



LUCA FIORENTINI

BOW-TIE INDUSTRIAL RISK MANAGEMENT ACROSS SECTORS

A BARRIER-BASED APPROACH

WILEY

**Bow-Tie Industrial Risk
Management Across Sectors**

Bow-Tie Industrial Risk Management Across Sectors

A Barrier-Based Approach

Professor Luca Fiorentini

WILEY

This edition first published 2022
© 2022 John Wiley & Sons Ltd

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, except as permitted by law. Advice on how to obtain permission to reuse material from this title is available at <http://www.wiley.com/go/permissions>.

The right of Luca Fiorentini to be identified as the author of this work has been asserted in accordance with law.

Registered Office

John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA
John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, UK

Editorial Office

111 River Street, Hoboken, NJ 07030, USA

For details of our global editorial offices, customer services, and more information about Wiley products visit us at www.wiley.com.

Wiley also publishes its books in a variety of electronic formats and by print-on-demand. Some content that appears in standard print versions of this book may not be available in other formats.

Limit of Liability/Disclaimer of Warranty

While the publisher and authors have used their best efforts in preparing this work, they make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives, written sales materials or promotional statements for this work. The fact that an organization, website, or product is referred to in this work as a citation and/or potential source of further information does not mean that the publisher and authors endorse the information or services the organization, website, or product may provide or recommendations it may make. This work is sold with the understanding that the publisher is not engaged in rendering professional services. The advice and strategies contained herein may not be suitable for your situation. You should consult with a specialist where appropriate. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this work was written and when it is read. Neither the publisher nor authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

Library of Congress Cataloging-in-Publication Data

Name: Fiorentini, Luca, 1976– author.

Title: Bow-tie industrial risk management across sectors : a barrier based approach / Professor Luca Fiorentini.

Description: First edition. | Hoboken, NJ : Wiley, 2022. | Includes bibliographical references and index. | Summary: "As stated by ISO 31000 "organizations of all types and sizes face internal and external factors and influences that make it uncertain whether and when they will achieve their objectives. The effect this uncertainty has on organization's objectives is a risk. All activities of an organization involve risk". ISO, together with the International Trade Centre and the United Nations Industrial Development Organization published a specific guide about the importance of the implementation of sound risk management practices in small and mid enterprises. Risk management is an integral part of all organizational processes and of decision making. It should be systematic, structured and timely. It also should be based on the best available information and tailored. It should consider human and cultural factors ("soft" factors) together with technical and organizational factors ("hard" factors)." – Provided by publisher.

Identifiers: LCCN 2021003284 (print) | LCCN 2021003285 (ebook) | ISBN 9781119523833 (hardback) | ISBN 9781119523826 (adobe pdf) | ISBN 9781119523673 (epub) | ISBN 9781119523857 (obook)

Subjects: LCSH: Risk management.

Classification: LCC HD61 .F49 2022 (print) | LCC HD61 (ebook) | DDC 658.15/5–dc23

LC record available at <https://lcn.loc.gov/2021003284>

LC ebook record available at <https://lcn.loc.gov/2021003285>

Cover Design: Wiley

Cover Image: © Nikolay_Popov/iStockphoto

Set in 9.5/12.5pt STIXTwoText by SPi Global, Pondicherry, India

*To my wife Sonia, with whom, day by day and together, I always reach new important goals.
Thank you for your support, patience and constant love, witnessed by the wonderful family
we have.*

Luca Fiorentini

Contents

List of Figures	<i>ix</i>
List of Tables	<i>xvii</i>
List of Acronyms	<i>xix</i>
Preface 1	<i>xxi</i>
	<i>Riccardo Ghini</i>
Preface 2	<i>xxiii</i>
	<i>Bernardino Chiaia</i>
Preface 3	<i>xxiv</i>
	<i>Luca Marmo</i>
Preface 4	<i>xxvi</i>
	<i>Giuseppe Conti</i>
Preface 5	<i>xxvii</i>
	<i>Claudio De Angelis</i>
Preface 6	<i>xxx</i>
	<i>Damiano Tranquilli</i>
Preface 7	<i>xxxiii</i>
	<i>Enzo Matticoli</i>
Preface 8	<i>xxxiv</i>
	<i>Salvatore Bagnato</i>
Author Preface	<i>xxxvii</i>
Acknowledgements	<i>xxxix</i>

1	Introduction to Risk and Risk Management	1
1.1	Risk Is Everywhere, and Risk Management Became a Critical Issue in Several Sectors	6
1.2	ISO 31000 Standard	10
1.3	ISO 31000 Risk Management Workflow	23
1.4	Uncertainty and the Human Factor	53
1.5	Enterprise Complexity and (Advanced) Risk Management (ERM)	58
1.6	Proactive and Reactive Culture of Organizations Dealing with Risk Management	62
1.7	A Systems Approach to Risk Management	76

