

Probabilistic Risk Analysis: Foundations and Methods

Tim Bedford

*Delft University of Technology
and
University of Strathclyde*

Roger Cooke

Delft University of Technology



PUBLISHED BY THE PRESS SYNDICATE OF THE UNIVERSITY OF CAMBRIDGE
The Pitt Building, Trumpington Street, Cambridge, United Kingdom

CAMBRIDGE UNIVERSITY PRESS

The Edinburgh Building, Cambridge CB2 2RU, UK
40 West 20th Street, New York, NY 10011-4211, USA
477 Williamstown Road, Port Melbourne, VIC 3207, Australia
Ruiz de Alarcón 13, 28014 Madrid, Spain
Dock House, The Waterfront, Cape Town 8001, South Africa

<http://www.cambridge.org>

© Cambridge University Press 2001

This book is in copyright. Subject to statutory exception
and to the provisions of relevant collective licensing agreements,
no reproduction of any part may take place without the written
permission of Cambridge University Press

First published 2001

Reprinted 2003

Printed in the United Kingdom at the University Press, Cambridge

Typeface Times 11/14pt *System* L^AT_EX2e [UPH]

A catalogue record for this book is available from the British Library

Library of Congress Cataloguing in Publication data

Bedford T.

Mathematical tools for probabilistic risk analysis / Tim Bedford and Roger M. Cooke.
p. cm.

Includes bibliographical references and index.

ISBN 0 521 77320 2

1. Reliability (Engineering)-Mathematics. 2. Risk assessment. 3. Probabilities. I.
Cooke, Roger M., 1946-II. Title.

TA169.B44 2001

620'.00452'0151-dc21

00-046762

ISBN 0 521 77320 2 hardback

Contents

<i>Illustrations</i>	<i>page</i>	xiii
<i>Tables</i>		xvi
<i>Preface</i>		xix
Part I: Introduction		1
1	Probabilistic risk analysis	3
1.1	Historical overview	4
1.1.1	The aerospace sector	4
1.1.2	The nuclear sector	5
1.1.3	The chemical process sector	8
1.1.4	The less recent past	9
1.2	What is the definition of risk?	9
1.3	Scope of probabilistic risk analyses	11
1.4	Risk analysis resources	12
1.4.1	Important journals	12
1.4.2	Handbooks	12
1.4.3	Professional organizations	12
1.4.4	Internet	13
Part II: Theoretical issues and background		15
2	What is uncertainty?	17
2.1	The meaning of meaning	17
2.2	The meaning of uncertainty	19
2.3	Probability axioms	21
2.3.1	Interpretations	22
2.4	Savage's theory of rational decision	24
2.4.1	Savage's axioms	26
2.4.2	Quantitative probability	28

2.4.3	Utility	28
2.4.4	Observation	28
2.5	Measurement of subjective probabilities	30
2.6	Different types of uncertainty	33
2.7	Uncertainty about probabilities	35
3	Probabilistic methods	39
3.1	Review of elementary probability theory	39
3.2	Random variables	41
3.2.1	Moments	42
3.2.2	Several random variables	43
3.2.3	Correlations	44
3.2.4	Failure rates	45
3.3	The exponential life distribution	47
3.3.1	Constant test intervals	48
3.3.2	Exponential failure and repair	50
3.4	The Poisson distribution	51
3.5	The gamma distribution	52
3.6	The beta distribution	53
3.7	The lognormal distribution	54
3.8	Stochastic processes	55
3.9	Approximating distributions	58
4	Statistical inference	61
4.1	Foundations	61
4.2	Bayesian inference	63
4.2.1	Bayes' Theorem	64
4.2.2	An example with the exponential distribution	67
4.2.3	Conjugate distributions	69
4.2.4	First find your prior	70
4.2.5	Point estimators from the parameter distribution	74
4.2.6	Asymptotic behaviour of the posterior	74
4.3	Classical statistical inference	75
4.3.1	Estimation of parameters	75
4.3.2	Non-parametric estimation	77
4.3.3	Confidence intervals	78
4.3.4	Hypothesis testing	79
5	Weibull Analysis	83
5.1	Definitions	85
5.2	Graphical methods for parameter fitting	85
5.2.1	Rank order methods	86
5.2.2	Suspended or censored items	88

5.2.3	The Kaplan–Meier estimator	91
5.3	Maximum likelihood methods for parameter estimation	92
5.4	Bayesian estimation	94
5.5	Extreme value theory	94
	Part III: System analysis and quantification	97
6	Fault and event trees	99
6.1	Fault and event trees	99
6.2	The aim of a fault-tree analysis	100
6.3	The definition of a system and of a top event	103
6.3.1	External boundaries	103
6.3.2	Internal boundaries	104
6.3.3	Temporal boundaries	104
6.4	What classes of faults can occur?	104
6.4.1	Active and passive components	105
6.4.2	Primary, secondary and command faults	105
6.4.3	Failure modes, effects and mechanisms	105
6.5	Symbols for fault trees	106
6.6	Fault tree construction	106
6.7	Examples	108
6.7.1	Reactor vessel	108
6.7.2	New Waterway barrier	109
6.8	Minimal path and cut sets for coherent systems	110
6.8.1	Cut sets	110
6.8.2	Path sets	112
6.9	Set theoretic description of cut and path sets	112
6.9.1	Boolean algebra	112
6.9.2	Cut set representation	114
6.9.3	Path set representation	115
6.9.4	Minimal cut set/path set duality	115
6.9.5	Parallel and series systems	117
6.10	Estimating the probability of the top event	117
6.10.1	Common cause	118
7	Fault trees – analysis	121
7.1	The MOCUS algorithm for finding minimal cut sets	121
7.1.1	Top down substitution	121
7.1.2	Bottom up substitution	122
7.1.3	Tree pruning	122
7.2	Binary decision diagrams and new algorithms	123
7.2.1	Prime implicants calculation	129

