



---

# GUIDELINES FOR HAZARD EVALUATION PROCEDURES

---

Third Edition

Center for Chemical Process Safety  
New York, New York



A JOHN WILEY & SONS, INC., PUBLICATION

This Page Intentionally Left Blank

# **GUIDELINES FOR HAZARD EVALUATION PROCEDURES**

This book is one in a series of process safety guideline and concept books published by the Center for Chemical Process Safety (CCPS). Please go to [www.wiley.com/go/ccps](http://www.wiley.com/go/ccps) for a full list of titles in this series.

---

# GUIDELINES FOR HAZARD EVALUATION PROCEDURES

---

Third Edition

Center for Chemical Process Safety  
New York, New York



A JOHN WILEY & SONS, INC., PUBLICATION

It is sincerely hoped that the information presented in this document will lead to an even more impressive safety record for the entire industry. However, neither the American Institute of Chemical Engineers, its consultants, CCPS Technical Steering Committee and Subcommittee members, their employers, their employers' officers and directors, nor ABSG Consulting Inc. and its employees warrant or represent, expressly or by implication, the correctness or accuracy of the content of the information presented in this document. As between (1) American Institute of Chemical Engineers, its consultants, CCPS Technical Steering Committee and Subcommittee members, their employers, their employers' officers and directors, and ABSG Consulting Inc. and its employees and (2) the user of this document, the user accepts any legal liability or responsibility whatsoever for the consequence of its use or misuse.

Copyright © 2008 by American Institute of Chemical Engineers, Inc. All rights reserved.

A Joint Publication of the Center for Chemical Process Safety of the American Institute of Chemical Engineers and John Wiley & Sons, Inc.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.  
Published simultaneously in Canada.

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, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4470, or on the web at [www.copyright.com](http://www.copyright.com). Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permission>.

**Limit of Liability/Disclaimer of Warranty:** While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

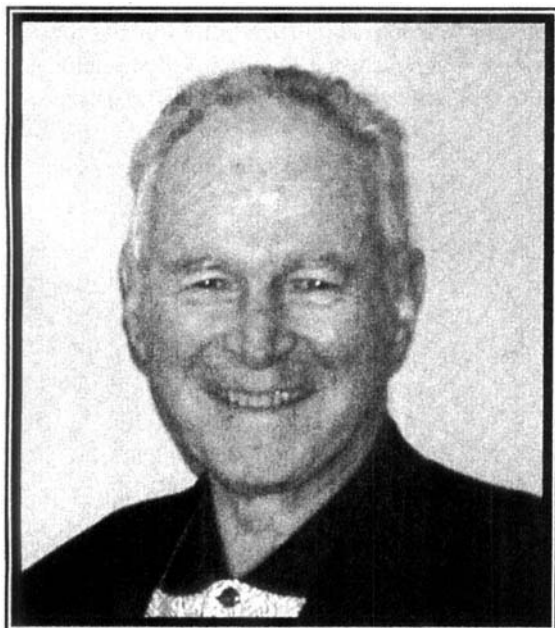
Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic format. For information about Wiley products, visit our web site at [www.wiley.com](http://www.wiley.com).

***Library of Congress Cataloging-in-Publication Data is available.***

ISBN 978-0-471-97815-2

Printed in the United States of America.

10 9 8 7 6 5 4



## **In Honor of Tom Carmody**

This third edition of CCPS' *Guidelines for Hazard Evaluation Procedures* is dedicated to Tom Carmody. Tom served as the first Director of CCPS from its first year in 1985 until 1993. He made extensive use of his leadership skills from Union Carbide in establishing the basis for the organization—how it would function, the products it would develop, the acquisition of sponsors, and the development of relationships with various national and international organizations interested in process safety. Although he had not been personally involved in process safety when he took over the position, he learned rapidly, making the best use of the technical experts from the various sponsor organizations. He was the right person at the right time to develop and grow CCPS. It is only fitting that this third edition be dedicated to Tom, since the first edition of *Guidelines for Hazard Evaluation Procedures* was CCPS' very first publication and the first fruits of his leadership.

Tom and his wife Jill reside in Amelia Island, Florida.

This Page Intentionally Left Blank



# Contents

Acknowledgments .....	xi
List of Tables .....	xiii
List of Figures .....	xvii
Abbreviations and Acronyms .....	xix
Glossary .....	xxi

## Part I – Hazard Evaluation Procedures

<b>Preface.....</b>	<b>3</b>
<b>Management Overview .....</b>	<b>11</b>
<b>1 Introduction to the Guidelines .....</b>	<b>15</b>
1.1 Background .....	16
1.2 Relationship of Hazard Evaluation to Risk Management Strategies .....	17
1.3 Anatomy of a Process Incident .....	18
1.4 The Role of Safeguards .....	23
1.5 Hazard Evaluation Throughout a Plant Lifetime .....	29
1.6 Hazard Evaluation and Regulations .....	29
1.7 Limitations of Hazard Evaluation .....	30
<b>2 Preparation for Hazard Evaluations .....</b>	<b>35</b>
2.1 Infrastructure .....	35
2.2 Analysis Objectives .....	36
2.3 Developing the Review Scope and Boundaries .....	38
2.4 Information Requirements .....	38
2.5 Use of Software Programs .....	41
2.6 Personnel and Skills .....	42
2.7 Schedule and Execution .....	45
2.8 Initial Team Review Meeting .....	47
<b>3 Hazard Identification Methods .....</b>	<b>51</b>
3.1 Analyzing Material Properties and Process Conditions .....	51
3.2 Using Experience .....	54
3.3 Developing Interaction Matrixes .....	55
3.4 Hazard Identification Results .....	58
3.5 Using Hazard Evaluation Techniques to Identify Hazards .....	59
3.6 Initial Assessment of Worst-Case Consequences.....	60
3.7 Hazard Reduction Approaches and Inherent Safety Reviews .....	62
<b>4 Non-Scenario-Based Hazard Evaluation Procedures .....</b>	<b>71</b>
4.1 Preliminary Hazard Analysis .....	73
4.2 Safety Review .....	79
4.3 Relative Ranking .....	84
4.4 Checklist Analysis .....	93