2	Bow-Tie Model	101
2.1	Hazards and Risks	101
2.2	Methods of Risk Management	102
2.3	The Bow-Tie Method	134
2.4	The Bow-Tie Method and the Risk Management Workflow from ISO 31000	138
2.5	Application of Bow-Ties	140
2.6	Level of Abstraction	147
2.7	Building a Bow-Tie	150
2.8	Hazards	152
2.9	Top Events	153
2.10	Threats	154
2.11	Consequences	156
2.12	Barriers	156
2.13	Escalation Factors and Associated Barriers	163
2.14	Layer of Protection Analysis (LOPA): A Quantified Bow-Tie to Measure Risks	165
2.15	Bow-Tie as a Quantitative Method to Measure Risks and Develop a Dynamic Quantified Risk Register	178
2.16	Advanced Bow-Ties: Chaining and Combination	183
3	Barrier Failure Analysis	185
3.1	Accidents, Near-Misses, and Non-Conformities in Risk Management	185
3.2	The Importance of Operational Experience	186
3.3	Principles of Accident Investigation	189
3.4	The Barrier Failure Analysis (BFA)	194
3.5	From Root Cause Analysis (RCA) to BFA	208
3.6	BFA from Bow-Ties	213
4	Workflows and Case Studies	217
4.1	Bow-Tie Construction Workflow with a Step-by-Step Guide	217
4.2	LOPA Construction Workflow with a Step-by-Step Guide	243
4.3	BFA Construction Workflow with a Step-by-Step Guide	250
4.4	Worked Examples	265
	Conclusions	365
	Appendix 1 Bow-Tie Easy Guide	371
	Appendix 2 BFA Easy Guide	373
	Appendix 3 Human Error and Reliability Assessment (HRA)	379
	References and Further Reading	409
	Index	417

List of Figures

- Figure 1** Descent from Col du Chardonnet. Is it safe? *Source:* Luca Marmo archive photo. *xxiv*
- Figure 2** Bas-relief depicting the god Kairos. *xxvii*
- Figure 3** The epistemological meaning of security. *xxviii*
- Figure 4** Swiss Cheese Model. *Source:* Reason, J., 1990. *5*
- Figure 5** Top five global risks in terms of likelihood (2007–2020). *Source:* World Economic Forum, 2020. *8*
- Figure 6** Top five global risks in terms of impact (2007–2020). *Source:* World Economic Forum, 2020. *9*
- Figure 7** Different perspectives on risk. *11*
- Figure 8** Definition of the scope of risk management. *12*
- Figure 9** Relationship between principles, framework, and risk management process. *13*
- Figure 10** The principles of RM according to ISO 31000. *15*
- Figure 11** The RM framework. *19*
- Figure 12** Components of a risk management framework. *20*
- Figure 13** Risk management framework. *23*
- Figure 14** Leadership and commitment. *24*
- Figure 15** Internal and external context. *25*
- Figure 16** Identify the requirements related to risk management. *26*
- Figure 17** Implementing the risk management framework. *27*
- Figure 18** Scheme of the risk management process according to ISO 31000. *28*
- Figure 19** Relationship between the RM principles, framework, and process. *29*
- Figure 20** Improving the risk management framework. *30*
- Figure 21** The risk assessment phase in the context of the RM process. *31*
- Figure 22** Level of risk. *34*
- Figure 23** Frequency analysis and probability estimation. *37*
- Figure 24** Risk acceptability and tolerability thresholds. *39*
- Figure 25** Example of a risk matrix with level of acceptability regions. *40*
- Figure 26** Prioritization of risk given impact and likelihood. *41*
- Figure 27** Risk prioritization and the risk matrix. *42*
- Figure 28** Matrix example for qualitative ALARP analysis. *43*

- Figure 29** Achieving balance in risk reduction. 44
- Figure 30** Risk treatment activities. 46
- Figure 31** Residual risk. 47
- Figure 32** Risk management process continuous improvement. 49
- Figure 33** Documenting the risk management process. 50
- Figure 34** Skills and knowledge for a risk manager. 50
- Figure 35** Resources to be allocated for an effective RM. 51
- Figure 36** Understand the mission, objectives, values, and strategies. 51
- Figure 37** Risk control hierarchy and in practice. 52
- Figure 38** Thinking-Behavior-Result model. *Source:* Adapted from Fiorentini and Marmo (2018). 54
- Figure 39** Stimulus-Response model. *Source:* Adapted from Fiorentini and Marmo (2018). 55
- Figure 40** Two-pointed model. *Source:* Adapted from Fiorentini and Marmo (2018). 55
- Figure 41** Inverted two-pointed model. *Source:* Adapted from Fiorentini and Marmo (2018). 56
- Figure 42** Human factors in process plant operation. *Source:* Adapted from Strobhar (2013). 57
- Figure 43** The principles of RM according to ISO 31000. 59
- Figure 44** Main types of business risks. 62
- Figure 45** Most common enterprise risks. 63
- Figure 46** Culture maturity level in an organization. 64
- Figure 47** Safety culture levels. 66
- Figure 48** Quality of risk management approach. 68
- Figure 49** The pathological condition. 69
- Figure 50** The reactive condition. 71
- Figure 51** The bureaucratic condition. 72
- Figure 52** The proactive condition. 74
- Figure 53** The generative condition. 75
- Figure 54** The Deming Cycle PDCA. 77
- Figure 55** Swiss Cheese Model applied to a major industrial event. 88
- Figure 56** Maturity model. *Source:* Courtesy of EXIDA L.C.C. (USA). 90
- Figure 57** Feed line propane-butane separation column. *Source:* Adapted from Assael and Kakosimos (2010). 108
- Figure 58** Basic structure of a fault tree (horizontal). 117
- Figure 59** Basic structure of a fault tree (vertical). 118
- Figure 60** Basic Events. 118
- Figure 61** Example of the fault tree, taking inspiration from the Åsta railway incident. *Source:* Sklet, S., 2002. 119
- Figure 62** Gates. 120
- Figure 63** Fire triangle using FTA. 120
- Figure 64** Flammable liquid storage system. *Source:* Modified from Assael, M. and Kakosimos, K., 2010. 121
- Figure 65** Example of FTA for a flammable liquid storage system. 122