7.2.2	Minimal p-cuts	130
7.2.3	Probability calculations	132
7.2.4	Examples	132
7.2.5	The size of the BDD	134
7.3	Importance	135
8	Dependent failures	140
8.1	Introduction	140
8.2	Component failure data versus incident reporting	140
8.3	Preliminary analysis	141
8.4	Inter-system dependencies	143
8.5	Inter-component dependencies – common cause failure	143
8.6	The square root bounding model	143
8.7	The Marshall–Olkin model	143
8.8	The beta-factor model	146
8.8.1	Parameter estimation	147
8.9	The binomial failure rate model	148
8.10	The α -factor model	151
8.11	Other models	151
9	Reliability data bases	153
9.1	Introduction	153
9.2	Maintenance and failure taxonomies	156
9.2.1	Maintenance taxonomy	156
9.2.2	Failure taxonomy	157
9.2.3	Operating modes; failure causes; failure mechanisms and failure modes	158
9.3	Data structure	160
9.3.1	Operations on data	161
9.4	Data analysis without competing risks	163
9.4.1	Demand related failures: non-degradable components	163
9.4.2	Demand related failures: degradable components	164
9.4.3	Time related failures; no competing risks	165
9.5	Competing risk concepts and methods	166
9.5.1	Subsurvivor functions and identifiability	168
9.5.2	Colored Poisson representation of competing risks	170
9.6	Competing risk models	172
9.6.1	Independent exponential competing risk	172
9.6.2	Random clipping	175
9.6.3	Random signs	175
9.6.4	Conditionally independent competing risks	177
9.6.5	Time window censoring	179

9.7	Uncertainty	179
9.7.1	Uncertainty due to non-identifiability: bounds in the absence of sampling fluctuations	180
9.7.2	Accounting for sampling fluctuations	182
9.7.3	Sampling fluctuations of Peterson bounds	182
9.8	Examples of dependent competing risk models	184
9.8.1	Failure effect	185
9.8.2	Action taken	186
9.8.3	Method of detection	188
9.8.4	Subcomponent	189
9.8.5	Conclusions	189
10	Expert opinion	191
10.1	Introduction	191
10.2	Generic issues in the use of expert opinion	192
10.3	Bayesian combinations of expert assessments	192
10.4	Non-Bayesian combinations of expert distributions	194
10.5	Linear opinion pools	199
10.6	Performance based weighting – the classical model	199
10.6.1	Calibration	200
10.6.2	Information	202
10.6.3	Determining the weights	203
10.6.4	Approximation of expert distributions	206
10.7	Case study – uncertainty in dispersion modeling	208
11	Human reliability	218
11.1	Introduction	218
11.2	Generic aspects of a human reliability analysis	220
11.2.1	Human error probabilities	220
11.2.2	Task analysis	220
11.2.3	Performance and error taxonomy	221
11.2.4	Performance shaping factors	223
11.3	THERP – technique for human error rate prediction	224
11.3.1	Human error event trees	226
11.3.2	Performance shaping factors	227
11.3.3	Dependence	227
11.3.4	Time dependence and recovery	228
11.3.5	Distributions for HEPs	228
11.4	The Success Likelihood Index Methodology	230
11.5	Time reliability correlations	232
11.6	Absolute Probability Judgement	235
11.7	Influence diagrams	236
11.8	Conclusions	238

12	Software reliability	240
12.1	Qualitative assessment – ways to find errors	240
12.1.1	FMECAs of software-based systems	240
12.1.2	Formal design and analysis methods	241
12.1.3	Software sneak analysis	241
12.1.4	Software testing	241
12.1.5	Error reporting	242
12.2	Software quality assurance	242
12.2.1	Software safety life-cycles	242
12.2.2	Development phases and reliability techniques	243
12.2.3	Software quality	245
12.2.4	Software quality characteristics	245
12.2.5	Software quality metrics	245
12.3	Software reliability prediction	245
12.3.1	Error seeding	247
12.3.2	The Jelinski–Moranda model	247
12.3.3	Littlewood’s model	248
12.3.4	The Littlewood–Verral model	249
12.3.5	The Goel–Okumoto model	250
12.4	Calibration and weighting	251
12.4.1	Calibration	251
12.4.2	Weighted mixtures of predictors	253
12.5	Integration errors	253
12.6	Example	255
	Part IV: Uncertainty modeling and risk measurement	257
13	Decision theory	259
13.1	Preferences over actions	261
13.2	Decision tree example	262
13.3	The value of information	264
13.3.1	When do observations help?	267
13.4	Utility	268
13.5	Multi-attribute decision theory and value models	269
13.5.1	Attribute hierarchies	270
13.5.2	The weighting factors model	271
13.5.3	Mutual preferential independence	271
13.5.4	Conditional preferential independence	274
13.5.5	Multi-attribute utility theory	277
13.5.6	When do we model the risk attitude?	280
13.5.7	Trade-offs through time	281

