

GUIDELINES FOR INVESTIGATING PROCESS SAFETY INCIDENTS

**PUBLICATIONS AVAILABLE FROM THE
CENTER FOR CHEMICAL PROCESS SAFETY
of the
AMERICAN INSTITUTE OF CHEMICAL ENGINEERS**

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

**GUIDELINES FOR INVESTIGATING
PROCESS SAFETY INCIDENTS
THIRD EDITION**

**CENTER FOR CHEMICAL PROCESS SAFETY
OF THE
AMERICAN INSTITUTE OF CHEMICAL
ENGINEERS
New York, NY**



WILEY

This edition first published 2019

© 2019 the American Institute of Chemical Engineers

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

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 rights of CCPS to be identified as the author of the editorial material in this work have been asserted in accordance with law.

Registered Office

John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA

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 is available.

Hardback ISBN: 9781119529071

Cover Images: Silhouette, oil refinery © manyx31/iStockphoto; Stainless steel © Creativ Studio Heinemann/Getty Images, Inc.; Dow Chemical Operations, Stade, Germany/Courtesy of The Dow Chemical Company

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

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, the American Institute of Chemical Engineers, its consultants, the CCPS Technical Steering Committee and Subcommittee members, their employers, their employers' officers and directors, and Baker Engineering and Risk Consultants, Inc.®, and its employees do not 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 Baker Engineering and Risk Consultants, Inc.®, and its employees and (2) the user of this document, the user accepts any legal liability or responsibility whatsoever for the consequences of its use or misuse.

CONTENTS

PREFACE	XXV
ACKNOWLEDGMENTS	XXVII
ACRONYMS AND ABBREVIATIONS	XXIX
1 INTRODUCTION	1
1.1 Building on the Past	1
1.2 Investigation Basics	2
1.2.1 The First Step	2
1.2.2 The Second Step	4
1.2.3 The Third Step	4
1.2.4 The Fourth step	4
1.2.5 The Fifth Step	5
1.2.6 The Sixth Step	5
1.3 Who Should Read This Book?	5
1.4 The Guideline's Objectives	6
1.5 The Guideline's Content and Organization	6
1.6 The Continuing Evolution of Incident Investigation	11
2 OVERVIEW OF CHEMICAL PROCESS INCIDENT CAUSATION	13
2.1 Stages of a Process-Related Incident	14
2.1.1 Three Phase Model of Process-Related Incidents	14
2.1.2 Event Tree	14
2.1.3 Swiss Cheese Model	16
2.1.4 Importance of Latent Failures	17
2.2 Key Causation Concepts	18

2.2.1	Loss of Containment or Energy	18
2.2.2	Management System Failure	20
2.2.3	Human Factors	21
2.2.4	Multiple Causation	22
2.2.5	Events vs Root Causes	22
2.2.6	Controlling Risk	23
2.3	Summary	24
3	AN OVERVIEW OF INVESTIGATION METHODOLOGIES	26
3.1	History of Investigation Methodologies and Tools	29
3.1.1	One-on-One Interview	29
3.1.2	Brainstorming	29
3.1.3	What If Analysis	30
3.1.4	5-Whys	30
3.1.5	Process of Elimination	31
3.1.6	Timelines	31
3.1.7	Sequence Diagrams	31
3.1.8	Predefined Trees	33
3.2	Tools for Use in Preparation for Root Cause Analysis	34
3.2.1	Timelines	34
3.2.2	Sequence Diagrams	35
3.2.3	Scientific Method	35
3.2.4	Causal Factor Identification	36
3.3	Structured Root Cause Analysis Methodologies	37
3.3.1	Checklists	37
3.3.2	Predefined Trees	38
3.3.3	Team-Developed Logic Trees	39
3.4	Selecting an Appropriate Methodology	43
3.4.1	Methodologies Used by CCPS Members	46
4	DESIGNING AN INCIDENT INVESTIGATION MANAGEMENT SYSTEM	47
4.1	System Considerations	49
4.1.1	An Organization's Responsibilities	49