<b>5</b>	<b>Scenario-Based Hazard Evaluation Procedures .....</b>	<b>99</b>
5.1	What-If Analysis .....	100
5.2	What-If/Checklist Analysis .....	107
5.3	Hazard and Operability Studies .....	115
5.4	Failure Modes and Effects Analysis .....	134
5.5	Fault Tree Analysis .....	142
5.6	Event Tree Analysis .....	158
5.7	Cause-Consequence Analysis and Bow-Tie Analysis .....	167
5.8	Other Techniques .....	173
<b>6</b>	<b>Selection of Hazard Evaluation Techniques .....</b>	<b>175</b>
6.1	Factors Influencing the Selection of Hazard Evaluation Techniques .....	176
6.2	Decision-Making Process for Selecting Hazard Evaluation Techniques .....	186
6.3	Example Using the Proposed Selection Criteria .....	186
6.4	Hazard Reviews for Management of Changes .....	194
6.5	Combined Hazard Reviews .....	197
6.6	Hazard Evaluation at Different Plant Lifetime Stages .....	198
6.7	Integrating Occupational Safety, Environment, Reliability, Maintainability, Quality, and Security into Hazard Evaluations .....	204
<b>7</b>	<b>Risk-Based Determination of the Adequacy of Safeguards .....</b>	<b>211</b>
7.1	Scenarios from Scenario-Based Hazard Evaluations .....	212
7.2	Severity of Consequences .....	213
7.3	Frequency of Initiating Causes .....	217
7.4	Effectiveness of Safeguards .....	218
7.5	Risk Estimation using Risk Matrix or Direct Calculation .....	220
7.6	Layer of Protection Analysis .....	223
<b>8</b>	<b>Analysis Follow-Up Considerations .....</b>	<b>233</b>
8.1	Development of Recommendations .....	233
8.2	Prioritization of Hazard Evaluation Results .....	235
8.3	Documentation of Hazard Evaluations .....	245
8.4	Development of a Management Response to a Hazard Evaluation .....	249
8.5	Resolution of Action Items .....	251
8.6	Communication of Special Findings/Sharing of Information .....	253
8.7	Use of Hazard Evaluation Results over the Plant Lifetime .....	254
<b>9</b>	<b>Extensions and Special Applications .....</b>	<b>257</b>
9.1	Hazard Evaluation of Procedure-Based Operations .....	257
9.2	Hazard Evaluation of Processes Controlled by Programmable Systems .....	268
9.3	Hazard Evaluation of Chemical Reactivity Hazards .....	272
9.4	Combinations of Tools .....	274
9.5	Human Factors and Human Reliability Analysis .....	276
9.6	Facility Siting .....	288

**Part II - Worked Examples and Appendices**

<b>Preface to the Worked Examples .....</b>	<b>297</b>
<b>Management Overview of the Worked Examples .....</b>	<b>299</b>
<b>10 Introduction to the Worked Examples .....</b>	<b>301</b>
10.1 Purpose .....	301
10.2 Instructional Strategy .....	302
10.3 How to Use the Worked Examples .....	303
<b>11 Description of the Example Facility and Process .....</b>	<b>305</b>
11.1 Company and Facility Background .....	305
11.2 Process Overview .....	306
11.3 Description of the Process Lifetime .....	306
<b>12 Hazard Identification for the Example Process .....</b>	<b>309</b>
12.1 Analysis of Material Properties .....	309
12.2 Review of Experience .....	310
12.3 Interaction Matrix .....	311
12.4 Hazard Evaluation Techniques Used for Hazard Identification .....	312
12.5 Summary .....	313
<b>13 Research and Development – What-If Analysis .....</b>	<b>315</b>
<b>14 Conceptual Design – Preliminary Hazard Analysis .....</b>	<b>327</b>
<b>15 Pilot Plant Operation – HAZOP Study .....</b>	<b>339</b>
<b>16 Detailed Engineering – Fault Tree and Event Tree Analysis .....</b>	<b>365</b>
<b>17 Construction/Start-up – Checklist Analysis and Safety Review .....</b>	<b>379</b>
<b>18 Routine Operation – Safety Review for Management of Change .....</b>	<b>389</b>
<b>19 Routine Operation – HAZOP Study for Cyclic Review .....</b>	<b>395</b>
<b>20 Plant Expansion – Relative Ranking and HAZOP for a Batch Process ..</b>	<b>409</b>
<b>21 Incident Investigation – FMEA and HRA .....</b>	<b>435</b>
<b>22 Decommissioning – What-If/Checklist Analysis .....</b>	<b>451</b>
<b>Appendices</b>	
Appendix A – Additional Checklists and Forms .....	462
Appendix B – Supplemental Questions for Hazard Identification .....	477
Appendix C – Symbols and Abbreviations for Example Problem Drawings .....	519
Appendix D – Software Aids .....	521
Appendix E – Chemical Compatibility Chart .....	523
Appendix F – Organizations Offering Process Safety Enhancement Resources ..	529
<b>Selected Bibliography .....</b>	<b>535</b>
<b>Index .....</b>	<b>537</b>

This Page Intentionally Left Blank

# Acknowledgments

The Center for Chemical Process Safety (CCPS) thanks all of the members of the HEP3 (Hazard Evaluation Procedures, 3<sup>rd</sup> Edition) Subcommittee of CCPS' Technical Steering Committee for providing input, reviews, technical guidance and encouragement to the project team throughout the preparation of this book. CCPS also expresses appreciation to the members of the Technical Steering Committee for their advice and support.