13.6	Other popular models	281
13.6.1	Cost–benefit analysis	281
13.6.2	The analytic hierarchy process	283
13.7	Conclusions	283
14	Influence diagrams and belief nets	286
14.1	Belief networks	286
14.2	Conditional independence	288
14.3	Directed acyclic graphs	289
14.4	Construction of influence diagrams	290
14.4.1	Model verification	292
14.5	Operations on influence diagrams	294
14.5.1	Arrow reversal	294
14.5.2	Chance node removal	294
14.6	Evaluation of influence diagrams	295
14.7	The relation with decision trees	295
14.8	An example of a Bayesian net application	296
15	Project risk management	299
15.1	Risk management methods	300
15.1.1	Identification of uncertainties	300
15.1.2	Quantification of uncertainties	302
15.1.3	Calculation of project risk	302
15.2	The Critical Path Method (CPM)	302
15.3	Expert judgement for quantifying uncertainties	304
15.4	Building in correlations	305
15.5	Simulation of completion times	305
15.6	Value of money	306
15.7	Case study	307
16	Probabilistic inversion techniques for uncertainty analysis	316
16.1	Elicitation variables and target variables	318
16.2	Mathematical formulation of probabilistic inversion	319
16.3	PREJUDICE	320
16.3.1	Heuristics	320
16.3.2	Solving for minimum information	321
16.4	Infeasibility problems and PARFUM	322
16.5	Example	323
17	Uncertainty analysis	326
17.1	Introduction	326
17.1.1	Mathematical formulation of uncertainty analysis	326
17.2	Monte Carlo simulation	327

17.2.1	Univariate distributions	327
17.2.2	Multivariate distributions	328
17.2.3	Transforms of joint normals	329
17.2.4	Rank correlation trees	330
17.2.5	Vines	334
17.3	Examples: uncertainty analysis for system failure	339
17.3.1	The reactor example	339
17.3.2	Series and parallel systems	341
17.3.3	Dispersion model	342
17.5	Appendix: bivariate minimally informative distributions	346
17.5.1	Minimal information distributions	346
18	Risk measurement and regulation	350
18.1	Single statistics representing risk	350
18.1.1	Deaths per million	350
18.1.2	Loss of life expectancy	351
18.1.3	Delta yearly probability of death	353
18.1.4	Activity specific hourly mortality rate	354
18.1.5	Death per unit activity	355
18.2	Frequency <i>vs</i> consequence lines	355
18.2.1	Group risk comparisons; ccdf method	356
18.2.2	Total risk	359
18.2.3	Expected disutility	360
18.2.4	Uncertainty about the fC curve	361
18.2.5	Benefits	362
18.3	Risk regulation	362
18.3.1	ALARP	362
18.3.2	The value of human life	363
18.3.3	Limits of risk regulation	365
18.4	Perceiving and accepting risks	365
18.4.1	Risk perception	367
18.4.2	Acceptability of risks	368
18.5	Beyond risk regulation: compensation, trading and ethics	369
	<i>Bibliography</i>	373
	<i>Index</i>	390

Illustrations

1.1	Risk curve	10
3.1	A schematic representation of a bathtub curve	46
3.2	Availability of a component under constant test intervals	49
3.3	Exponential failure and repair	50
3.4	A lognormal density	54
3.5	A lognormal failure rate	55
4.1		65
4.2	Prior and posterior density and distribution functions	68
4.3	Prior and posterior density and distribution functions (100 observations)	70
5.1	Densities for the Weibull distribution	85
5.2	A Weibull plot of the data in Table 5.4	89
5.3	Revised Weibull plot for Table 5.6	91
6.1	An event tree	100
6.2	The Cassini event tree	101
6.3	Security system	102
6.4	AND and OR gates	103
6.5	Common gates and states	107
6.6	Schematic diagram for the reactor protection system	108
6.7	Fault tree for the reactor protection system	109
6.8	Schematic diagram for the New Waterway water-level measurement system	110
6.9	Fault tree for the New Waterway water-level measurement system	111
6.10	Cut set fault tree representation for the reactor protection example	114
6.11	Path set fault tree representation for the reactor protection example	116
6.12	Dual tree for the reactor protection example	116
6.13	Very simple fault tree	119
7.1	Cut set calculation for the reactor protection system	122
7.2	A power system	124
7.3	The simple coherent fault tree from Example 7.2	125
7.4	The simple non-coherent fault tree from Example 7.3	126
7.5	A binary decision tree for Example 7.2	127