4.1.2	Workforce Responsibilities	51
4.1.3	Role of the Management System Developers	53
4.1.4	Integration with Other Functions and Teams	54
4.1.5	Involvement by Regulatory Agencies	55
4.2	Typical Management System Topics	58
4.2.1	Classifying Incidents	58
4.2.2	Specifying and Managing Documentation	59
4.2.3	Legal Considerations	60
4.2.4	Describing Team Organization and Functions	63
4.2.5	Electronic Process Data and Control Systems	64
4.2.6	Defining Training Requirements	65
4.2.7	Emphasizing Root Causes	69
4.2.8	Fostering a Blame-Free Policy	70
4.2.9	Developing Recommendations	70
4.2.10	Recommendation Responsibilities	71
4.2.11	Implementing the Recommendations and Follow-up Activities	72
4.2.12	Providing a Template for Formal Reports	73
4.2.13	Management System Review and Approval	73
4.2.14	Planning for Continuous Improvement	73
4.3	Management System	74
4.3.1	Initial Implementation—Training	75
4.3.2	Developing a Specific Investigation Plan	75
5	INITIAL NOTIFICATION, CLASSIFICATION AND INVESTIGATION OF PROCESS SAFETY INCIDENTS	79
5.1	Internal Reporting	79
5.2	Incident Classification	81
5.2.1	Severity Classification	82
5.2.2	Local Jurisdiction	89
5.2.3	Other Options for Establishing Classification Criteria	89
5.3	Incident Notification	90
5.3.1	Corporate Notification	90
5.3.2	Agency Notification	91

5.3.3	Other Stakeholder Notification	91
5.3.4	Other Notifications	92
5.4	Type of Investigation	92
5.4.1	Which Investigation System to Use?	92
5.4.2	Investigation Approach	93
5.5	Summary	94
6	BUILDING AND LEADING AN INCIDENT INVESTIGATION TEAM	96
6.1	Team Approach	96
6.2	Advantages of the Team Approach	97
6.3	Leading a Process Safety Incident Investigation Team	98
6.4	Potential Team Composition	100
6.5	Building a Team for a Specific Incident	104
6.5.1	Composition and Size of Investigation Team	104
6.6	Team Activities	106
6.7	Summary	108
7	WITNESS MANAGEMENT	110
7.1	Overview	110
7.1.1	Witness Issues Following a Major Occurrence	111
7.1.2	Investigation Team Priorities for Managing Witnesses	112
7.2	Identifying Witnesses	113
7.3	Witness Interviews	115
7.3.1	Human Factors Related to Interviews	115
7.3.2	Collecting Information from Witnesses	118
7.3.3	Initial Witness Statements	120
7.3.4	Conducting the Interview	121
7.4	Conducting Follow-up Activities	134
7.5	Conducting Follow-up Interviews	135
7.6	Reliability of Witness Statements	135
7.7	Summary	135

8	EVIDENCE IDENTIFICATION, COLLECTION AND MANAGEMENT	137
8.1	Overview	137
8.1.1	Developing a Specific Plan	138
8.1.2	Investigation Environment Following a Major Occurrence	139
8.1.3	Priorities for Managing an Incident Investigation Team	141
8.2	Sources of Evidence	144
8.2.1	Types of Sources	144
8.2.2	Physical Evidence and Data	147
8.2.3	Paper Evidence and Data	149
8.2.4	Electronic Evidence and Data	152
8.2.5	Position Evidence and Data	153
8.3	Evidence Gathering	156
8.3.1	Initial Site Visit	157
8.3.2	Identifying and Documenting Evidence	159
8.3.3	Tools and Supplies	162
8.3.4	Photography and Video	164
8.4	Timelines and Sequence Diagrams	168
8.4.1	Constructing a Timeline	168
8.4.2	Constructing a Sequence Diagram	174
8.5	Summary	176
9	EVIDENCE ANALYSIS AND CAUSAL FACTOR DETERMINATION	178
9.1	Scientific Method	178
9.2	Confirmation Bias	181
9.3	Evidence Analysis	181
9.3.1	Data Organization - Timelines	182
9.3.2	Use of Protocols	182
9.3.3	Mechanical Failure Analysis	184
9.3.4	Advanced Data Systems	187
9.4	Hypothesis Formulation	187
9.4.1	Fact/Hypothesis Matrix	188
9.5	Hypothesis Testing	190
9.5.1	Engineering Analysis	190