The CCPS staff liaison for this project was Bob Ormsby, who also coordinated meetings and facilitated subcommittee reviews and communications. The subcommittee had the following members, whose significant efforts and contributions are gratefully acknowledged:

Jonathan Babcock  
Eli Lilly and Company

Bob Lenahan  
Bayer BMS

Kumar Bhimavarapu  
FM Global

Donald Lorenzo  
ABS Consulting

Christine E. Browning  
Eastman Chemical Company

Narayanan Sankaran  
UOP

Paul Butler  
Buckman Laboratories

John C. Stoney  
BP

Ken Harrington, HEP3 Subcommittee Chair  
Chevron/Phillips

Angela Summers  
SIS-TECH Solutions, LP

Wayne Jamison  
Intel

Tim Wagner  
The Dow Chemical Company

Jim Johnston  
Wyeth

Joe Wilson  
Syngenta

Unwin Company (Columbus, Ohio) prepared this Third Edition of the *Guidelines for Hazard Evaluation Procedures*, building on the previous work of Battelle Memorial Institute (First Edition) and JBF Associates, Inc. (Second Edition). Robert W. Johnson was Unwin Company's lead author and project manager for the Third Edition. John F. Murphy was a principal author, and Steven W. Rudy, John E. Corn, and Bryan T. Haywood authored and reviewed particular sections within their areas of expertise. William G. Bridges and Revonda Tew of Process Improvement Institute, Inc. (Knoxville, Tennessee) contributed the new section on hazard evaluation of procedure-based operations.

CCPS and the Unwin Company project team also gratefully acknowledge the valuable suggestions and feedback submitted by the following persons who provided peer review comments on the final draft manuscript.

Jeffrey Castillo	Monsanto Company
Carol Garland	Eastman Chemical Company
Richard C. Griffin	Chevron Phillips Chemical Company LP
Kevin L. Klein	Solutia, Inc.
Mark M. Moderski	Lummus
Adrian L. Sepeda	CCPS Emeritus
Martin Sich	
Steve Sigmon	Honeywell Specialty Materials
Robert J. Stack	The Dow Chemical Company

In addition, comments on specific sections were provided by Paul Delanoy, Gregory Schultz and David Wechsler of The Dow Chemical Company.

# List of Tables

## Table

1.1	Hazard evaluation synonyms	16
1.2	CCPS elements of risk-based process safety	17
1.3	Elements of process incidents	19
1.4	Governmental regulations related to identifying and evaluating process hazards	30
1.5	Classical limitations of hazard evaluations	31
2.1	Typical hazard evaluation objectives at different stages of a process lifetime	37
2.2	Examples of information used to perform a hazard evaluation	40
2.3	Candidates for membership on a hazard evaluation team	44
2.4	Important team leader responsibilities	46
3.1	Common material property data for hazard identification	53
3.2	Examples of hazardous chemical compounds	55
3.3	Other parameters commonly used in an interaction matrix	56
3.4	Typical hazard identification results	58
3.5	Examples of checklist questions used in hazard identification	60
3.6	Inherent safety review team composition	66
4.1	Time estimates for using the Preliminary Hazard Analysis technique	74
4.2	Typical format for a Preliminary Hazard Analysis worksheet	76
4.3	Sample page from the H <sub>2</sub> S system example Preliminary Hazard Analysis table	78
4.4	Time estimates for using the Safety Review technique	80
4.5	Summary of Relative Ranking indexes	87
4.6	Time estimates for using Relative Ranking techniques	89
4.7	Data for the Relative Ranking example	92
4.8	Results from the Relative Ranking example	92
4.9	Time estimates for using the Checklist Analysis technique	94
4.10	Sample items from the checklist for the DAP process example	98
5.1	Time estimates for using the What-If Analysis technique	102
5.2	Typical format for a What-If Analysis worksheet	104
5.3	What-if questions for the DAP process example	104
5.4	Sample page from the What-If Analysis table for the DAP process example	105
5.5	Time estimates for using the What-If/Checklist Analysis technique	109
5.6	What-if questions for the chlorine feed line example	110
5.7	Example of a hazard checklist	113
5.8	Additional safety issues generated by using hazard checklists in the chlorine example	114
5.9	Common HAZOP Study terminology	117
5.10	Original HAZOP Study guide words and meanings	118
5.11	Common HAZOP Study process parameters	118
5.12	Time estimates for using the HAZOP Study technique	120
5.13	Typical format for a HAZOP Study worksheet	123
5.14	Example library of relevant deviations for process section types	127

**Table**

<b>5.15</b>	Inherent safety strategies as HAZOP Study guide words	128
<b>5.16</b>	Sample deviations from the HAZOP Study table for the DAP process example	131
<b>5.17</b>	Time estimates for using the FMEA technique	135
<b>5.18</b>	Typical format for an FMEA worksheet	137
<b>5.19</b>	Examples of equipment failure modes used in an FMEA	138
<b>5.20</b>	Sample page from the FMEA table for the DAP process example	140
<b>5.21</b>	Logic and event symbols used in fault trees	143
<b>5.22</b>	Time estimates for using the Fault Tree Analysis technique	145
<b>5.23</b>	Rules for constructing fault trees	150
<b>5.24</b>	Minimal cut sets for the emergency cooling system example fault tree	157
<b>5.25</b>	Time estimates for using the Event Tree Analysis technique	159
<b>5.26</b>	Time estimates for using the Cause-Consequence Analysis technique	168
<b>5.27</b>	Incident sequence minimal cut sets for "loss of cooling water to the oxidation reactor"	171
<b>6.1</b>	Categories of factors that could influence the selection of hazard evaluation techniques	176
<b>6.2</b>	Typical information available to hazard analysts	179
<b>6.3</b>	Types of processes	181
<b>6.4</b>	Summary of typical staff effort estimates for hazard evaluation techniques	185
<b>6.5</b>	MOC review documents related to environment, health and safety	195
<b>6.6</b>	Some items to consider in a readiness review	201
<b>6.7</b>	Comparison between site security and process safety scenario elements	207
<b>7.1</b>	Scenarios are unique initiating cause / loss event combinations	214
<b>7.2</b>	Example of EHS impact categories and severity magnitudes used in hazard evaluations	215
<b>7.3</b>	Example initiating cause frequency scale (order-of-magnitude basis)	219
<b>7.4</b>	Example preventive safeguard failure probabilities	221
<b>7.5</b>	Example LOPA worksheet from Table B.2 of Reference 5	231
<b>8.1</b>	Classification of hazard evaluation techniques for the purpose of ranking action items	237
<b>8.2</b>	Typical ways of ranking recommendations from hazard evaluations	238
<b>8.3</b>	Example ranking of recommendations in qualitative categories of urgency	239
<b>8.4</b>	Example of structural importance ranking	240
<b>8.5</b>	Prioritization attributes of hazard evaluation techniques	241
<b>8.6</b>	Example of a Failure Modes, Effects and Criticality Analysis table	242
<b>8.7</b>	Example criticality (impact) categories	243
<b>8.8</b>	Example frequency categories	243
<b>8.9</b>	Example risk ranking categories	245
<b>8.10</b>	Some issues that influence the contents of hazard evaluation reports	246
<b>8.11</b>	Items to consider including in hazard evaluation reports	247
<b>8.12</b>	Examples of risk management considerations	250
<b>8.13</b>	Typical reasons why rejecting a hazard evaluation recommendation might be justified	251
<b>8.14</b>	Example action item tracking log	252
<b>8.15</b>	Some uses for hazard evaluation results over the life of a project	255
<b>9.1</b>	Definitions of guide words for HAZOP Study of procedure-based operations	260
<b>9.2</b>	Guide words for Two Guide Word Analysis of procedure-based operations	261
<b>9.3</b>	Example Two Guide Word Analysis documentation	262
<b>9.4</b>	Example choice of methods for hazard evaluation of all modes of operations	264
<b>9.5</b>	Programmable versus manual control	270