7.6	Application of the simplification rules	128
7.7	BDD for Example 7.3	128
7.8	BDD representation for the reactor protection example	133
7.9	BDD representation for the electrical power system example	133
7.10	Probability calculations for the electrical power system example	134
7.11	Fault tree example	137
8.1	Auxiliary Feedwater System	141
9.1	Maintenance and failure in time	159
9.2	Hierarchical categories	160
9.3	Superposed and pooled time histories	163
9.4	Calendar time picture of censored data	170
9.5	Censored failure data from four plants	173
9.6	Data fields for coloring	185
9.7	Coloring of 'failure effect'	186
9.8	Coloring of 'action taken'	187
9.9	Coloring of 'method of detection'	188
9.10	Coloring of 'subcomponent'	189
10.1	The expert's interpolated density	203
10.2	Expert ranking	204
10.3	Interpolation of expert quantiles	206
10.4	Combination of expert distributions	207
10.5	Range graphs	214
10.6	Range graphs	215
11.1	Classification of expected cognitive performance	222
11.2	The dynamics of GEMS	223
11.3	Example human error event tree	226
11.4	Example human time reliability correlation	229
11.5	Hypothetical lognormal density of HEPs	230
11.6	An ID for human error probabilities	236
12.1	Classification of software reliability models	244
12.2	A u -plot	252
12.3	Cumulative times until failure	254
12.4	Expected number of failures as function of time using LV model	255
12.5	The u -plot	256
13.1	The decision tree for the research project	263
13.2	The decision tree for the extended research proposal	265
13.3	Simple attribute hierarchy	270
13.4	The construction of a marginal value function	273
13.5	Indifference curves for cost and delay	276
13.6	Indifference curves for cost and performance given delay = 5	276
13.7	The trade-off between cost and performance	278
14.1	A simple belief net	286
14.2	Alarm influence diagram	292
14.3	A Bayesian belief net and the corresponding moral graph	294
14.4	An influence diagram for fire risk	298
15.1	A simple network	303

15.2	Determining the critical path	303
15.3	Form of the loss function for overspending	306
15.4	Program standard offer	308
15.5	Program alternative offer	309
15.6	Triangular distribution	312
15.7	Distribution of project duration	313
15.8	Distribution of project duration, with new option	314
16.1	Box model for soil migration	319
16.2	Marginal distributions for the target variables	324
17.1	The diagonal band distribution with parameter α	331
17.2	A dependence tree	333
17.3	Partial correlation vine	338
17.4	Rank correlation tree for power lines, Case 2	339
17.5	Rank correlation tree for power lines, Case 3	339
17.6	Distributions for powerline system failure probability	340
17.7	Distribution for series system lifetime	341
17.8	Mean series system lifetime, depending on rank correlation	341
17.9	Mean parallel system lifetime, depending on rank correlation	342
17.10	Unconditional cobweb plot	343
17.11	Conditional cobweb plot: high concentration at 0.5 km downwind	344
17.12	Conditional cobweb plot: mid-range concentration at 0.5 km downwind	345
17.13	Conditional cobweb plot: low concentration at 0.5 km downwind	346
18.1	Frequency consequence lines	356
18.2	The Dutch group risk criterion	357
18.3	Unacceptable risks	358
18.4	Equally risky activities	360
18.5	Changes in numbers of deaths of motor cyclists in different US states	366

Tables

5.1	Swedish nuclear power plant data failure fields	84
5.2	A small mortality table for failure data	87
5.3	Median ranks	88
5.4	A small mortality table with median rank estimates	88
5.5	Failure times and suspensions	89
5.6	Revised median rank estimates, with suspensions	90
5.7	Kaplan–Meier estimates	92
5.8	Extreme value distributions	96
6.1	Laws of Boolean algebra	113
7.1	Truth table for Example 7.2	125
7.2	Truth table for Example 7.3	126
7.3	The p-cut calculation for the electrical power system	135
7.4	Comparison of fault tree size and BDD size for various test cases	135
7.5	FV importance of basic events	137
7.6	Approximate conditional probability of basic events given failure of Component 2 and T	138
8.1	Generic causes of dependent component failures	144
8.2	Some β -factors	148
9.1	Maintenance jobs and schedules	157
9.2	Maintenance and failure type	158
9.3	Component socket time histories, 314 pressure relief valves	160
10.1	Expert 1 data	212
10.2	Expert 3 data	212
10.3	Expert 4 data	213
10.4	Expert 5 data	213
10.5	Expert 8 data	214
10.6	Global weights for the five experts	216
10.7	Equal weights for the five experts	216
11.1	Some generic HEPs used in WASH-1400	219
11.2	Stages in a human reliability analysis	221
11.3	Failure modes for the three performance levels	224

11.4	HEP modification factors, Table 20-16 from [Swain and Guttman, 1983]	227
11.5	Levels of dependency	228
11.6	Typical values of the distribution	235
11.7	Marginal and conditional probabilities for the ID in Figure 11.6	237
14.1	Conditional probability tables	297
15.1	An example Project Uncertainty Matrix	301
15.2	Criticality indices for activities	313
16.1	Quantile information for elicitation variables at various downwind distances	323
16.2	Product moment correlation matrix for target variables	325
16.3	Rank correlation matrix for target variables	325
17.1	Moments and quantiles for uncertainty distribution	340
18.1	Annual risk of death in the United States	352
18.2	Loss of life expectancy	352
18.3	Hourly specific mortality rates	354
18.4	Deaths per 10^9 km traveled	355
18.5	Risk goals for various technologies	363
18.6	Median costs of life-saving measures per sector	364

Part I

Introduction

Probabilistic risk analysis

Probabilistic risk analysis (PRA), also called quantitative risk analysis (QRA) or probabilistic safety analysis (PSA), is currently being widely applied to many sectors, including transport, construction, energy, chemical processing, aerospace, the military, and even to project planning and financial management. In many of these areas PRA techniques have been adopted as part of the regulatory framework by relevant authorities. In other areas the analytic PRA methodology is increasingly applied to validate claims for safety or to demonstrate the need for further improvement. The trend in all areas is for PRA to support tools for management decision making, forming the new area of *risk management*.