- Figure 66** Fault tree example. 123
- Figure 67** The structure of a typical ETA diagram. 124
- Figure 68** Event tree analysis for the Åsta railway accident. 125
- Figure 69** Pipe connected to a vessel. 126
- Figure 70** Example of event tree for the pipe rupture. 126
- Figure 71** Bow-Tie diagram structure. 127
- Figure 72** F-N Curve. 129
- Figure 73** Example of a risk matrix with acceptability regions. 130
- Figure 74** Calibrated risk graph. 131
- Figure 75** A typical Bow-Tie. 135
- Figure 76** Bow-Tie as the combination of an FTA and an ETA. 136
- Figure 77** The Swiss Cheese Model by James Reason. 137
- Figure 78** Bow-Tie project risk assessment. 140
- Figure 79** Bow-Tie diagram – transfer of a data center. 141
- Figure 80** Bow-Tie diagram on virtual classroom training. 146
- Figure 81** Level of abstraction. 147
- Figure 82** Zoom level and point in time. 148
- Figure 83** Example of point in time. 149
- Figure 84** Basic elements of a Bow-Tie diagram. 151
- Figure 85** Determining the threshold level to cause the top event. 155
- Figure 86** Barrier functions. 157
- Figure 87** Location of elimination and prevention barriers. 158
- Figure 88** Location of control and mitigation barriers. 158
- Figure 89** Barrier systems. 159
- Figure 90** Using the same barrier on either side of the Bow-Tie diagram. 160
- Figure 91** Classification of safety barriers. *Source:* Sklet, S., 2006. 162
- Figure 92** Barrier classification promoted by the AIChE CCPS Guidelines. 163
- Figure 93** The energy model. *Source:* Haddon, W., 1980. 164
- Figure 94** Generic safety functions related to a process model. *Sources:* Hollnagel, E., 2004. Barrier And Accident Prevention. Hampshire, UK: Ashgate; Duijm et al., 2004. 164
- Figure 95** Layers of defence against a possible industrial accident. 166
- Figure 96** A comparison between ETA and LOPA's methodology. 167
- Figure 97** Actions of a barrier. 172
- Figure 98** Misuse of escalation factors, with nested structure. 174
- Figure 99** Defining “activities” for a barrier. 175
- Figure 100** Quantifying a simplified Bow-Tie. 181
- Figure 101** Scale of the effectiveness of a barrier and the relationship between effectiveness and PFD (correct). 183
- Figure 102** Relationship between effectiveness and PFD (correct). 183
- Figure 103** Bow-Tie concatenation example. 184
- Figure 104** Difference between accident, near-accident and unintended circumstance. 186
- Figure 105** Principles of incident analysis. 187
- Figure 106** The importance of accident investigations. 188

- Figure 107** Steps in the analysis of the operational experience of organizations. 188
- Figure 108** Steps in accident investigations. 190
- Figure 109** The pyramid of conclusions. 192
- Figure 110** Example a Tripod Beta diagram. 193
- Figure 111** Possible Tripod Beta appearances. 194
- Figure 112** Example of a BFA diagram 1. 197
- Figure 113** Example of a BFA diagram 2. 198
- Figure 114** BFA core elements. 199
- Figure 115** General structure of a BFA diagram. 200
- Figure 116** Event chaining in BFA. 200
- Figure 117** Defeated barriers are not BFA events. 200
- Figure 118** Barrier identification in BFA. 201
- Figure 119** Correct and incorrect barrier identification in BFA. 201
- Figure 120** BFA analysis. 201
- Figure 121** Events types in a BFA diagram. 202
- Figure 122** Example of timeline developed for the *Norman Atlantic* investigation. 204
- Figure 123** Timeline example. 206
- Figure 124** The onion-like structure between immediate causes and root causes. 207
- Figure 125** Benefit of RCA. 208
- Figure 126** RCA Process. 209
- Figure 127** Levels of analysis. 211
- Figure 128** The Bow-Tie diagram. 213
- Figure 129** Bow-Tie risk assessment and incident analysis. 215
- Figure 130** Bow-Tie preparation workflow. 218
- Figure 131** From organization to critical tasks. 233
- Figure 132** Example of Barrier Criticality Assessment. 235
- Figure 133** Steps to identify critical barriers. 236
- Figure 134** Example of a barrier audit. 238
- Figure 135** Traditional audit: one element of the management system is analyzed at a time. 240
- Figure 136** Audit barrier-based: all elements of the management system identified as relevant to a specific barrier are analyzed. 240
- Figure 137** General workflow of LOPA. 244
- Figure 138** The general workflow of a survey. 250
- Figure 139** Incident barrier states and relation between barrier state and barrier lifecycle. 258
- Figure 140** Recommendations development and review. 264
- Figure 141** On the left: pier with a damaged downpipe; the concrete is wet and deteriorated. On the right: a similar pier with a safe downpipe; the concrete is in good condition. 267
- Figure 142** Effects of ageing and humidity on the concrete. The reinforcement bars are corroded and there are signs of rust on the beams. 268
- Figure 143** Concrete spalling on a Gerber support with a consequent capacity reduction. The cause of the damage has to be searched for on a damaged downpipe on the road joint (recently substituted). 268