**Table**

<b>9.6</b>	Example deviations and causes with programmable control	271
<b>9.7</b>	Example positive and negative human factors	277
<b>9.8</b>	Time estimates for using the Human Reliability Analysis technique	280
<b>9.9</b>	Contributors to error-likely situations	283
<b>9.10</b>	HRA event tree incident sequences for the operator response to an alarm example	287
<b>9.11</b>	Facility siting considerations related to personnel and property protection	291
<b>10.1</b>	Summary of example problems	303
<b>11.1</b>	Primary VCM process materials and their primary hazards	306
<b>11.2</b>	Summary of lifetime phases for the example VCM process	308
<b>12.1</b>	VCM process materials	310
<b>12.2</b>	Hazardous properties of VCM process materials	310
<b>12.3</b>	Sample questions from the interaction matrix	311
<b>13.1</b>	Summary of key characteristics of chemicals used in the VCM manufacturing process	317
<b>13.2</b>	Sample What-If questions for the R&D phase example	319
<b>13.3</b>	Sample What-If Analysis results for the R&D phase	323
<b>13.4</b>	What-if Analysis staff requirements for the R&D phase	324
<b>14.1</b>	Partial list of materials in the VCM plant	329
<b>14.2</b>	Major equipment in the VCM plant	329
<b>14.3</b>	Preliminary questions for the conceptual design Preliminary Hazard Analysis	330
<b>14.4</b>	Sample Preliminary Hazard Analysis results for the VCM plant conceptual design	335
<b>14.5</b>	Preliminary Hazard Analysis staff requirements for the conceptual design phase	337
<b>15.1</b>	Furnace start-up procedure	350
<b>15.2</b>	Sample HAZOP Study results for the VCM pilot plant (deviation-by-deviation approach)	353
<b>15.3</b>	Sample action items from the VCM pilot plant HAZOP Study	355
<b>15.4</b>	HAZOP Study staff requirements for the VCM pilot plant	357
<b>15.5</b>	Sample HAZOP Study results for the VCM pilot plant (cause-by-cause approach)	357
<b>15.6</b>	Sample action items from the VCM pilot plant HAZOP Study (cause-by-cause approach)	358
<b>15.7</b>	Sample HAZOP Study results for the VCM pilot plant, with scenario risk estimates	364
<b>16.1</b>	VCM plant incinerator shutdowns	367
<b>16.2</b>	Steps in a combined Fault Tree and Event Tree Analysis	369
<b>16.3</b>	Fault Tree Analysis steps	373
<b>16.4</b>	Sample incident sequence minimal cut sets — incinerator explosion	377
<b>16.5</b>	Incinerator safety improvement alternatives	377
<b>16.6</b>	Combined FTA / ETA staff requirements for the detailed engineering phase	378
<b>17.1</b>	Checklist analysis results for the HCl storage tank inspection	386
<b>17.2</b>	Action items from the HCl storage tank Checklist Analysis	387
<b>17.3</b>	Checklist Analysis and Safety Review staff requirements for construction/start-up phase	387
<b>18.1</b>	Sample MOC review action items	393
<b>18.2</b>	Safety Review staff requirements for the MOC review	393
<b>19.1</b>	Sample HAZOP Study results for the routine operation phase	405
<b>19.2</b>	Sample action items from the routine operation phase	407
<b>19.3</b>	Sample FMEA results for the routine operation phase	407
<b>19.4</b>	HAZOP Study staff requirements for the routine operation phase	408
<b>20.1</b>	PVC reactor/site information	414
<b>20.2</b>	Relative Ranking results for the plant expansion phase	415

**Table**

<b>20.3</b>	PVC batch reactor operating procedure	416
<b>20.4</b>	Sample HAZOP Study results for the PVC reactor	422
<b>20.5</b>	Sample recommendations from the HAZOP Study of the PVC batch reactor	423
<b>20.6</b>	Relative Ranking staff requirements for the plant expansion phase	425
<b>20.7</b>	PVC batch reactor HAZOP Study staff requirements for the plant expansion phase	425
<b>21.1</b>	Sample results from the incident investigation FMEA	448
<b>21.2</b>	Minimal cut sets for the incident investigation HRA event tree	449
<b>21.3</b>	FMEA staff requirements for the incident investigation	450
<b>22.1</b>	Sample decommissioning checklist	452
<b>22.2</b>	Sample recommendations from the furnace decommissioning What-If/Checklist Analysis	459
<b>22.3</b>	Decommissioning What-If/Checklist Analysis staff requirements	460
<b>A1.1</b>	Example What-If checklist used in evaluating hazards of facility/operational changes	464
<b>A2.1</b>	Management of change hazard review form	466
<b>A3.1</b>	Example reactivity checklist	469
<b>C.1</b>	Abbreviations used in example problem drawings	519
<b>D.1</b>	Hazard evaluation software aids	521
<b>E.1</b>	Not dangerously reactive exceptions	525
<b>F.1</b>	Professional and industry organizations offering process safety enhancement resources	529

