. Eng. Syst. Saf., Vol. 22, pp. 295–312.
77. USNRC (2000) Memorandum and order, CLI-00-03, Docket No. 55-32443-SP.
78. Wreathall J (1982) Operator action trees: An approach to quantifying operator error probability during accident sequences. NUS Rep. No. 4159, NUS Corporation.
79. USNRC (2004) Guidance for the review of changes to human actions. NUREG 1764.
80. IAEA (1991) Case study on the use of PSA methods: Human reliability analysis. IAEA-TECDOC-592.
81. Rasmussen J (1986) Information Processing and Human–machine Interaction: An Approach to Cognitive Engineering. New York: North-Holland Series in System Science and Engineering.
82. Hannaman GW, Spurgin AJ, Lukic YD (1984) Human cognitive reliability model for PRA analysis. NUS-4531, EPRI.

Index

Abnormal-event vocabularies, 98
Accident management, 111
Accident-frequency analysis, 123
Accident-progression analysis, 133
Accident-sequence
  grouping, 132
  quantification, 130
  screening, 130
Adequate protection, 6
Alarm
  demand probability, 200
  false, 197
  false-alarm function, 198
  false-alarm probability, 200
  generating function, 197
  inactive, 197
  inactive-alarm function, 199
  inactive-alarm probability, 200
ALARP, 22, 39
Alpha-factor model, 206
  CCBE probability, 210
  parameter definition, 209
  parameter distribution, 212
  staggered testing, 214
Ammonia storage facility, 116
Automatic actuation, 109

Basic events, 145
  transition diagram, 146
Beta-factor model, 215
Brain bottleneck, 226

Categorization
  function and SSC, 62
  guideline, 52
  performance evaluation, 86
  qualitative criteria, 56
  redundant-valve example, 58
  risk-informed, 57
  safety-significance, 55
  sensitivity studies, 60
Category
  machinery safety, 52
Cause-defense matrix, 77
Change control, 107
Collision safety, 223
Common-cause failure, 73, 203
  2-component CCCG, 210
  3-component CCCG, 211
  alpha parameter definition, 209
  alpha-factor model, 206
  basic event, 206, 208
  beta-factor model, 215
  cause-level analysis, 204
  component group, 206, 208
  component total probability, 209
  first-order probability, 212
  simultaneous failure probability, 208
  start and run failure, 207
  voting-system failure probability, 211
  voting-system minimal cut sets, 211
Coupling mechanisms, 73

Damage probability, 142
Database analysis, 132
Decision making
  deterministic, 16
  integrated, 16

principles, 17
probabilistic, 17
Defense-in-depth, 18, 85, 86
Demand failure probability
1oo1, 91
1oo2, 91
2oo2, 92
2oo3, 92
example, 93
Demand-failure probability
common cause, 90
independent, 87
Dependency
along accident sequence, 129
common-cause failures, 73
component hardware failure, 73, 76
cooling-requirement, 75
explicit, 73, 131
failure analysis, 131
functional, 71
human-interaction, 72, 75
implicit, 73, 131
inter, 108
outer, 108
phenomenological-effect, 76
power-requirement, 74
purity-requirement, 75
safety principles, 74
shared-component, 74
spatial, 73
type, 71
Detection, 80
system behavior, 82
Deterministic analysis, 120
Deterministic approach, 16
Diagnostic coverage, 81

Early detection and treatment, 80
EC 61508, 84
EN 50126, 38, 40, 41
EN 50128, 38
EN 50129, 38
EN 951, 35
EN 954, 52, 55, 74, 78
Event tree
analysis, 118
construction, 126
coupled with fault trees, 126
function, 126
HRA event tree, 239
large ET/small FT, 127
LOCA, 117
pruning, 119
small ET/large FT, 129
system, 127
External event, 61
PRA standards, 143

Fail-safe design, 109
Fail-soft design, 109
Failure
common cause, 203
dependent, 71
early, 164
partial, 218
primary, 161
random, 15, 163
secondary, 161
start and run, 207
systematic, 15
wearout, 166
Fatality statistics, 4
Fault tolerance
hardware, 83
Fault tree
analysis, 117
construction, 130
linking, 188
module, 187
single large, 184
Fault-tolerant design, 218
FMEA, 101
Function, 36
names, 100
Functional safety system, 36

Graceful degradation, 217
reliability quantification, 222
Guidelines, 70

Hazard, 95
association, 97
classification, 96
measures, 96
Hazardous
event, 35
situation, 35
HAZOP, 97

High-demand mode, 40
Human actions
  safety significance, 62
Human error
  available time, 235
  classification, 226
  HRA event tree, 239
  lapse, 227
  median operator-detection time, 235
  median response time, 234
  mistake, 227
  no detection, 227
  nonresponse probability, 234
  performance-shaping factors, 229
  prevention, 107
  skill level, 241
  slip, 227
  stress, 229, 241
  task analysis, 238
  THERP, 237, 242
Human-factors review, 62, 65, 66, 79
Human-reliability analysis, 131

IEC 61508, 35, 36, 38, 40, 41, 52, 55, 60, 74, 76, 78, 80, 81, 84, 89, 92
IEC 61511, 19, 20, 21, 22, 24, 35, 38, 39, 40, 41, 44, 50, 60, 74, 76, 78, 83, 84, 85
Importance
  Fussell–Vesely, 58, 64
  RAW, 58, 64
Inclusion-exclusion formula
  bounds, 196
  exact, 195
Inherently safer design, 105
Initiating event, 113
  analysis, 125
  definition, 103
  mitigation, 108
  prevention, 105
Internal event, 58
ISO 12100, 96
ISO 13849, 52
ISO 14121, 96
ISO 9000, 70