9.5.2	Computational Modeling	191
9.5.3	Reconstruction	191
9.5.4	Test the Items under Simulated Conditions	192
9.5.5	Testing of Human Input/Performance	192
9.6	Select the Final Hypothesis	193
9.6.1	Causal Factor Identification	193
9.6.2	Causal Factor Charting	198
9.6.3	Developing a Causal Factor Chart	200
9.7	Summary	202
10	DETERMINING ROOT CAUSES—STRUCTURED APPROACHES	203
10.1	Concept of Root Cause Analysis	203
10.2	Case Histories	206
10.3	Methodologies for Root Cause Analysis	208
10.3.1	5 Whys Technique	208
10.3.2	Structured Root Cause Determination	212
10.4	Root Cause Determination Using Logic Trees	214
10.4.1	Gather Evidence and List Facts	215
10.4.2	Timeline Development	215
10.4.3	Logic Tree Development	215
10.5	Building a Logic Tree	219
10.5.1	Choosing the Top Event	220
10.5.2	Logic Tree Basics	220
10.5.3	Example—Chemical Spray Injury	228
10.5.4	What to Do if the Process Stalls	232
10.5.5	Guidelines for Stopping Tree Development	232
10.6	Example Applications	235
10.6.1	Fire and Explosion Incident—Fault Tree	235
10.6.2	Data-Driven Cause Analysis	239
10.6.3	Logic Tree Summary	241
10.7	Root Cause Determination Using Predefined Trees	242
10.7.1	Scenario Determination	244
10.7.2	Causal Factors	244
10.7.3	Predefined Tree	245

10.8	Using Predefined Trees	246
10.8.1	Predefined Tree Methodology	247
10.8.2	Example—Environmental Incident	248
10.8.2	Quality Assurance	255
10.8.3	Predefined Tree Summary	255
10.9	Checklists	256
10.9.1	Use of Checklists	257
10.9.2	Checklist Summary	258
10.10	Human Factors Applications	258
10.11	Summary	259
11	THE IMPACT OF HUMAN FACTORS	261
11.1	Human Factors Concepts	262
11.2	Incorporating Human Factors into the Incident Investigation Process	267
11.2.1	Human Factors Before and During the Incident	268
11.2.2	Human Factors during the Causal Analysis	269
11.2.3	Human Factors in Developing Recommendations	275
11.2.4	After the Investigation	275
11.3	Other References	276
11.4	Summary	276
12	DEVELOPING EFFECTIVE RECOMMENDATIONS	278
12.1	Key Concepts	278
12.2	Developing Effective Recommendations	280
12.2.1	Team Responsibilities	280
12.2.2	Attributes of Good Recommendations	280
12.3	Types of Recommendations	283
12.3.1	Inherently Safer Design	284
12.3.2	Layers of Protection	285
12.3.3	Commendation/Disciplinary Action	289
12.3.4	The “Further Action Required” Recommendation	289
12.4	The Recommendation Process	290
12.4.1	Select Each Cause	290

12.4.2	Perform a Completeness Test	290
12.4.3	Assessing the Effectiveness	291
12.4.4	Prepare to Present Recommendations	291
12.4.5	Review Recommendations with Management	293
12.4.6	Tracking and Closure of Recommendations	293
12.5	Summary	294
13	PREPARING THE FINAL REPORT	295
13.1	Report Scope	295
13.2	Interim Reports	296
13.3	Writing the Report	297
13.4	Sample Report Format	299
13.4.1	Executive Summary	300
13.4.2	Introduction	301
13.4.3	Background	301
13.4.4	Sequence of Events and Description of the Incident	302
13.4.5	Findings	302
13.4.6	Causal Factors	303
13.4.7	Root Causes	304
13.4.8	Recommendations	304
13.4.9	Noncontributory Factors	306
13.4.10	Attachments or Appendices	306
13.5	Report Review and Quality Assurance	307
13.5.1	Reviewing the Report	307
13.5.2	Avoiding Common Mistakes	308
13.6	Investigation Document and Evidence Retention	310
13.7	Summary	311
14	IMPLEMENTING RECOMMENDATIONS	314
14.1	Activities Related to Recommendation Implementation	315
14.2	Validation of Effectiveness – Case Studies	317
14.2.1	Nuclear Plant Incident	317
14.2.2	Aircraft Incident	318
14.2.3	Petrochemical Plant Incident	318
14.2.4	Challenger Space Shuttle Incident	318