# List of Figures

**Overview** Interrelation of book chapters

9

## Figure

1.1	Aspects of understanding risk	18
1.2	Anatomy of a catastrophic incident	21
1.3	Basic incident sequence without safeguards	21
1.4	Identifying the initiating cause and the loss event in an incident scenario	22
1.5	Preventive and mitigative safeguards come into play after an initiating cause	23
1.6	Generic “bow-tie” diagram showing relation of safeguards to loss event	24
1.7	Emergency cooling system schematic	26
2.1	Information available for hazard review	39
3.1	Adverse consequences associated with process hazards	52
3.2	Typical interaction matrix	57
3.3	NOAA Worksheet compatibility chart display	59
3.4	Implementation of inherently safer design within a process risk management system	65
4.1	DAP process schematic for the Checklist Analysis example	97
5.1	Schematic for the chlorine feed line example	110
5.2	Example of a simplified checklist for hazard evaluation	111
5.3	Overview of the HAZOP Study technique	121
5.4	HAZOP Study method flow diagram	124
5.5	DAP process schematic for the HAZOP Study example	131
5.6	DAP process schematic for the FMEA example	139
5.7	Example fault tree structure	148
5.8	Sample fault tree with gates and basic events identified	149
5.9	Matrix for resolving gates of the sample fault tree	151
5.10	Emergency cooling system schematic for the Fault Tree Analysis example	153
5.11	Development of the Top event for the emergency cooling system example	154
5.12	Development of the first two intermediate events	155
5.13	Completed fault tree for the emergency cooling system example	156
5.14	First step in constructing an event tree	160
5.15	Developing the first safeguard in the sample event tree	161
5.16	Developing the second safeguard in the sample event tree	162
5.17	Developing the third safeguard in the sample event tree	163
5.18	Example of an incident sequence fault tree	164
5.19	Event tree for the initiating cause “loss of cooling water to the oxidation reactor”	166
5.20	Branch point symbol used in Cause-Consequence Analysis	169
5.21	Consequence symbol used in Cause-Consequence Analysis	169
5.22	Cause-consequence diagram for “loss of cooling water to the oxidation reactor”	170
5.23	Generic “bow-tie” diagram	172

**Figure**

6.1	Typical uses for hazard evaluation techniques	180
6.2	Criteria for selecting hazard evaluation techniques	187
6.3	Example flowchart for selecting a hazard evaluation technique	188
7.1	Summary of commonly used approaches to identifying incident scenarios	213
7.2	Preventive and mitigative safeguards	218
7.3	Example risk matrix using order-of-magnitude frequency and severity categories	222
8.1	Example risk matrix	244
9.1	Typical usage of procedure-based techniques at some facilities	263
9.2	Illustration for case study	266
9.3	Example HRA event tree structure	284
9.4	HRA event tree for the operator response to an alarm example	286
11.1	Schematic of the example VCM manufacturing process	307
12.1	Interaction matrix for VCM process materials	312
13.1	VCM process block diagram	316
14.1	VCM plant layout	328
15.1	VCM pilot plant P&ID	340
16.1	VCM plant incinerator P&ID	366
16.2	Example event tree for the VCM plant — generic process upset initiating cause	370
16.3	Example event tree for the VCM plant — low fuel gas pressure initiating cause	371
16.4	Preliminary fault tree developed for the incinerator shutdown system	372
16.5	Final fault tree for the incinerator shutdown system	374
16.6	Fault tree for incident scenario 1-7—explosion	375
17.1	Schematic of the HCl storage tank	382
19.1	Revised incinerator P&ID	396
20.1	VCM plant layout — PVC siting alternatives	410
20.2	PVC batch reactor P&ID	412
20.3	F&EI calculations for low-pressure PVC reactor site #1	426
20.4	Radius of exposure calculations for low-pressure PVC reactor site #1	427
20.5	F&EI calculations for high-pressure PVC reactor site #1	428
20.6	Radius of exposure calculations for high-pressure PVC reactor site #1	429
20.7	F&EI calculations for low-pressure PVC reactor site #2	430
20.8	Radius of exposure calculations for low-pressure PVC reactor site #2	431
20.9	F&EI calculations for high-pressure PVC reactor site #2	432
20.10	Radius of exposure calculations for high-pressure PVC reactor site #2	433
20.11	PVC unit block diagram	434
21.1	HCl column P&ID	436
21.2	HRA event tree for loss of overhead condensing	446
22.1	Process flow diagram for the VCM furnace area	453
A3.1	Instructions for use of example reactivity checklist	468
C.1	Symbols used in example problem drawings	520
E.1	Cargo compatibility chart from <i>CHRIS Manual</i>	524

## Abbreviations and Acronyms

<b>ACC</b>	American Chemistry Council
<b>ACGIH</b>	American Conference of Government and Industrial Hygienists
<b>AEGL</b>	Acute Exposure Guideline Level
<b>AIChE</b>	American Institute of Chemical Engineers
<b>AIHA</b>	American Industrial Hygiene Association
<b>ALARP</b>	As low as reasonably practicable
<b>ANSI</b>	American National Standards Institute
<b>API</b>	American Petroleum Institute
<b>ARC®</b>	Accelerating Rate Calorimeter; accelerating rate calorimetry
<b>ASME</b>	American Society of Mechanical Engineers
<b>ASSE</b>	American Society of Safety Engineers
<b>BLEVE</b>	Boiling liquid expanding vapor explosion
<b>BPCS</b>	Basic process control system
<b>CCA</b>	Cause-Consequence Analysis
<b>CCF</b>	Common cause failure
<b>CCPS</b>	AIChE Center for Chemical Process Safety
<b>CEI</b>	Chemical Exposure Index
<b>CHAZOP</b>	Chemistry HAZOP <i>or</i> Computer HAZOP
<b>CPI</b>	Chemical process industry
<b>CPQRA</b>	Chemical Process Quantitative Risk Analysis
<b>CSB</b>	U.S. Chemical Safety and Hazard Investigation Board
<b>DAP</b>	Diammonium phosphate
<b>DIERS</b>	AIChE Design Institute for Emergency Relief Systems
<b>DIPPR</b>	AIChE Design Institute for Physical Property Data
<b>EHS</b>	Environmental, health and safety
<b>EPA</b>	U.S. Environmental Protection Agency
<b>ERPG</b>	Emergency Response Planning Guideline
<b>ETA</b>	Event Tree Analysis
<b>F&amp;EI</b>	Fire and Explosion Index
<b>FMEA</b>	Failure Modes and Effects Analysis
<b>FMECA</b>	Failure Modes, Effects, and Criticality Analysis
<b>FTA</b>	Fault Tree Analysis
<b>HAZOP</b>	Hazard and Operability Study [ <i>or</i> Analysis]
<b>HE</b>	Hazard evaluation
<b>HEP</b>	Hazard evaluation procedures
<b>HEP3</b>	<i>Guidelines for Hazard Evaluation Procedures, 3<sup>rd</sup> Edition</i>
<b>HRA</b>	Human Reliability Analysis