- Figure 144** The spalling of concrete caused the corrosion to progress. The reinforcement bars broken due to the limited cross-section are causing a reduction of the capacity of the girder. 269
- Figure 145** Bow-Tie diagram for “Local reduction of the resisting capacity of a bridge due to ageing”. 270
- Figure 146** Employee infected with COVID-19 virus. 271
- Figure 147** Fire in flight. 272
- Figure 148** BFA on food contamination (near miss). 273
- Figure 149** Web-based software development – Bow-Tie. 274
- Figure 150** IT systems protection Bow-Tie. 280
- Figure 151** Satellite view of Matera. 283
- Figure 152** Matera – Piazza Vittorio Veneto. On the right: steps. *Source:* Google LLC. 284
- Figure 153** Developed Bow-Tie to assess crowding-related risks – zooming the threats and preventive barriers. 285
- Figure 154** Developed Bow-Tie to assess crowding-related risks – zooming the consequences and mitigative barriers. 286
- Figure 155** Map to develop simulated scenarios. 287
- Figure 156** Different levels of service. 287
- Figure 157** Piazza Vittorio Veneto and the bottleneck in Via San Biagio, Matera. 288
- Figure 158** Impact of the soft obstacles on the pedestrian flow. 289
- Figure 159** Bow-Tie Risk assessment (whole picture). 290
- Figure 160** Helicopter loss of control Bow-Tie risk assessment. 291
- Figure 161** Treatment of critically ill patients. 292
- Figure 162** Treatment of patient with pain. 293
- Figure 163** Preparing parenterals (excluding cytostatic drugs). 294
- Figure 164** Administration of parenterals (excluding cytostatic drugs). 295
- Figure 165** Medication verification in handoff during hospital admission. 296
- Figure 166** Medication verification in handoff during hospital discharge (1 of 2). 296
- Figure 167** Medication verification in handoff during hospital discharge (2 of 2). 297
- Figure 168** Administration of medicines. 298
- Figure 169** Treatment of patients with acute coronary syndrome. 299
- Figure 170** Administering intravascular iodinated contrast media (excluding intensive care patients). 300
- Figure 171** Applying a central venous catheter (CVC). 301
- Figure 172** Operating on a patient. 302
- Figure 173** Hospitalization of vulnerable elders (> 70 years) (1 of 4). 303
- Figure 174** Hospitalization of vulnerable elders (> 70 years) (2 of 4). 304
- Figure 175** Hospitalization of vulnerable elders (> 70 years) (3 of 4). 305
- Figure 176** Hospitalization of vulnerable elders (> 70 years) (4 of 4). 306
- Figure 177** Performing surgical procedures. 307
- Figure 178** Elaboration of the threat “external corrosion” and main escalating factors and controls. 308

- Figure 179** Link between controls and the company HSE management system procedures. 309
- Figure 180** BFA of Flixborough (UK) incident. 310
- Figure 181** BFA of Seveso (Italy) incident. 311
- Figure 182** BFA of Bhopal (India) incident. 312
- Figure 183** BFA of *Piper Alpha* (UK – offshore) incident. 313
- Figure 184** BFA of Pembroke Refinery (Milford Haven) (UK) incident. 314
- Figure 185** BFA of Texas City (US) incident. 315
- Figure 186** BFA of Macondo (*Deepwater Horizon*) (US – Offshore) incident. 316
- Figure 187** BFA of Fukushima (Daiichi) (Japan) incident. 317
- Figure 188** Drug administration Bow-Tie. 318
- Figure 189** Area involved in the accident. Right, unwinding section of the line, left, the front wall impinged by flames. *Source:* Taken from Marmo, Piccinini and Fiorentini, 2013. 320
- Figure 190** The flattener and the area involved in the accident. Details of the area struck by the jet fire, view from the front wall. *Source:* Taken from Marmo, Piccinini and Fiorentini, 2013. 320
- Figure 191** Details of the hydraulic pipe that provoked the flash fire. *Source:* Taken from Marmo, Piccinini and Fiorentini, 2013. 321
- Figure 192** Map of the area struck by the jet fire and by the consequent fire. The dots represent the presumed position of the workers at the moment the jet was released. *Source:* Marmo, Piccinini and Fiorentini, 2013. 322
- Figure 193** Footprint of the jet fire on the front wall. *Source:* Marmo, Piccinini and Fiorentini, 2013. 322
- Figure 194** Timescale of the accident. F1 is the time interval in which the ignition occurred. F2 is the time interval in which it is probable that the workers noticed the fire. The group 5 and group 6 events are defined as in Table 28. *Source:* Marmo, Piccinini and Fiorentini, 2013. 323
- Figure 195** The domain used in the FDS fire simulations. *Source:* Marmo, Piccinini and Fiorentini, 2013. 326
- Figure 196** Simulated area, elevation. *Source:* Marmo, Piccinini and Fiorentini, 2013. 326
- Figure 197** Jet fire simulation results: flames at 1 s from pipe collapse. *Source:* Marmo, Piccinini and Fiorentini, 2013. 328
- Figure 198** Jet fire simulation results: flames at 2 s from pipe collapse. *Source:* Marmo, Piccinini and Fiorentini, 2013. 329
- Figure 199** Jet fire simulation results: flames at 3 s from pipe collapse. *Source:* Marmo, Piccinini and Fiorentini, 2013. 330
- Figure 200** Jet fire simulation results: temperature at 1 s from pipe collapse. *Source:* Marmo, Piccinini and Fiorentini, 2013. 331
- Figure 201** Jet fire simulation results: temperature at 2 s from pipe collapse. *Source:* Marmo, Piccinini and Fiorentini, 2013. 332
- Figure 202** Jet fire simulation results: temperature at 3 s from pipe collapse. *Source:* Marmo, Piccinini and Fiorentini, 2013. 333