LOCA event tree, 117
Logic
  backward, 118
  forward, 118
Lognormal distribution, 168
LOPA, 46

Maintenance
  corrective, 107
  instantaneous repair, 162
  online, 107
  periodic, 106
  predictive, 106
  preventive, 106
Markov
  analysis, 217
  differential equation, 222
  transition diagram, 220
Master logic diagram, 103
Minimal cut sets, 184
Minimal path sets, 185
Minimal-cut generation, 186
Mitigation, 9, 105
  accident, 110
  offsite consequence, 111
  onsite consequence, 111
  systems, 108
MOCUS, 186

NEI 00-04, 52
Nonseries-parallel system, 183
Normal control systems, 108
NUREG-1150, 103, 121, 123, 125, 131, 134, 135, 138
NUREG-1764, 62, 64, 229, 232
NUREG/CR-3385, 58
NUREG/CR-5485, 72, 74, 77, 206, 215

Oil tanker, 116

Parallel system, 181
Parameter
  availability, 153
  combined process, 153, 156, 160
  constant failure rate, 158
  constant repair rate, 158
  expected number of failures, 154
  expected number of repairs, 155
  failure density, 148
  failure intensity, 154
  failure rate, 149
  failure-to-repair process, 151, 156, 159

fractional time availability, 162
MTTF, 150
MTTR, 153
nonrepairability, 151
relations, 155
reliability, 147
repair density, 152
repair intensity, 154
repair rate, 152
repair-to-failure process, 147, 155, 158
repairability, 152
unavailability, 153
unreliability, 148
Parameter estimation, 163
exponential, 163
Weibull early, 164
Weibull wearout, 166
Performance evaluation, 86
Performance-shaping factors, 229
Plant familiarization, 124
Poisson process, 162
Postinitiator human error, 227
Power-source
unavailability, 161
unreliability, 161
PRA
ASME quality standard, 121, 124, 125
level 1, 123, 133
level 2, 133
level 3, 134
nonnuclear, 120
three levels, 122
WASH-1400, 117
with material hazards, 113, 116
without material hazards, 113, 114, 137
PRA parameters, 174
Bayesian approach, 176
data, 174
demand and standby failure, 177
demand failure, 177
hierarchical Bayes, 178
rate, 176
types, 174
unavailability, 177
Preinitiator human error, 226
Pressure-tank example, 42, 59
Prevention, 9, 105
Probabilistic approach, 17
Protection layer, 21
Public confidence, 6

Quality-assurance program, 54

Railway
freight, 116
passenger, 114
Reactor scram, 37
Recovery, 109
Regulations, 70
Reliability block diagram, 179
Risk, 95
ALARP, 22
aversive, 38
calculation, 134
expected consequence, 136
graph, 51
increase, 10
individual, 3, 26, 29
level 1 profile, 138
level 2 profile, 137
level 3 profile, 134
profiles, 113
radiation fatality, 22
reduction measures, 103
societal, 3, 26, 27, 29, 30
tolerability, 22
TOR framework, 26
TOR requirements, 24
Robustness, 110

Safe-failure fraction, 82
Safety goals
CDF, 8
health objectives, 2
LERF, 8
permanent change, 10
policy statement, 2
qualitative, 3
quantitative, 3
risk increase, 10
risk-aversive, 38
subsidiary, 6, 9
temporary, 6
temporary change, 12
Safety integrity level, 35, 38

demand mode, 45
high-demand mode, 40
Safety margins, 22, 78, 105
Safety principles
component hardware failure dependencies, 76
cooling-requirement dependencies, 75
human-interaction dependencies, 75
phenomenological-effect dependencies, 76
power-requirement dependencies, 74
purity-requirement dependencies, 75
shared-component dependencies, 74
Safety significance
categorization, 55
integrated assessment, 67
qualitative assessment, 65
qualitative criteria, 56
quantitative assessment, 63
Safety-layer matrix, 49
Seismic
epicenter distance, 140
excess frequency, 142
frequency, 142
ground-motion, 142
hazard curve, 139
hazards, 138
magnitude, 140
Semiquantitative method, 42
Sensitivity studies, 60
Series system, 180
SFF, 83
Shutdown, 61
SIL, 83
SIS, 36, 45
Quantification, 87
Source-term analysis, 134
Special treatment, 86
SSC
Safety-related, 53
Standardization, 106
Standards, 70
Steer-by-cable, 223
Steer-by-wire, 217
Stress, 229
Stress and response model, 170
lognormal, 173
normal, 172
Structure function
2/3 gate, 189
AND gate, 189
coherent, 195
definition, 189
minimal-cut representation, 191
minimal-path representation, 192
OR gate, 189
pivot expansion, 193
unavailability, 190
upper and lower bounds, 194
Symptom-based procedures, 109

THERP, 237
general procedure, 242
TOR, 22, 24, 26

Uncertainty, 14, 69
aleatory, 14
analysis, 133
completeness, 15
epistemic, 14
modeling, 15
parameter, 14
risk profiles, 138

Voting system, 181
1oo1, 91
1oo2, 91
2oo2, 92
2oo3, 92
failure probability, 211
minimal cut sets, 211

WASH-1400, 117