14.2.5	Typical Plant Incidents	319
14.3	Practical Suggestions for Successful Recommendation Implementation	319
14.3.1	Assigning a Responsible Individual	320
14.3.2	Due Dates and Priorities to Implement Recommendations	320
14.3.3	Challenges to Resolving Recommendations	321
14.3.4	Tracking Action Items	323
14.3.5	Follow-up Verification	323
15	CONTINUOUS IMPROVEMENT FOR THE INCIDENT INVESTIGATION SYSTEM	326
15.1	Regulatory Compliance Review	327
15.2	Investigation Quality Assessment	329
15.3	Causal Category Analysis	331
15.4	Review of Near-Miss Events	334
15.5	Recommendations Review	334
15.6	Investigation Follow-up Review	336
15.7	Key Performance Indicators	337
15.8	Summary	338
16	LESSONS LEARNED	340
16.1	Various Sources of Learning from Incidents	341
16.1.1	Internal Sources	341
16.1.2	External Sources	341
16.1.3	Cross-Industry	343
16.2	Identifying Learning Opportunities	343
16.3	Sharing and Institutionalizing Lessons Learned	345
16.4	Senior Management – Incident Sharing and Commitment	347
16.5	Examples of Sharing Lessons Learned	348
16.5.1	Creating a Process Safety Alert from a Case Study	348
16.5.2	Safety Newsletter	350
16.5.3	Videos of Incidents	355
16.5.4	Detailed Incident Reports and Databases	355
16.6	Summary	355

APPENDIX A. PHOTOGRAPHY GUIDELINES FOR MAXIMUM RESULTS	357
APPENDIX B. EXAMPLE PROTOCOL – CHECKING POSITION OF A CHAIN VALVE	362
APPENDIX C. PROCESS SAFETY EVENTS LEVELING CRITERIA	366
APPENDIX D. EXAMPLE CASE STUDY	368
APPENDIX E. QUICK CHECKLIST FOR INVESTIGATORS	398
APPENDIX F. EVIDENCE PRESERVATION CHECKLIST – PRIOR TO ARRIVAL OF THE INVESTIGATION TEAM	404
APPENDIX G. GUIDANCE ON CLASSIFYING POTENTIAL SEVERITY OF A LOSS OF PRIMARY CONTAINMENT	406
GLOSSARY	416
REFERENCES	427
INDEX	437

LIST OF FIGURES

Figure 2.1	Event Tree for a Process-related Incident	15
Figure 2.2	Swiss Cheese Model	16
Figure 2.3	Latent (hidden) Failure	17
Figure 2.4	Incident Prevention Strategies	19
Figure 2.5	Universal Concept for Controlling Risk	23
Figure 3.1	Overview of Investigation Tools	28
Figure 3.2	Schematic of an MES display	32
Figure 3.3	Top Portion of the Generic MORT Tree	34
Figure 3.4	Common Features of Investigation Methodologies	45
Figure 4.1	Management System for Process Safety Investigation	48
Figure 4.2	Checklist for Developing an Incident Investigation Plan	76
Figure 5.1	Logic Tree for Determining Incident Classification	87
Figure 5.2	Example Risk Matrix for Determining Incident Classification	88
Figure 6.1	Investigation Team Collaboration	107
Figure 7.1	Iteration between Witness and Physical Evidence Collection and Analysis	111
Figure 7.2	List of Potential Witnesses	114
Figure 7.3	Illustration of Human Observation Limitations	116
Figure 7.4	Overview of Interview Process	122
Figure 8.1	Iteration between Data Analysis and Data Gathering	138
Figure 8.2	Forms of Data Fragility	145
Figure 8.3	As-found Position of Valves—Example Photo	155
Figure 8.4	Initial Site Visit—Example Photo	157
Figure 8.5	Timeline Example Based on Precise Data	169
Figure 8.6	Timeline Example Based on Approximate Data	170