- Figure 203** Scheme of the hydraulic circuits with two-position (a) and three-position (b) solenoid valves. *Source:* Marmo, Piccinini and Fiorentini, 2013. 334
- Figure 204** Event tree of the accident. The grey boxes indicate a lack of safety devices. *Source:* Marmo, Piccinini and Fiorentini, 2013. 336
- Figure 205** Damages on the forklift. 340
- Figure 206** Frames from the 3D video, reconstructing the incident dynamics. 342
- Figure 207** Bow-Tie diagram of the ThyssenKrupp fire. 343
- Figure 208** Twente stadium roof collapse Tripod Beta analysis. 345
- Figure 209** Water treatment Bow-Tie analysis. 346
- Figure 210** Timeline of the sample (developed with CGE-NL IncidentXP). 348
- Figure 211** Possible RCA of the sample (developed with CGE-NL IncidentXP). 348
- Figure 212** Possible Tripod Beta of the sample (developed with CGE-NL IncidentXP). 349
- Figure 213** Possible BFA of the event (developed with CGE-NL IncidentXP). 350
- Figure 214** Bow-Ties developed to assess fire risk in multiple railway stations. 352
- Figure 215** Fire load. 354
- Figure 216** Bow-Tie worksheet developed by TECSA S.r.l. and Royal Haskoning DHV to quantify a Bow-Tie scheme with a LOPA approach. Not real scores and data presented in the image. 356
- Figure 217** Barriers/protection layer scores. 357
- Figure 218** Weakest barriers and the public. 359
- Figure 219** Bow-Tie model for fire risk assessment in PV plants. 361
- Figure 220** Map of ceramuc density in Italy. 362
- Figure 221** Annual average temperature in Italy. 363
- Figure 222** Deming Cycle from a barrier-based perspective. 366
- Figure 223** Bow-Tie core elements and general structure. 371
- Figure 224** Bow-Tie guiding principles. 372
- Figure 225** BFA core elements. 374
- Figure 226** Incident barrier state. 375
- Figure 227** Incident barrier state decision support tree. 376
- Figure 228** BFA guiding principles. 377
- Figure 229** Classification of human failure. 380
- Figure 230** Fault tree analysis, current configuration (ANTE). 399
- Figure 231** Fault tree analysis, better configuration (configuration A). 400
- Figure 232** Fault tree analysis, the best configuration (POST configuration). 401
- Figure 233** Frequency estimation of the scenario “Oxygen sent to blow down, during start up of reactor of GAS1”. 402
- Figure 234** The Swiss Cheese Model by James Reason. *Source:* Reason, 1990. 404
- Figure 235** Level 1: Unsafe acts. 405
- Figure 236** Level 2: Preconditions. 406
- Figure 237** Level 3: Supervision issues. 406
- Figure 238** Level 4: Organizational issues. 407

List of Tables

Table 1	Applicability of tools for risk assessment.	32
Table 2	Example of “what-if” analysis. <i>Source</i> : Adapted from Assael, M. and Kakosimos, K., 2010.	109
Table 3	Guidewords for HAZOP analysis.	109
Table 4	Extract of an example of HAZOP analysis. Adapted from Assael and Kakosimos (2010).	111
Table 5	Subdivision of the analyzed system into areas.	112
Table 6	Hazards and assumed event in HAZID.	113
Table 7	List of typical consequences.	113
Table 8	HAZID worksheet.	114
Table 9	Different classification of barriers as physical or non-physical.	161
Table 10	Comparison of defined hazards with insufficient detail and optimal degree for evaluation.	170
Table 11	Comparison of defined top events with insufficient detail and with an optimal degree for evaluation.	171
Table 12	Comparison of defined causes with insufficient detail and with an optimal degree for evaluation.	171
Table 13	Comparison of defined consequences with insufficient detail and with an optimal degree of evaluation.	172
Table 14	Barrier Types.	173
Table 15	Quality scores and judgments on the effectiveness of barriers.	182
Table 16	Standard Performance Scores (PS).	182
Table 17	Definition of BRFs in Tripod Beta.	195
Table 18	Example of spreadsheet event timeline.	203
Table 19	Example of Gantt chart investigation timeline.	203
Table 20	Barrier function score (FS).	234
Table 21	Barrier consequence of failure score (CS).	234
Table 22	Barrier redundancy score (RS).	234
Table 23	Barrier criticality ranking.	235
Table 24	Barrier criticality assessment example.	235
Table 25	Interpretation of the barrier-based audit response histograms.	239
Table 26	Survey team members should and should not.	252

Table 27 General information about the case study. 319

Table 28 Record of the supervisor systems (adapted from Italian). *Source:* Marmo, Piccinini and Fiorentini, 2013. 323

Table 29 Threshold values according to Italian regulations. *Source:* Marmo, Piccinini and Fiorentini, 2013. 325

Table 30 Summary of the investigation. 341

Table 31 Example of calculating HEP with the SPAR-H Method. 392

Table 32 PIF (current configuration) 397

Table 33 PIF (Configuration A) 398

Table 34 PIF (POST configuration) 398

Table 35 Frequency of incidental assumptions considered. 403

List of Acronyms

AHJ	authority having jurisdiction
AIChE	American Institute of Chemical Engineers
ALARP	as low as reasonably practicable
BCM	business continuity management
BCMS	Business Continuity Management System
BFA	barrier failure analysis
BIA	business impact analysis
BPCS	basic process control system
BRF	basic risk factor
BSCAT	barrier-based systematic cause analysis technique
BT	Bow-Tie
CCD	cause-consequence diagram
CCPS	Centre for Chemical Process Safety
COSO	Committee of Sponsoring Organizations of the Treadway Commission
ERM	enterprise risk management
ETA	event tree analysis
FARSI	functionality, availability, reliability, survivability and interactions
FMEA	failure modes and effects analysis
FMECA	failure modes, effects, and criticality analysis
FMEDA	failure modes, effects, and diagnostic analysis
FSMS	fire safety management system
FTA	fault tree analysis
GAMAB	globally at least as good
GIGO	garbage in, garbage out
HAZID	hazard identification
HAZOP	hazard and operability analysis
HEART	human error assessment and reduction technique
HEMP	hazard and effects management process
HEP	human error probability
HFACS	human factors analysis and classification scheme
HLS	high-level system
HSE	health, safety, and environment
HSEQ	health, safety, environment, and quality
ICT	information and communications technology