<b>IChemE</b>	Institution of Chemical Engineers (United Kingdom)
<b>ICI</b>	Imperial Chemical Industries
<b>IEC</b>	International Electrotechnical Commission
<b>ISA</b>	The Instrumentation, Systems, and Automation Society
<b>IDLH</b>	Immediately dangerous to life and health
<b>IPL</b>	Independent protection layer
<b>LC<sub>Lo</sub></b>	Lethal concentration low
<b>LD<sub>50</sub></b>	Lethal dose, 50% mortality
<b>LEL</b>	Lower explosive limit
<b>LFL</b>	Lower flammable limit
<b>LOPA</b>	Layer of Protection Analysis
<b>MCS</b>	Minimal cut set
<b>MSDS</b>	Material safety data sheet
<b>MORT</b>	Management Oversight and Risk Tree
<b>NFPA</b>	National Fire Protection Association
<b>OSHA</b>	U.S. Occupational Safety and Health Administration
<b>PEL</b>	Permissible exposure limit
<b>PFD</b>	Process flow diagram <i>or</i> Probability of failure on demand
<b>P&amp;ID</b>	Piping and instrumentation diagram
<b>PHA</b>	Process hazard analysis <sup>1</sup>
<b>PreHA</b>	Preliminary Hazard Analysis <sup>1</sup>
<b>PSF</b>	Performance shaping factor
<b>PSM</b>	Process safety management
<b>R&amp;D</b>	Research and development
<b>SCBA</b>	Self-contained breathing apparatus
<b>SHI</b>	Substance Hazard Index
<b>SIF</b>	Safety instrumented function
<b>SIL</b>	Safety integrity level
<b>SIS</b>	Safety instrumented system
<b>SOP</b>	Standard operating procedure
<b>STEL</b>	Short term exposure limit; 15 min time-weighted-average maximum concentration
<b>TLV<sup>®</sup></b>	Threshold Limit Value; occupational exposure limit recommended by ACGIH
<b>UEL</b>	Upper explosive limit
<b>UFL</b>	Upper flammable limit
<b>VPP</b>	[OSHA] Voluntary Protection Program
<b>VSP2<sup>™</sup></b>	Vent Sizing Package, Version 2
<b>WI</b>	What-If [Analysis]
<b>WI/CL</b>	What-If/Checklist [Analysis]

---

<sup>1</sup> The first and second editions of these *Guidelines* used the abbreviation “PHA” for Preliminary Hazard Analysis; however, use of this abbreviation has been changed to PreHA to avoid confusion with the now more common term Process Hazard Analysis which is associated with the acronym PHA.

## Glossary

See Part I, Sections 1.3 (Anatomy of an Incident) and 1.4 (The Role of Safeguards) to understand how some of the Glossary terms fit together in the context of hazard evaluation procedures.

***Abnormal situation:*** A disturbance in an industrial process with which the basic process control system of the process cannot cope. In the context of hazard evaluation procedures, synonymous with *deviation*.

***Acute hazard:*** The potential for injury or damage to occur as a result of an instantaneous or short duration exposure to the effects of an incident.

***Administrative control:*** A procedural requirement for directing and/or checking engineered systems or human performance associated with plant operations.

***ALARP:*** As low as reasonably practicable; the concept that efforts to reduce risk should be continued until the incremental sacrifice (in terms of cost, time, effort, or other expenditure of resources) is grossly disproportionate to the incremental risk reduction achieved. The term *as low as reasonably achievable* (ALARA) is often used synonymously.

***Audit (process safety audit):*** An inspection of a plant or process unit, drawings, procedures, emergency plans, and/or management systems, etc., usually by an independent, impartial team. (See “Safety Review” for contrast.)

***Autoignition temperature:*** The lowest temperature at which a fuel/oxidant mixture will spontaneously ignite under specified test conditions.

***Basic event:*** An event in a fault tree that represents the lowest level of resolution in the model such that no further development is necessary (e.g., equipment item failure, human failure, or external event).

***Basic process control system (BPCS):*** A system that responds to input signals from the process and its associated equipment, other programmable systems, and/or from an operator, and generates output signals causing the process and its associated equipment to operate in the desired manner and within normal production limits.

***Branch point:*** A node with two paths in an event tree or cause-consequence diagram. One path represents success of a safeguard and the other path represents failure of the safeguard.

***Cause:*** In the context of hazard evaluation procedures, an *initiating cause*.

***Cause-Consequence Analysis:*** A method for illustrating the possible outcomes arising from the logical combination of selected input events or states. A combination of fault tree and event tree models.

**Checklist (traditional):** A detailed list of desired system attributes or steps for a system or operator to perform. Usually written from experience and used to assess the acceptability or status of the system or operation compared to established norms.

**Chronic hazard:** The potential for injury or damage to occur as a result of prolonged exposure to an undesirable condition.