Since PRA tools are becoming ever more widely applied, and are growing in sophistication, one of the aims of this book is to introduce the reader to the main tools used in PRA, and in particular to some of the more recent developments in PRA modeling. Another important aim, though, is to give the reader a good understanding of uncertainty and the extent to which it can be modeled mathematically by using probability. We believe that it is of critical importance not just to understand the mechanics of the techniques involved in PRA, but also to understand the foundations of the subject in order to judge the limitations of the various techniques available. The most important part of the foundations is the study of uncertainty. What do we mean by uncertainty? How might we quantify it?

After the current introductory chapter, in Part two we discuss theoretical issues such as the notion of uncertainty and the basic tools of probability and statistics that are widely used in PRA. Part three presents basic modeling tools for engineering systems, and discusses some of the techniques available to quantify uncertainties (both on the basis of reliability data, and using expert judgement). In Part four we discuss uncertainty modeling and risk measurement. The aim is to show how dependent uncertainties are important

and can be modeled, how value judgements can be combined with uncertainties to make optimal decisions under uncertainty, and how uncertainties and risks can be presented and measured.

1.1 Historical overview

This introductory section reviews the recent history of these developments, focusing in particular on the aerospace, nuclear and chemical process sectors.

1.1.1 The aerospace sector

A systematic concern with risk assessment methodology began in the aerospace sector following the fire of the Apollo test AS-204 on January 27, 1967, in which three astronauts were killed. This one event set the National Aeronautics and Space Administration (NASA) back 18 months, involved considerable loss of public support, cost NASA salaries and expenses for 1500 people involved in the subsequent investigation, and ran up \$410 million in additional costs [Wiggins, 1985]. Prior to the Apollo accident, NASA relied on its contractors to apply 'good engineering practices' to provide quality assurance and quality control.

On April 5, 1969 the Space Shuttle Task Group was formed in the Office of Manned Space Flight of NASA. The task group developed 'suggested criteria' for evaluating the safety policy of the shuttle program which contained quantitative safety goals. The probability of mission completion was to be at least 95% and the probability of death or injury per mission was not to exceed 1%. These numerical safety goals were not adopted in the subsequent shuttle program.

The reason for rejecting quantitative safety goals given at the time was that low numerical assessments of accident probability could not guarantee safety: '... the problem with quantifying risk assessment is that when managers are given numbers, the numbers are treated as absolute judgments, regardless of warnings against doing so. These numbers are then taken as fact, instead of what they really are: subjective evaluations of hazard level and probability.' ([Wiggins, 1985], p. 85).

An extensive review of the NASA safety policy following the Challenger accident of January 28, 1986 brought many interesting facts to light. A quantitative risk study commissioned by the US Air Force in 1983 estimated the Challenger's solid rocket booster failure probability per launch as 1 in 35. NASA management rejected this estimate and elected to rely on

their own engineering judgment, which led to a figure of 1 in 100.000 [Colglazier and Weatherwas, 1986]

It has also become clear that distrust of reassuring risk numbers was not the reason that quantitative risk assessment was abandoned. Rather, initial estimates of catastrophic failure probabilities were so high that their publication would have threatened the political viability of the entire space program. For example, a General Electric ‘full numerical probabilistic risk assessment’ on the likelihood of successfully landing a man on the moon indicated that the chance of *success* was ‘less than 5%’. When the NASA administrator was shown these results, he ‘felt that the numbers could do irreparable harm, and disbanded the effort’ [Bell and Esch, 1989].

By contrast, a congressional report on the causes of the Shuttle accident (quoted in [Garrick, 1989]) concluded that the qualitative method of simply identifying failures leading to loss of vehicle accidents (the so-called *critical items*) was limited because not all elements posed an equal threat. Without a means of identifying the *probability* of failure of the various elements NASA could not focus its attention and resources effectively.

Since the shuttle accident, NASA has instituted programs of quantitative risk analysis to support safety during the design and operations phases of manned space travel. The NASA risk assessment effort reached a high point with the publication of the SAIC Shuttle Risk Assessment [Fragola, 1995]. With this assessment in hand, NASA was able to convince the US Congress that the money spent on shuttle development since the Challenger accident had been well used, even though no failure paths had been eliminated. The report showed that the *probability* of the most likely failure causes had been significantly reduced.

The European space program received a setback with the failure of the maiden flight of Ariane 5. A board of inquiry [ESA, 1997] revealed that the disaster was caused by software errors and the management of the software design. The accident demonstrates the problem of integrating working technologies from different environments into a new reliable system.