Figure 8.7 Timeline Example Based on a Combination of Precise and Approximate Data	172
Figure 8.8 Timeline Tips	173
Figure 8.9 Sequence Diagram for Tank Overflow Example	176
Figure 9.1 Scientific Method Process	179
Figure 9.2 Basic Steps in Failure Analysis	184
Figure 9.3 Rules for Causal Factor Charting	201
Figure 9.4 Example of a Causal Factor Chart	202
Figure 10.1 Example of 5 Whys Root Cause Analysis	209
Figure 10.2 Example of Ishikawa Fishbone Diagram	210
Figure 10.3 Structured Root Cause Methods Described in This Chapter	213
Figure 10.4 Flowchart for Root Cause Determination Using Logic Trees	214
Figure 10.5 Generic Logic Tree Displaying the AND-Gate	221
Figure 10.6 Generic Logic Tree for a Fire	221
Figure 10.7 Generic Logic Tree Displaying the OR-Gate	222
Figure 10.8 Logic Tree using the OR-Gate to establish an Ignition Source	222
Figure 10.9 Other Symbols Used in Logic Trees	224
Figure 10.10 Logic Tree Tips	224
Figure 10.11 Example Top of the Logic Tree, Employee Slip	225
Figure 10.12 Example Logic Tree Branch Level, Oil Spill	225
Figure 10.13 Example Logic Tree, Hand-carried Containers	226
Figure 10.14 Logic Tree, Slip/Trip/Fall Incident	227
Figure 10.15 Logic Tree Top, Employee Burn	228
Figure 10.16 Logic Tree Branch, Acid Spray	229
Figure 10.17 Expanded Logic Tree Sample, Employee Burn	230
Figure 10.18 Operator Fatality Branch	236
Figure 10.19 Fire Branch	236
Figure 10.20 Fact/Hypothesis Matrix for the Kettle Exit Piping Failure	237
Figure 10.21 Exit Piping Crack Branch	238
Figure 10.22 Flowchart for Root Cause Determination—Predefined Tree/Checklist	243
Figure 10.23 Example of Root Causes Arranged Hierarchically within a Section of a Predefined Tree	246

Figure 10.24 Incident Sequence	249
Figure 10.25 Complete Causal Factor Chart for Fish Kill Incident	250
Figure 10.26 Top of the Predefined Tree	251
Figure 10.27 First Question of the Human Performance Difficulty Category	252
Figure 10.28 Human Engineering Branch of the Tree	253
Figure 10.29 Analysis of the Human Engineering Branch	254
Figure 11.1 Common Human Factors Model	263
Figure 11.2 Example of Poor Pump and Switch Arrangement	264
Figure 11.3 Incident Causation Model	272
Figure 12.1 Incident Investigation Recommendation Flowchart	279
Figure 12.2 Layers of Safety	287
Figure 12.3 Bow-Tie Barrier Method	288
Figure 12.4 Example Recommendations and Assessment Strategies	292
Figure 14.1 Flowchart for Implementation and Follow-up	316
Figure 16.1 Example Safety Alert	349
Figure 16.2 CCPS Process Safety Beacon	350
Figure 16.3 ICI Safety Newsletter No. 96/1 & 2	351
Figure 16.4 ICI Safety Newsletter No. 96/7	352
Figure 16.5 Learning Event Report Example	353
Figure 16.6 Process Safety Bulletin Example	354

LIST OF TABLES

Table 2.1	Attributes of a Management System	21
Table 3.1	Some Characteristics of Selected Public Methodologies	44
Table 4.1	Suggested Training for Effective Implementation	66
Table 5.1	Common Classification Schemes	82
Table 5.2	Tier 1 Process Safety Event Severity Categories	84
Table 5.3	Example of Likelihood Levels for Determining Incident Classification	89
Table 5.4	Examples of the Impacts of a 1000-lb Cyclohexane Release	93
Table 7.1	Example Questions for Witnesses and Emergency Responders	128
Table 8.1	Scene Activities and Typical Responsibilities	142
Table 8.2	Examples of Paper Evidence	151
Table 8.3	Examples of Electronic Data	153
Table 8.4	Examples of Position Data	154
Table 8.5	Example Data Collection Form for Recording Physical Evidence	161
Table 9.1	Example Fact/Hypothesis Matrix – Chemical Reduction Explosion	189
Table 10.1	Strengths and Weaknesses of the 5 Whys Technique	211
Table 10.2	Strengths and Weaknesses of Logic Trees	242
Table 10.3	Strengths and Weaknesses of Predefined Trees	256
Table 11.1	Human Factors Issues	273
Table 13.1	Sample Sections of an Incident Investigation Report	300
Table 13.2	Findings, Causal Factors, Root Causes and Recommendations	305
Table 13.3	Example Checklist for Written Reports	308
Table 15.1	Requirement Compliance Checklist	327
Table 15.2	Investigation Key Element Audit Checklist	330