IE	initial event
IEC	International Electrotechnical Commission
IEF	initial event frequency
IPL	individual protection layer
IRM	The Institute of Risk Management
IRPA	individual risk per annum
IRT	independent protection layer response time
ISO	International Organization for Standardization
IT	information technology
KPI	key performance indicator
LFE	learning from experience
LOPA	layer of protection analysis
LOPC	loss of primary containment
MEM	minimum endogenous mortality
MGS	at least the same level of safety
MOC	management of change
NFPA	National Fire Protection Association
NMAU	not more than unavoidable
PDCA	Plan-Do-Check-Act
P&ID	pipng and instrumentation diagram
PDF	probability of failure on demand
PHA	preliminary hazard analysis
PIF	performance-influencing factor
PPE	personal protective equipment
PSM	process safety management
QIQO	quality in, quality out
QRA	quantitative risk assessment
RA	risk assessment
RAGAGEP	recognized and generally accepted good engineering practice
RBD	reliability block diagram
RCA	root cause analysis
RM	risk management
ROI	return on investment
RPN	risk priority number
RRF	risk-reducing factor
SCE	safety critical equipment
SHIPP	system hazard identification, prediction and prevention
SIF	safety instrumented function
SIL	safety integrity level
SIS	safety instrumented system
SLC	safety life cycle
SLIM	Success Likelihood Index Method
SMS	safety management system
SPAR-H	Standardized Plant Analysis Risk-Human Reliability Analysis
THERP	technique for human error-rate prediction
TR	technical report

Preface 1

Riccardo Ghini

Quality Head Italy & Malta and South Europe Cluster, Sanofi

Risk assessment is a basic concept that has always accompanied me throughout my work and professional experience, so being able to contribute, albeit marginally, to the drafting of this monumental work fills me with pride and happiness.

Since the time of Legislative Decree 626/94, the ability to evaluate the probability of occurrence and the possible consequences of accidents and injuries at work has been a fundamental skill for me to develop, through the study of ever-more-refined methods and techniques of investigation. Finding all these useful analysis tools grouped in this way, brilliantly described and accompanied by real application examples, represents for me, and for all professionals, a unique opportunity for enrichment and deepening.

In fact, as my career continued, I soon realized how the concepts underlying this book can be effectively applied, not only in the field of work safety, but also in all areas of business activity, where words like “risk,” “scenario,” “analysis of the causes,” and “continuous improvement” have become commonly used, as they are based on the very structure of the management systems developed in accordance with the various reference standards, now completely standardized.

Furthermore, we mustn't fail to mention the importance assumed by the methods of analysis, assessment, and operational management of the risks associated with the predicate offenses of Legislative Decree 231/2001 (administrative liability of companies and entities), which constitute the essential element in the preparation of a Corporate Organization, Management, and Control Model that effectively prevents the occurrence of the types of offense and, at the same time, constitutes a valid exemption in the context of a possible criminal trial.

The real cultural transition, however, takes place when the concept of risk assessment is adopted and is also applied outside the professional sphere, elevating it to a rational criterion to guide our daily choices: “do I overtake or not overtake the car that's in front of me?”, “do I subscribe to this insurance policy or not?”, “do I vaccinate my children or not?” These are all questions and situations we face every day, and for which it is very useful to identify the possible “top event,” the “consequences” that can be generated, and the “causes” that can originate it, as well as to know what “barriers” we can implement in our defence.

This book is therefore much more than a scientific text for a few super-technicians and experts; it is a concrete and useful reference to all, to bring order and reasoning into our decisions, whatever they may be, in a world increasingly dominated by superficiality and disinformation.

I would also like to underline another aspect, often not adequately communicated: the concept of risk not only with a negative meaning, as a threat or weighting of an unfavourable event, but also, from the perspective of ISO 31000, as a positive deviation from the result expected, therefore, as an opportunity, to be evaluated and seized for the development of the organization. A better understanding of this dimension of risk would certainly facilitate a wider and more extensive use of the methodologies illustrated in the book.

At this point, before diving into reading and studying, I just have to applaud the authors, who represent all-Italian excellence, similar to Ferrari and Parmigiano Reggiano, in this scientific field traditionally the prerogative of Anglo-Saxon and American schools, and of which we must all be proud.

Preface 2

Bernardino Chiaia

Head of SISCON (Safety of Infrastructures and Constructions), Politecnico di Torino

The number and the magnitude of accidents worldwide in the industrial sector and in the realm of civil and transportation infrastructures has risen since the 1970s and continues to grow both in frequency and socioeconomic impact. Several major accidents in the industrial sector (see, e.g., the Seveso chemical plant disaster in 1976, the Bhopal gas tragedy in 1984, the Chernobyl nuclear accident in 1986, the *Deepwater Horizon* oil spill in 2010, the explosion in Warehouse 12 at the Port of Beirut in 2020) have been under the lens of the United Nations Office for Disaster Risk Reduction (UNISDR), which puts great effort in developing safety guidelines within the Sendai Framework for Disaster Risk Reduction 2015–2030.

At the same time, the number of infrastructure failures in developed countries rose dramatically since the beginning of the new millennium. This is partly due to ageing and poor maintenance of bridges, viaducts, tunnels, and dams, which were constructed mainly in the first 35 years after World War II. Moreover, traffic loads and required performances have increased 20 times the original design conditions. On the other hand, in underdeveloped countries there is clear evidence that industrial regulations are less strict and that a general lack of a culture of safety generally results in looser applications of the rules, thus producing a physiological higher percentage of accidents.

In this evolving context, the barrier-based approach named *Bow-Tie* represents a successful methodology to approach risk analysis in a consistent and robust manner. The method allows a synthetic and powerful control of multiple hazard scenarios, clearly differentiating between proactive and reactive risk management.