1.1.2 The nuclear sector

Throughout the 1950s, following Eisenhower’s ‘Atoms for Peace’ program, the American Atomic Energy Commission (AEC) pursued a philosophy of risk assessment based on the ‘maximum credible accident’. Because ‘credible accidents’ were covered by plant design, residual risk was estimated by studying the hypothetical consequences of ‘incredible accidents’. An early study released in 1957 focused on three scenarios of radioactive releases

from a 200 megawatt nuclear power plant operating 30 miles from a large population center. Regarding the probability of such releases the study concluded that ‘no one knows now or will ever know the exact magnitude of this low probability’.

Successive design improvements were intended to reduce the probability of a catastrophic release of the reactor core inventory. Such improvements could have no visible impact on the risk as studied with the above methods. On the other hand, plans were being drawn for reactors in the 1000 megawatt range located close to population centers, and these developments would certainly have a negative impact on the consequences of the ‘incredible accident’.

The desire to quantify and evaluate the effects of these improvements led to the introduction of *probabilistic* risk analysis. As mentioned above, the basic methods of probabilistic risk assessment originated in the aerospace program in the 1960s. The first full scale application of these methods, including an extensive analysis of the accident consequences, was undertaken in the *Reactor Safety Study* WASH-1400 [NRC, 1975] published by the US Nuclear Regulatory Commission (NRC). This study is rightly considered to be the first modern PRA.

The reception of the *Reactor Safety Study* in the scientific community may best be described as turbulent. The American Physical Society [APS, 1975] conducted an extensive review of the first draft of the *Reactor Safety Study*. In the accompanying letter attached to their report, physicists Wolfgang Panofsky, Victor Weisskopf and Hans Bethe concluded, among other things, that the calculation methods were ‘fairly unsatisfactory’, that the emergency core cooling system is unpredictable and that relevant physical processes ‘which could interfere with its functioning have not been adequately analyzed’, and that ‘the consequences of an accident involving major radioactive release have been underestimated as to casualties by an order of magnitude’. The final draft of the *Reactor Safety Study* was extensively reviewed by, among others, the Environmental Protection Agency [EPA, 1976] and the Union of Concerned Scientists [Union of Concerned Scientists, 1977].

In 1977 the United States Congress passed a bill creating a special ‘review panel’ of external reactor safety experts to review the ‘achievements and limitations’ of the *Reactor Safety Study*. The panel was led by Prof. Harold Lewis, and their report is known as the ‘Lewis Report’ [Lewis *et al.*, 1979]. While the Lewis Report recognized the basic validity of the PRA methodology and expressed appreciation for the pioneering effort put into the *Reactor Safety Study*, they also uncovered many deficiencies in the treatment of probabilities. They were led to conclude that the uncertainty bands claimed for the conclusions in the *Reactor Safety Study* were ‘greatly understated’.

Significantly, the Lewis Report specifically endorsed the use of subjective probabilities in the *Reactor Safety Study*.

In January 1979 the NRC distanced itself from the results of the *Reactor Safety Study*: ‘In particular, in light of the Review Group conclusions on accident probabilities, the Commission does not regard as reliable the *Reactor Safety Study*’s numerical estimate of the overall risk of a reactor accident.’ [NRC, 1979]

The future of PRA after the NRC’s announcement of 1979 did not look bright. However, the dramatic events of March 1979 served to change that. In March 1979 the Three Mile Island – 2 (TMI) Nuclear Generating Unit suffered a severe core damage accident. Subsequent study of the accident revealed that the accident sequence had been predicted by the *Reactor Safety Study*. The probabilities associated with that sequence, particularly those concerning human error, do not appear realistic in hindsight.

Two influential independent analyses of the TMI accident, the Report of the President’s Commission on the Accident at Three Mile Island [Kemeny *et al*, 1979] and the Rogovin Report [Rogovin and Frampton, 1980], credited the *Reactor Safety Study* with identifying the small loss-of-coolant accidents as the major threat to safety, and recommended that greater use should be made of probabilistic analyses in assessing nuclear plant risks. They also questioned whether the NRC was capable of regulating the risks of nuclear energy, and recommended that the regulatory body be massively overhauled (which recommendation was not carried out).

Shortly thereafter a new generation of PRAs appeared in which some of the methodological defects of the *Reactor Safety Study* were avoided. The US NRC released *The Fault Tree Handbook* [Vesely *et al.*, 1981] in 1981 and the *PRA Procedures Guide* [NRC, 1983] in 1983 which shored up and standardized much of the risk assessment methodology. Garrick’s review [Garrick, 1984] of PRAs conducted in the aftermath of the Lewis report discussed the main contributors to accident probability identified at the plants. He also noted the necessity to model uncertainties properly in order to use PRA as a management tool, and suggested the use of on-line computer PRA models to guide plant management (a process now called a ‘living PRA’).