Table 15.3 Example Categories for Incident Investigation Findings	332
Table 15.4 Recommendations Review Checklist	335
Table 15.5 Example Follow-Up Checklist	336
Table 16.1 Questions for Identifying Learning Opportunities	344

PREFACE

The American Institute of Chemical Engineers (AIChE) has helped chemical plants, petrochemical plants, and refineries address the issues of process safety and loss control for over 30 years. Through its ties with process designers, plant constructors, facility operators, safety professionals, and academia, the AIChE has enhanced communication and fostered improvement in the high safety standards of the industry. AIChE's publications and symposia have become an information resource for the chemical engineering profession on the causes of incidents and the means of prevention.

The Center for Chemical Process Safety (CCPS), a directorate of AIChE, was established in 1985 to develop and disseminate technical information for use in the prevention of major chemical accidents. CCPS is supported by a diverse group of industrial sponsors in the chemical process industry and related industries who provide the necessary funding and professional guidance for its projects. The CCPS Technical Steering Committee and the technical subcommittees oversee individual projects selected by the CCPS. Professional representatives from sponsoring companies staff the subcommittees and a member of the CCPS staff coordinates their activities.

Since its founding, CCPS has published many volumes in its "Guidelines" series and in smaller "Concept" texts. Although most CCPS books are written for engineers in plant design and operations and address scientific techniques and engineering practices, several guidelines cover subjects related to chemical process safety management. A successful process safety program relies upon committed managers at all levels of a company, who view process safety as an integral part of overall business management and act accordingly.

Incident investigation is an essential element of every process safety management program. This book presents underlying principles, management system considerations, investigation tools, and specific methodologies for investigating incidents in a way that will support implementation of a rigorous process safety program at any facility. The principles and suggested practices contained in this expanded third edition are not limited to chemical and petroleum process incidents. The basic concepts and provided examples are equally applicable to mining,

pharmaceutical, manufacturing, mail order fulfillment, and numerous other hazardous industries.

A team of incident investigation experts from the petroleum, chemical, and consulting industries, as well as a regulatory agency representative, drafted the chapters for this guideline and provided real-world examples to illustrate some of the tools and methods used in their profession. The subcommittee members reviewed the content extensively and industry peers evaluated this book to help ensure it represents a factual accounting of industry best practices. This third edition of the guideline provides updated information on many facets of the investigative process as well as additional details on important considerations such as human factors, forensics, and legalities surrounding incident investigations.

ACKNOWLEDGMENTS

The American Institute of Chemical Engineers wishes to thank the Center for Chemical Process Safety (CCPS) and those involved in its operation, including its many sponsors whose funding made this project possible; the members of its Technical Steering Committee who conceived of and supported this Guidelines project; and the members of its Incident Investigation Subcommittee. The Incident Investigation Subcommittee of the Center for Chemical Process Safety authored this third edition of the Guidelines for Investigating Process Safety Incidents.

The members of the CCPS Incident Investigation Subcommittee were:

Michael Broadribb, *Baker Engineering and Risk Consultants, Inc.*

Laurie Brown, *Eastman Chemical Company*

Chonai Cheung, *Contra Costa County*

Eddie Dalton, *BASF*

Carolina Del Din, *PSRG*

Jerry Forest, *Celanese, Subcommittee Chair*

Scott Guinn, *Chevron Corporation*

Christopher Headen, *Cargill*

Kathleen Kas, *Dow Chemical Company*

Mark Paradies, *System Improvements, Inc.*

Nestor Paralicci, *Andeavor*

Muddassir Penkar, *Evonik Canada Inc.*

Morgan Reed, *Exponent*

Meg Reese, *Occidental Chemical Corp.*

Marc Rothschild, *DuPont*

Joy Shah, *Reliance Industries Ltd*

Dan Sliva, *CCPS Staff Advisor*

Robert (Bob) Stankovich, *Eli Lilly*

Lee Vanden Heuvel, *ABS Consulting*

Terry Waldrop, *AIG*

Scott Wallace, *Olin*

Della Wong, *Canadian Natural Resources*

The third edition was authored by Baker Engineering and Risk Consultants, Inc. The authors at BakerRisk were:

Quentin A. Baker
Michael P. Broadribb
Cheryl A. Grounds
Thomas V. Rodante
Roger C. Stokes

Dan Sliva was the CCPS staff liaison and was responsible for overall administration of the project.