In this book Dr Fiorentini clearly shows the applicability and the advantages of the methodology to various situations. He shows that, once all the hazard scenarios have been correctly identified and well defined, the definition of the most appropriate barriers represents the core of the methodology to ensure risk reduction. In the non-standard case of civil engineering, for example, the Bow-Tie method shows how inspections and maintenance operations represent *preventive* control barriers against the risk of structural collapse, whereas retrofitting, traffic limitations, and active monitoring represent *mitigating* or *recovery* barriers.

The wide experience of Dr Fiorentini, along with his clarity and scientific rigour, make the book a unique and comprehensive essay on the Bow-Tie methodology of risk assessment.

Preface 3

Luca Marmo

Professor of Safety of Industrial Processes, Politecnico di Torino Department of Applied Science and Technology

In over 30 years of mountaineering and ski touring (see an example in Figure 1), I have done thousands of risk analyses, probably more than I have ever done in my professional career. Each preparation for a climb includes risk analysis. Imagine, or remember, if you have the same passion as me, a classic of European ski mountaineering, the high street Chamonix Zermatt. Climbing it takes three days if you are a pro climber, four if you are super-trained—better five or six if you are merely human—between glaciers, crevasses, overhanging rocks, and descents hanging from a rope with skis on your shoulders. 6,300 m of positive altitude difference, all between 1,600 and 3,800 m of altitude. Risky? Yes. Accidents, even fatal ones, in these environments are not so rare. However, those who do not practice mountaineering tend to overestimate the risks because they do not have the cognitive tools to evaluate them.



Figure 1 Descent from Col du Chardonnet. Is it safe? *Source:* Luca Marmo archive photo.

- processes 2, 4
 - sustainability 4
 - systems approach 76–99
 - complexity management 78
 - functional safety 89–91
 - industrial safety 87–89
 - ISO 9001/ISO 45001/ISO 14001 82–86
 - ISO 19011 95–97
 - ISO 19600 98–99
 - ISO 22301 92–94
 - ISO 39001 97–98
 - ISO 55000 91–92
 - ISO IEC 27001 94–95
 - RAGAGEP 89–91
 - tailoring 16–17
 - risk matrix
 - BT, risk evaluation 130
 - BT workflows 221–222
 - intolerable risk 222
 - residual risk 222
 - ISO 31000 39–41
 - risk priority number (RPN), FMECA 115, 116
 - risk register
 - BT 178–183
 - HAZOP 111
 - ISO 9001/ISO 45001/ISO 14001 86
 - risk source
 - BT 261
 - defined 6
 - ISO 31000 368
 - risk treatment
 - BT workflows, BFA 261
 - defined 6
 - HAZOP 111
 - ISO 22301 93
 - ISO 31000 31, 45–47
 - RM
 - culture 68
 - systems approach 80
 - risk zero 6
 - risk-reducing factors (RRFs)
 - BT, cost-benefit assessment 134
 - Deepwater Horizon* 368
 - ISO 9001/ISO 45001/ISO 14001 85, 86
 - ISO 22301 94
 - RM systems approach 80
 - industrial safety 88, 89
 - RAGAGEP 89
 - tolerable risk 133
 - RM. *See* risk management
 - road traffic safety. *See* ISO 39001
 - root cause analysis (RCA)
 - BFA 208–213
 - BT workflows, BFA 257, 347–348
 - risk identification 30
 - root causes
 - accident investigation 190, 191, 192
 - accidents 53
 - BFA 196, 207
 - BT workflows, BFA 262
 - ISO 31000 14
 - routine violations 386
 - RPN. *See* risk priority number
 - RRFs. *See* risk-reducing factors
 - RS. *See* redundancy score
 - rule-based performance, human error
 - 381–382
- S**
- Saetre, T. I. 265
 - safety critical equipment (SCE), BT
 - critical barriers 233
 - LOPA 167
 - safety instrumental functions (SIFs), BT
 - 131, 132
 - safety instrumented systems (SISs), BT
 - calibrated risk graph 131
 - LOPA 168
 - safety integrity levels (SILs) 89
 - BT
 - calibrated risk graph 131–133
 - LOPA 168
 - BT workflows
 - BFA 262
 - LOPA 244, 247
 - FEMA 115
 - safety life cycle (SLC) 89
 - safety management system (SMS)
 - BT, hazards and risks 101
 - FSM 358