The accident at the Chernobyl Nuclear Power Plant occurred on April 26, 1986. A test was carried out in order to determine how long the reactor coolant pumps could be operated using electrical power from the reactors’ own turbine generator under certain abnormal conditions. At the beginning of the test some of the main coolant pumps slowed down, causing a reduction of coolant in the core. The coolant left began to boil, adding reactivity to

the core (due to the so-called positive void coefficient of the RBMK reactor type). This caused a sudden increase in power which could not be controlled because the control systems worked too slowly. The power surge caused the fuel to overheat and disintegrate. Pieces of fuel ejected into the coolant then caused a steam explosion whose force blew the cover off the reactor. There were 31 early deaths and (amongst other radiological effects) a 'real and significant' increase in childhood carcinoma of the thyroid [OECD, 1996]. Thousands of people have been displaced and blame the reactor accident for all sorts of health problems.

The management of western nuclear power corporations moved quickly to assure the public that this type of accident could not occur in the US and western Europe because of the difference in reactor design. The Three Mile Island and Chernobyl accidents, in addition to regular publicity about minor leaks of radioactive material from other power stations and processing plants, however, have fostered a climate of distrust in nuclear power and in the capacity of management to run power stations properly.

Besides technical advances in the methodology of risk analyses, the 1980s and 1990s have seen the further development of numerical safety goals. Examples are the USNRC policy statement of 1986 [NRC, 1986] and the UK *Tolerability of risk* document [HSE, 1987]. These documents seek to place the ALARP principle ('as low as reasonably possible') into a numerical framework by defining upper levels of intolerable risk and lower levels of broadly tolerable risk.

1.1.3 The chemical process sector

In the process sector, government authorities became interested in the use of probabilistic risk analysis as a tool for estimating public exposure to risk in the context of licensing and citing decisions. Important European efforts in this direction include two studies of refineries on Canvey Island ([HSE, 1978], [HSE, 1981]) in the UK, a German sulphuric acid plant study [Jäger, 1983], and the Dutch LPG and COVO studies ([TNO, 1983], [COVO, 1982]). The COVO study [COVO, 1982] was a risk analysis of six potentially hazardous objects in the Rijnmond area. The group which performed the study later formed the consulting firm Technica, which has since played a leading role in risk analysis.

The impetus for much of this work was the Post-Seveso Directive [EEC, 1982] adopted by the European Community following the accidental release of dioxin by a chemical plant near Seveso, Italy. The directive institutes a policy of risk management for chemical industries handling hazardous

materials in which each member state has the responsibility for developing its own risk management methodology. The Dutch government took the lead in requiring quantitative risk analyses of potentially hazardous objects, and has invested heavily in developing tools and methods for implementing this policy. This lead has been followed by several other member countries.

Dutch legislation requires the operator of a facility dealing with hazardous substances to submit an 'External Safety Report' (Externe Veiligheid Rapport, EVR). About 70 companies in the Netherlands fall under this reporting requirement. EVRs are to be updated every 5 years.

The quantitative risk analysis required in EVRs may be broken down into four parts. The first part identifies the undesirable events which may lead to a threat to the general public. The second part consists of an effect and damage assessment of the undesired events. The third part calculates the probability of damage, consisting of the probability of an undesired release of hazardous substances, and the probability of propagation through the environment causing death. The fourth part determines the individual and group risk associated with the installation.

For new installations, the risk of death of an 'average individual' exposed at any point outside the installation perimeter for an entire year must not exceed 10^{-6} . The group risk requirement stipulates that the probability of 10^n or more fatalities ($n > 1$) must not exceed 10^{-3-2n} per year. If this probability exceeds 10^{-5-2n} per year then further reduction is required.

Risk based regulation is now common in many different sectors. An overview of some of the risk goals currently set is given in Table 18.5.

1.1.4 The less recent past

We have concentrated on the developments in a few important sectors since the end of the second world war. The reader interested in looking further into the past is referred to [Covello and Mumpower, 1985] which starts about 3200 BC, and [Bernstein, 1996].

1.2 What is the definition of risk?

The literature on the subject of risk has grown rapidly in the last few years, and the word 'risk' is used in many different ways. The purpose of this section is to discuss briefly what we mean by risk, and in what way the concept can be described in a mathematical setting. The limitations of the mathematical approach to measuring risk will be highlighted in Chapter 18. Our discussion here is largely drawn from [Kaplan and Garrick, 1981].

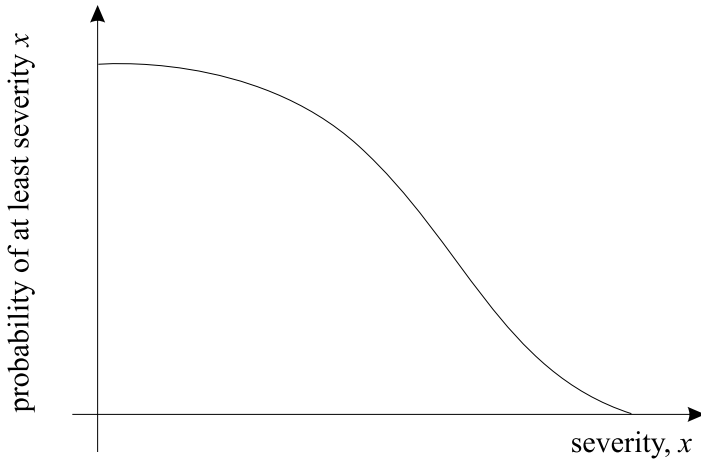


Fig. 1.1. Risk curve

A *hazard* is considered as a source of danger but the concept does not contain any notion of the likelihood with which that danger will actually impact on people or on the environment. We are often *uncertain* about whether or not a hazard will actually lead to negative consequences (that is, whether the potentiality will be converted into actuality). As will be argued in Chapter 2, that uncertainty can – in principle – be quantified by *probability*. The definition of *risk* combines both of the above elements. A risk analysis tries to answer the questions:

- (i) What can happen?
- (ii) How likely is it to happen?
- (iii) Given that it occurs, what are the consequences?