**Common cause failure:** The occurrence of two or more failures that result from a single event or circumstance.

**Consequence:** Result of a specific event. In the context of qualitative hazard evaluation procedures, the *consequences* are the effects following from the initiating cause, with the consequence description taken through to the loss event and sometimes to the loss event impacts. In the context of quantitative risk analyses, the *consequence* refers to the physical effects of the loss event usually involving a fire, explosion, or release of toxic or corrosive material.

**Consequence analysis:** The analysis of the effects of incident outcome cases independent of frequency or probability.

**CPQRA:** The abbreviation for Chemical Process Quantitative Risk Analysis. The process of hazard identification, followed by numerical evaluation of incident consequences and frequencies, and their combination into an overall measure of risk when applied to the chemical process industry. Ordinarily applied to episodic events. Related to Probabilistic Risk Assessment (PRA) used in the nuclear industry.

**Deviation:** A process condition outside of established design limits, safe operating limits, or standard operating procedures.

**Dow Chemical Exposure Index (CEI):** A method, developed by The Dow Chemical Company, used to identify and rank the relative acute health hazards associated with potential chemical releases. The CEI is calculated from five factors: a measure of toxicity; the quantity of volatile material available for a release; the distance to each area of concern; the molecular weight of the material being evaluated; and process variables that can affect the conditions of a release such as temperature, pressure, and reactivity.

**Dow Fire and Explosion Index (F&EI):** A method, developed by The Dow Chemical Company, for ranking the relative potential fire and explosion effect radius and property damage / business interruption impacts associated with a process. Analysts calculate various hazard and exposure factors using material characteristics and process data.

**Emergency response planning guidelines (ERPG):** A system of guidelines for airborne concentrations of toxic materials prepared by the AIHA. For example, ERPG-2 is the maximum airborne concentration below which it is believed nearly all individuals could be exposed for up to one hour without experiencing or developing irreversible or other serious health effects or symptoms that could impair an individual's ability to take protective action.



**Engineered control:** A specific hardware or software system designed to maintain a process within safe operating limits, to safely shut it down in the event of a process upset, or to reduce human exposure to the effects of an upset.

**Episodic event:** An unplanned event of limited duration, usually associated with an incident.

**Episodic release:** A release of limited duration, usually associated with an incident.

**Error-likely situation:** A work situation in which the performance-shaping factors are not compatible with the capabilities, limitations, or needs of the worker. In such situations, workers are much more likely to make errors, particularly under stressful conditions.

**Event:** An occurrence involving the process caused by equipment performance or human action or by an occurrence external to the process.

**Event sequence:** See *Incident sequence*.

**Event tree:** A logic model that graphically portrays the combinations of events and circumstances in an incident sequence.

**External event:** Event external to the system caused by (1) a natural hazard — earthquake, flood, tornado, extreme temperature, lightning, etc., or (2) a human-induced event — aircraft crash, missile, nearby industrial activity, fire, sabotage, etc.

**Failure:** Cessation of equipment to operate as specified.

**Failure mode:** A symptom or condition by which a failure is observed. A failure mode might be identified as loss of function; premature function (function without demand); an out-of-tolerance condition; or a simple physical characteristic such as a leak observed during inspection.

**Failure Modes and Effects Analysis (FMEA):** A systematic, tabular method for evaluating and documenting the effects of known types of component failures.

**Failure Modes, Effects, and Criticality Analysis (FMECA):** A variation of FMEA that includes a quantitative estimate of the severity of consequence of a failure mode.

**Fault event:** A failure event in a fault tree that requires further development.

**Fault tree:** A logic model that graphically portrays the combinations of failures that can lead to a specific main failure or incident of interest (Top event).

**Frequency:** Number of occurrences of an event per unit time (e.g., 1 event in 1000 yr =  $1 \times 10^{-3}$  events/yr).

**Hazard:** A physical or chemical condition that has the potential for causing harm to people, property, or the environment.

**Hazard analysis:** See *Hazard evaluation*.

**Hazard and Operability (HAZOP) Study:** A scenario-based hazard evaluation procedure in which a team uses a series of guide words to identify possible deviations from the intended design or operation of a process, then examines the potential consequences of the deviations and the adequacy of existing safeguards.

**Hazard checklist:** An experience-based list of hazards, potential incident situations, or other process safety concerns used to stimulate the identification of hazardous situations for a process or operation.

**Hazard evaluation:** Identification of individual hazards of a system, determination of the mechanisms by which they could give rise to undesired events, and evaluation of the consequences of these events on health (including public health), environment, and property. Uses qualitative techniques to pinpoint weaknesses in the design and operation of facilities that could lead to incidents.

**Hazard identification:** The pinpointing of material, system, process, and plant characteristics that can produce undesirable consequences through the occurrence of an incident.

**Hazardous event:** See *Loss event*.

**Human error:** Any human action (or lack thereof) that exceeds some limit of acceptability (i.e., an out-of-tolerance action) where the limits of human performance are defined by the system. Includes actions by designers, operators, or managers that may contribute to or result in incidents.

**Human factors:** A discipline concerned with designing machines, operations, and work environments to match human capabilities, limitations, and needs.

**Human Reliability Analysis (HRA):** A method used to evaluate whether necessary human actions, tasks, or jobs will be completed successfully within a required time period. In these *Guidelines*, HRA is used strictly in a qualitative context. HRA is also used to determine the probability that no extraneous human actions detrimental to the system will be performed.

**HRA event tree:** A graphical model of sequential events in which the tree limbs designate human actions and other events as well as different conditions or influences upon these events.

**Impact:** A measure of the ultimate loss and harm of a loss event. *Impact* may be expressed in terms of numbers of injuries and/or fatalities, extent of environmental damage, and/or magnitude of losses such as property damage, material loss, lost production, market share loss, and recovery costs.

**Incident:** An unplanned event or sequence of events that either resulted in or had the potential to result in adverse impacts.

**Incident sequence:** A series of events composed of an initiating cause and intermediate events leading to an undesirable outcome.

**Initiating cause:** In the context of hazard evaluation procedures, the operational error, mechanical failure, or external event or agency that is the first event in an incident sequence and marks the transition from a normal situation to an abnormal situation. Synonymous with *initiating event*.

