

Probabilistic Risk Analysis

Foundations and Methods

概率风险分析

Tim Bedford

Roger Cooke

CAMBRIDGE

世界图书出版公司

Probabilistic Risk Analysis: Foundations and Methods

Tim Bedford

*Delft University of Technology
and
University of Strathclyde*

Roger Cooke

Delft University of Technology



CAMBRIDGE
UNIVERSITY PRESS

世界图书出版公司

书 名: Probabilistic Risk Analysis: Foundations and Methods
作 者: T. Bedford, R. Cooke
中 译 名: 概率风险分析
出 版 者: 世界图书出版公司北京公司
印 刷 者: 北京世图印刷厂
发 行: 世界图书出版公司北京公司 (北京朝内大街 137 号 100010)
联系电话: 010-64015659, 64038347
电子信箱: kjsk@vip.sina.com
开 本: 24 印 张: 17.5
出版年代: 2003 年 9 月
书 号: 7-5062-5945-1 / O · 364
版权登记: 图字: 01-2003-5539
定 价: 78.00 元

世界图书出版公司北京公司已获得 Cambridge University Press 授权在中国大陆
独家重印发行。

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
10 Stamford Road, Oakleigh, VIC 3166, 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

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

This edition of *Probabilistic Risk Analysis* by T. Bedford and R.
Cooke is published by arrangement with the Syndicate of the Press
of University of Cambridge, Cambridge, England.

Licensed edition for sale in the People's Republic of China only.
Not for export elsewhere.

Probabilistic Risk Analysis: Foundations and Methods

Preface

We have written this book for numerate readers who have taken a first university course in probability and statistics, and who are interested in mastering the conceptual and mathematical foundations of probabilistic risk analysis. It has been developed from course notes used at Delft University of Technology. An MSc course on risk analysis is given there to mathematicians and students from various engineering faculties. A selection of topics, depending on the specific interests of the students, is made from the chapters in the book. The mathematical background required varies from topic to topic, but all relevant probability and statistics are contained in Chapters 3 and 4.

Probabilistic risk analysis differs from other areas of applied science because it attempts to model events that (almost) never occur. When such an event does occur then the underlying systems and organizations are often changed so that the event cannot occur in the same way again. Because of this, the probabilistic risk analyst must have a strong conceptual and mathematical background.

The first chapter surveys the history of risk analysis applications. Chapter 2 explains why probability is used to model uncertainty and why we adopt a subjective definition of probability in spite of its limitations. Chapters 3 and 4 provide the technical background in probability and statistics that is used in the rest of the book. The remaining chapters are more-or-less technically independent of each other, except that Chapter 7 must follow Chapter 6, and 14 should follow 13. The final chapter gives a broad overview of risk measurement problems and looks into the future of risk analysis.

Almost all the chapters are concluded with exercises. The answers to these exercises are not given in the book, but bona fide teachers who are using the book in conjunction with their courses may contact David Tranah (dtranah@cambridge.org) and ask for a PDF file with the solutions to the problems.

Acknowledgements

A large number of people, including many students of our course 'Risk Analysis', have given us comments on this book. Special thanks are due to Frank Phillipson, Mart Janssen, Frank Rabouw, Linda van Merrienboer, Eeke Mast, Gilbert Pothoff, Erwin van Iperen, Lucie Aarts, Mike Frank, Antoine Rauzy, Christian Pressyl, Joe Fragola, Floor Koornneef and co-authors of various chapters, Bernd Kraan, Jan Norstrøm and Lonneke Holierhoek.

Special thanks go of course to our families and friends for putting up with us during the preparation of this manuscript.

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