Kaplan and Garrick [Kaplan and Garrick, 1981] define risk to be a set of *scenarios* s_i , each of which has a *probability* p_i and a *consequence* x_i . If the scenarios are ordered in terms of increasing severity of the consequences then a risk curve can be plotted, for example as shown in Figure 1.1. The risk curve illustrates what is the probability of *at least* a certain number of casualties in a given year.

Kaplan and Garrick [Kaplan and Garrick, 1981] further refine the notion of risk in the following way. First, instead of talking about the probability of an event, they talk about the *frequency* with which such an event might take place. They then introduce the notion of uncertainty about the frequency (the ‘probability of a frequency’). This more sophisticated notion of risk will be discussed further in Chapter 2.

For the moment the reader should bear in mind that the basic method of risk analysis is the identification and quantification of scenarios, probabilities and consequences. The tools that will be described in this book are dedicated to these tasks.

1.3 Scope of probabilistic risk analyses

The goals and sizes of probabilistic risk analyses vary widely. The nuclear sector has made the largest commitments of resources in this area. Some of the larger chemical process studies have been of comparable magnitude, although the studies performed in connection with the Post-Seveso Directive tend to be much smaller. In the aerospace sector, the methods have not yet been fully integrated into the existing design and operations management structures, although the United Space Alliance (the consortium operating the space shuttle for NASA) is probably currently the furthest in an integrated risk management approach.

The *Procedures Guide* [NRC, 1983], gives a detailed description of the various levels of commitment of resources in nuclear PRAs, and we summarize this below, as the general format is applicable to other sectors as well. Three levels are distinguished:

- level 1, systems analysis;
- level 2, systems plus containment analysis;
- level 3, systems, containment and consequence analysis.

These are explained further below.

Level 1: systems analysis The systems analysis focuses on the potential release of hazardous substances and/or energy from the design envelope of the facility in question. In the case of a nuclear reactor, this concerns primarily the release of radioactive material from the reactor core. Phases within level 1 include event tree modeling, analysis of human reliability impacts, database development, accident sequence quantification, external event analysis and uncertainty analysis.

Level 2: containment analysis The containment analysis includes an analysis of pathways into the biosphere, and a transport analysis to determine important parameters such as composition of release, quantity of release, time profile of release, physics of release event (e.g. elevated or ground source, pressurized or ambient, etc.).

Level 3: consequence analysis Here the pathways by which the hazardous material can reach and affect man are identified, using an analysis of the dispersion through the atmosphere and groundwater, propagation through the food chain, and the toxicological effects in the human body, in both the short and long term. In addition the economic impact of land interdiction, clean-up, relocation etc. should be included.

1.4 Risk analysis resources

1.4.1 Important journals

The journal that best covers the area discussed in this book is *Reliability Engineering and System Safety*. There are several journals covering the mathematical theory of reliability such as *IEEE Transactions on Reliability* and *Microelectronics and Reliability*, and many (applied) statistics and OR journals that frequently publish papers on reliability: *Technometrics*, *Applied Statistics*, *Operations Research*, *Lifetime Data Analysis*, *Biometrika*, *The Scandinavian Journal of Statistics* etc. Papers on risk analysis are to be found in engineering journals and also in a number of interdisciplinary journals. Amongst the engineering journals are *Journal of Hazardous Materials* and *Safety Science*. Interdisciplinary journals covering risk analysis are *Risk Analysis*, *Risk: Health, Safety and Environment*, *The Journal of Risk Research* and *Risk, Decision and Policy*.

1.4.2 Handbooks

Important textbooks and handbooks in this area are: [Vesely *et al.*, 1981], [NRC, 1983], [Swain and Guttman, 1983], [Kumamoto and Henley, 1996], [CCPS, 1989], [O'Connor, 1994].

1.4.3 Professional organizations

The Society of Reliability Engineers (SRE) has branches in many countries, as does the IEEE Reliability Society. The International Association for Probabilistic Safety Assessment and Management (IAPSAM) is an international organization which organizes the PSAM conferences. The European Safety and Reliability Association, ESRA, is the European umbrella organization of national associations in the area of risk and reliability analysis and organizes the yearly ESREL conferences. The European Safety Reliability and Data Association, ESReDA, is another European organization with industrial members that organizes regular seminars. The Society for Risk Analysis and

the Risk Analysis and Policy Association are two US based interdisciplinary organizations.

1.4.4 Internet

The IEEE Reliability Society maintains an excellent website, with references to other sites, information about standards and much more. The URL is **<http://engine.ieee.org/society/rs/>**. Riskworld is a good source of information about risk analysis and can be found at **<http://www.riskworld.com/>**. The European Safety and Reliability Society maintains an up-to-date list of links at its site **<http://www.esra.be>**.