**Initiating event:** See *Initiating cause*.

**Intermediate event:** An event that occurs after the initiating cause and before the loss event in an incident sequence.

**Layer of protection:** A physical entity supported by a management system that is capable of preventing an initiating cause from propagating to a specific loss event or impact.

**Layer of Protection Analysis (LOPA):** An approach that analyzes one incident scenario (cause-consequence pair) at a time, using predefined values for the initiating cause frequency, independent protection layer failure probabilities, and consequence severity, in order to compare an order-of-magnitude scenario risk estimate to tolerable risk goals for determining where additional risk reduction or more detailed analysis is needed. Scenarios are identified elsewhere, typically using a scenario-based hazard evaluation procedure such as a HAZOP Study.

**Likelihood:** A measure of the expected probability or frequency of occurrence of an event.

**Loss event:** Point of time in an abnormal situation when an irreversible physical event occurs that has the potential for loss and harm impacts. Examples include release of a hazardous material, ignition of flammable vapors or ignitable dust cloud, and overpressurization rupture of a tank or vessel. An incident might involve more than one loss event, such as a flammable liquid spill (first loss event) followed by ignition of a flash fire and pool fire (second loss event) that heats up an adjacent vessel and its contents to the point of rupture (third loss event). Generally synonymous with *hazardous event*.

**Minimal cut set:** A combination of failures and conditions necessary and sufficient to cause the occurrence of the Top event in a fault tree.

**Mitigate:** Reduce the impact of a loss event.

**Mitigative safeguard:** A safeguard that is designed to reduce loss event impact.

**Operator:** An individual responsible for monitoring, controlling, and performing tasks as necessary to accomplish the productive activities of a system. Often used in a generic sense to include people who perform all kinds of tasks (e.g., reading, calibration, maintenance).

**Passive equipment:** Hardware that is not physically actuated in order to perform its function, such as secondary containment or a blast wall.

**Performance shaping factor (PSF):** Any factor that influences human performance. PSFs include factors intrinsic to an individual (personality, skill, etc.) and factors in the work situation (task demands, plant policies, hardware design, training, etc.).

**Process safety management:** A program or activity involving the application of management principles and analytical techniques to ensure the safety of process facilities. Sometimes called **process hazard management**.

**Preventive safeguard:** A safeguard that forestalls the occurrence of a particular loss event, given that an initiating cause has occurred; i.e., a safeguard that intervenes between an initiating cause and a loss event in an incident sequence. (Note that *containment and control measures* are also preventive in the sense of preventing initiating causes from occurring; however, the term *preventive safeguard* in the context of hazard evaluation procedures is used with the specific meaning given here.)

**Quantitative risk analysis:** The systematic development of numerical estimates of the expected frequency and severity of potential incidents associated with a facility or operation based on engineering evaluation and mathematical techniques.

**Rare event:** An event or incident whose expected frequency is very small. The event is not statistically expected to occur during the normal life of a facility or operation.

**Recovery factors:** Feedback factors that limit or prevent the undesirable consequences of a human error.

**Risk:** The combination of the expected frequency (events/year) and severity (effects/event) of a single incident or a group of incidents.

**Risk assessment:** The process by which the results of a risk analysis (i.e., risk estimates) are used to make decisions, either through relative ranking of risk reduction strategies or through comparison with risk targets.

**Risk management:** The systematic application of management policies, procedures, and practices to the tasks of analyzing, assessing, and controlling risk in order to protect employees, the general public, the environment, and company assets.

**Risk measures:** Ways of combining and expressing information on likelihood with the magnitude of loss or injury (e.g., risk indexes, individual risk measures, and societal risk measures).

**Safeguard:** Any device, system, or action that would likely interrupt the chain of events following an initiating cause or that would mitigate loss event impacts. See **Preventive safeguard**; **Mitigative safeguard**.

**Safety Review:** An inspection of a plant or process unit, drawings, procedures, emergency plans, and/or management systems, etc., usually by a team and usually problem-solving in nature. (See "Audit" for contrast.)

**Safety system:** Equipment and/or procedures designed to limit or terminate an incident sequence, thus mitigating the incident and its consequences.

**Scenario:** An unplanned event or incident sequence that results in a loss event and its associated impacts, including the success or failure of safeguards involved in the incident sequence.

***Scribe/recorder:*** A hazard evaluation team member who is responsible for capturing the significant results of discussions that occur during a hazard evaluation team meeting.

***Source term:*** For a hazardous material and/or energy release to the surroundings associated with a loss event, the release parameters (magnitude, rate, duration, orientation, temperature, etc.) that are the initial conditions for determining the consequences of the loss event. For vapor dispersion modeling, it is the estimation, based on the release specification, of the actual cloud conditions of temperature, aerosol content, density, size, velocity and mass to be input into the dispersion model.

***Task analysis:*** A human error analysis method that requires breaking down a procedure or overall task into unit tasks and combining this information in the form of event trees. It involves determining the detailed performance required of people and equipment and determining the effects of environmental conditions, malfunctions, and other unexpected events on both.

***Top event:*** The loss event or other undesired event at the “top” of a fault tree that is traced downward to more basic failures using Boolean logic gates to determine its possible causes.

***Two Guide Word Analysis:*** A procedure-based hazard evaluation technique, similar to a HAZOP Study, in which the adequacy of existing safeguards is evaluated by asking what would happen if each step in a procedure was (1) skipped or (2) performed incorrectly.

***Undeveloped event:*** An event in a fault tree that is not developed because it is of no significance, because more detailed information is unavailable, or because its frequency or probability can be estimated without determining its basic events.

***What-If Analysis:*** A scenario-based hazard evaluation procedure using a brainstorming approach in which typically a team that includes one or more persons familiar with the subject process asks questions or voices concerns about what could go wrong, what consequences could ensue, and whether the existing safeguards are adequate.

***What-If/Checklist Analysis:*** A What-If Analysis that uses some form of checklist or other listing of broad categories of concern to structure the what-if questioning.

***Worst case:*** A conservative (high) estimate of the consequences of the most severe incident identified.

***Worst credible case:*** The most severe incident considered plausible or reasonably believable.

This Page Intentionally Left Blank