CCPS also gratefully acknowledges the comments and suggestions received from the following peer reviewers:

Amy Brethat, *NOVA Chemicals Corporation*
Steven D. Emerson, *Emerson Analysis*
Patrick Fortune, *Suncor Energy*
Walter L. Frank, *Frank Risk Solutions, Inc.*
Barry Guillory, *Louisiana State University*
Jerry L. Jones, *CFEISBC Global*
Gerald A. King, *Armstrong Teasdale LLP*
Susan M. Lee, *Andeavor*
William (Bill) D. Mosier, *Syngenta Crop Protection, LLC*
Mike Munsil, *PSRG*
Pamela Nelson, *Solvay Group*
Katherine Pearson, *BP Americas*
S. Gill Sigmon, *AdvanSix*

Their insights, comments, and suggestions helped ensure a balanced perspective to this Guideline.

The efforts of the document editor at BakerRisk are gratefully acknowledged for contributions in editing, layout, and assembly of the book. The document editor was Phyllis Whiteaker.

The members of the CCPS Incident Investigation Subcommittee wish to thank their employers for allowing them to participate in this project and lastly, we wish to thank Anil Gokhale of the CCPS staff for his support and guidance.

ACRONYMS AND ABBREVIATIONS

ACC	American Chemistry Council
AIChE	American Institute of Chemical Engineers
ALARP	As Low as Reasonably Practicable
ANSI	American National Standards Institute
API	American Petroleum Institute
ARIP	Accidental Release Information Program
ARIA	Analysis, Research and Information on Accidents
ASME	American Society of Mechanical Engineers
BARPI	Bureau for Analysis of Industrial Risks and Pollutions
BP	Boiling Point
BI	Business Interruption
BLEVE	Boiling Liquid Expanding Vapor Explosion
BPCS	Basic Process Control System
C	Consequence factor, related to magnitude of severity
CCF	Common Cause Failure
CCPS	Center for Chemical Process Safety,
CE/A	Change Evaluation/Analysis
CEFIC	(European) Chemical Industry Council
CEI	Dow Chemical Exposure Index
CELD	Cause and Effect Logic Diagram
CFD	Computational Fluid Dynamics
CIRC	Chemical Incidents Report Center
CLC	Comprehensive List of Causes
COMAH	Control of Major Accident Hazards
CPQRA	Chemical Process Quantitative Risk Assessment
CSB	Chemical Safety and Hazards Investigation Board (US)
CTM	Causal Tree Method
CW	Cooling Water
<i>D</i>	Number of times a component or system is challenged (hr ⁻¹ or year ⁻¹)
DCS	Distributed Control System
DIERS	Design Institute for Emergency Relief Systems
DMAIC	Define, Measure, Analyze, Improve, Control
DOT	Department of Transportation
E&CF	Events & Causal Factor Charting
EBV	Emergency Block Valve
EHS	Environmental, Health & Safety