- safety management system (SMS) (*cont'd*)
- FSMS 351, 358
 - incident barriers 376
 - RM systems approach
 - industrial safety 87–88
 - RAGAGEP 90
 - SAP, BT workflows 218
 - SCE. *See* safety critical equipment
 - scribes, HAZOP 110
 - secondary barriers, BT
 - BT, DC 144, 145
 - escalation factors 165
 - LOPA 174–175
 - workflows 222, 223
 - secondary cause, BFA 196, 199, 208, 374
 - semi-quantitative methods, ISO31000 RM
 - risk analysis 35
 - sensitivity analysis, ISO 31000 38
 - session management, BT workflows, web-based software development 279
 - Seveso Directive, RM systems approach
 - industrial safety 87
 - SHIPP. *See* system hazard identification, prediction and prevention
 - short-term solution, BFA 202
 - BT workflows 261
 - shut-down, BT workflows, LOPA 246
 - Sicari, R. 266
 - SIFs. *See* safety instrumental functions
 - significant incidents 220
 - Silady 162
 - SILs. *See* safety integrity levels
 - SISs. *See* safety instrumented systems
 - situational violations 386
 - skill-based performance, human error
 - 381–382
 - Sklet, S. 119, 159, 162, 213
 - SLC. *See* safety life cycle
 - SLIM. *See* Success Likelihood Index Method
 - slips 382–383
 - SMART. *See* specific, measurable, agreed, realistic and timely
 - Smith, J. 265
 - SMS. *See* safety management system
 - socio-technical category, SPAR-H 388–389
 - SOPs. *See* standard operating procedures
 - SPAR-H. *See* Standardized Plant Risk Human Reliability Analysis
 - specific, measurable, agreed, realistic and timely (SMART)
 - BT, safety culture 66
 - BT workflows, BFA 262
 - stakeholders
 - accident investigation 190
 - BT workflows 227
 - communication 368–369
 - governance 366
 - ISO 9001/ISO 45001/ISO 14001 85
 - ISO 31000 14
 - risk treatment 45, 46
 - system performance review 49
 - ISO 55000 91
 - reporting 368–369
 - RM 15
 - systems approach 81
 - standard operating procedures (SOPs), RM
 - systems approach 82
 - Standardized Plant Risk Human Reliability Analysis (SPAR-H) 388–391, 392–393
 - ISO 31000, human factors 54
 - start-up
 - BT workflows, LOPA 246
 - RM systems approach 81
 - SLIM 397
 - Statement of Applicability, ISO IE 27001 95
 - Stimulus-Response model 55
 - strategic risk
 - ERM 61
 - ISO 9001/ISO 45001/ISO 14001 85
 - strategy and objective-setting, ISO 31000,
 - ERM 59
 - stress/stressors 245
 - mistakes 384
 - SPAR-H 389, 392
 - Strobhar, D. 54
 - Success Likelihood Index Method (SLIM)
 - 388, 391–407
 - sustainability, RM 4
 - Swain 177
 - Swiss Cheese Model 4, 5, 367–368

- BT 137–138
 - RM systems approach, industrial safety 88
 - SLIM 402, 404–407
 - system automation and demand, ISO 31000, PSFs 58
 - system hazard identification, prediction and prevention (SHIPP) 160
 - system performance review, ISO 31000 49–53
- t**
- Tafaro, S. 265
 - tailoring
 - ISO 31000 368
 - RM 16–17
 - tasks, BT workflows 228–229
 - taxonomies
 - BFA 196, 370
 - BT workflows 219–221
 - Taylor, J. 54
 - teams, risk identification 33
 - technical specialists
 - accident investigation 190
 - HAZOP 110
 - Technique for Human Error Rate Prediction (THERP) 387
 - ISO 31000, human factors 54
 - tertiary cause, BFA 196, 199, 208, 374
 - THERP. *See* Technique for Human Error Rate Prediction
 - Thinking-Behavior-Result model 54
 - threats
 - BT 150, 154–156, 371, 372
 - BT workflows 228
 - IT operations 280
 - web-based software development 275
 - three D's (detect, decide and deflect), BT workflows 247
 - ThyssenKrupp fire investigation, BT workflows 318–341, 342–343
 - TIER, RCA 213
 - timeline
 - BFA 202–206
 - incident analysis 347–349
 - cause-and-effect analysis 255
 - RCA 210
 - Tripod Beta accident investigation 193
 - time-to-reliability correlation (T/RC) 388
 - tolerable mitigated event frequency (TMEF) 133
 - tolerable risk
 - ALARP 222, 248
 - BT 102
 - BT workflows
 - LOPA 248–249
 - risk matrix 222
 - ISO 31000 38–39
 - LOPA IPLs 247
 - risk indices 130
 - risk matrix 41, 222
 - RRFs 133
 - Top events
 - BT 127, 153–154, 371, 372
 - barriers 157
 - BFA 202
 - domino effects 92
 - LOPA 170
 - BT workflows 223
 - top-down approach, BT workflows 240–241
 - total unmitigated hazard cost (TUHC) 133
 - transparency
 - BT workflows 223–224
 - RM 15
 - Travers, I. 265
 - T/RC. *See* time-to-reliability correlation
 - Treadway Commission, COSO 59, 60–61
 - Tripod Beta
 - accident investigation 192–194, 195
 - BT workflows, BFA 257, 258
 - RCA 212
 - Twente Stadium roof collapse, BT workflows 345
 - TUHC. *See* total unmitigated hazard cost
 - Twente Stadium roof collapse, Tripod Beta 345
- u**
- UEF. *See* unmitigated event frequency
 - uncertainty
 - BT 102

uncertainty (*cont'd*)
 ISO 31000 368
 human factors 53–58
 risk analysis, ISO 31000 38
 RM 15
 underlying cause 52
 BFA 202, 207
 HAZID 113
 RCA 208
 understanding violations 385–386
 United Nations Industrial Development
 Organization, International Trade
 Centre 368
 unmitigated event frequency (UEF) 133

V

validation
 BT, DC 145
 BT workflows, web-based software
 development 277
 MOC 277
 RCA 209
 risk assessment 31
 Vanden Heuvel, L. 210, 212
 vehicle safety, ISO 39001 98
 verification, BT, barriers 162
 violations 385–386

 defined 380
 reporting 264
 Vision 2000 366

W

water treatment, BT workflows 344, 346
 web-based software development, BT
 workflows 271–279
 what-if (WI)
 BT, risk identification 106–108, 109
 BT workflows 285, 286
 mistakes 385
 WI. *See* what-if
 Willauer, H. 324
 Williams, F. 324
 Woods, D. 54
 Work Bow-Tie, RM systems approach
 industrial safety 87
 work control, RM systems approach 81
 work organization, ISO 31000, PSFs 58
 work processes
 inverted two-pointed model 56
 SPAR-H 390, 393
 workflows. *See* Bow-Tie workflows; ISO
 31000 workflows
 World Economic Forum, Annual Global Risk
 Report by 7