EI	Energy Institute
EPA	United States Environmental Protection Agency
eMARS	European Commission Major Accident Reporting System
EPSC	European Process Safety Centre
ERPG	Emergency Response Planning Guideline
ETA	Event Tree Analysis
<i>F</i>	Failure Rate (hr ⁻¹ or year ⁻¹)
<i>f</i>	Frequency (hr ⁻¹ or year ⁻¹)
F&EI	Dow Fire and Explosion Index
F/N	Fatality Frequency versus Cumulative Number
FCE	Final Control Element
FEA	Finite Element Analysis
FMEA	Failure Modes and Effect Analysis
FTA	Fault Tree Analysis
HAZMAT	Hazardous Materials
HAZOP	Hazard and Operability Study
HAZWOPER	Hazardous Waste Operations and Emergency Response
HBTA	Hazard–Barrier–Target Analysis
HE	Hazard Evaluation
HIRA	Hazard Identification and Risk Analysis
HMI	Human Machine Interface
HSE	(UK) Health and Safety Executive
HRA	Human Reliability Analysis
ICCA	International Council of Chemical Associations
IChemE	Institution of Chemical Engineers
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IOGP	International Association of Oil & Gas Producers
IPL	Independent Protection Layer
ISA	The Instrumentation, Systems, and Automation Society (formerly, Instrument Society of America)
ISBL	Inside Battery Limits
ISD	Inherently Safer Design
ISO	International Organization for Standardization
JSA	Job Safety Analysis
KPI	Key Performance Indicators
LAH	Level Alarm—High
LAL	Level Alarm—Low
LEL	Lower Explosive Limit
LFL	Lower Flammability Limit

LI	Level Indicator
LIC	Level Indicator—Control
LNG	Liquefied Natural Gas
LOPA	Layer of Protection Analysis
LOPC	Loss of Primary Containment
LOTO	Lockout/Tagout
LSHH	Level Sensor High High
LT	Level Transmitter
MARS	Major Accident Reporting System
MAWP	Maximum Allowable Working Pressure
MCSOII	Multiple-Cause, Systems-Oriented Incident Investigation
MES	Multilinear Event Sequencing
MHIDAS	Major Hazard Incident Data System
MI	Mechanical Integrity
MIC	Methyl isocyanate
MM	Million
MOC	Management of Change
MOM	Singapore's regulatory standard for incident investigation
MORT	Management Oversight Risk Tree
MSDS	Material Safety Data Sheet
NAICS	North American Industry Classification System
NFPA	National Fire Protection Association
N ₂	Nitrogen
NOM	Mexico's regulatory standard for incident investigations
NTSB	National Transportation Safety Board
IOGP	International Association of Oil and Gas Producers
OREDA	The Offshore Reliability Data project
ORPS	Occurrence Reporting and Processing System
OSBL	Outside Battery Limits
OSHA	United States Occupational Safety and Health Administration
P_{fatality}	Probability of Fatality
P_{ignition}	Probability of Ignition
$P_{\text{person present}}$	Probability of Person Present
P	Probability
P&ID	Piping and Instrumentation Diagram
PCB	Polychlorinated Biphenyl
PFD	Probability of Failure on Demand
PHA	Process Hazard Analysis
PI	Pressure Indicator

PIF	Performance Influencing Factor
PL	Protection Layer
PLC	Programmable Logic Controller
PM	Preventive Maintenance
PPE	Personal Protective Equipment
PSHH	Pressure Sensor High High
PSI	Process Safety Information
PSID	Process Safety Incident Database
PSM	Process Safety Management
PSM	also Canada's (non-regulatory) standard, individualized by district
PSV	Pressure Safety Valve (Relief Valve)
R	Risk
RCA	Root Cause Analysis
RIDDOR	Reporting of Injuries, Diseases and Dangerous Occurrence Regulations
RMP	Risk Management Program (US)
RQ	Release Quantity
RV	Relief Valve
SAWS	China's regulatory guideline for incident investigations
SCAT	Systematic Cause Analysis Technique
SCE	Safety Critical Equipment
SDS	Safety Data Sheets
SEMS	Safety and Environmental Management System
SHE	Safety Health & Environment
SIF	Safety Instrumented Function
SIS	Safety Instrumented System
SMART	Specific, Measureable, Agreed/Attainable, and Realistic/Relevant, with Timescales
SOL	Safe Operating Limit
SOP	Standard Operating Procedure
SOURCE	Seeking Out the Underlying Root Causes of Events
SRK	Skills, Rules, Knowledge
SSDC	System Safety Development Center
STEP	Sequentially Timed Events Plot
T	Test Interval for the Component or System (hours or years)
T_0	starting time
T_n	ending time

TNO	Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO; English: Netherlands Organization for Applied Scientific Research)
UEL	Upper Explosive Limit
UFL	Upper Flammable Limit
VCE	Vapor Cloud Explosion
VLE	Vapor Liquid Equilibrium
XV	Remote Activated/Controlled Valve

1 INTRODUCTION

1.1 BUILDING ON THE PAST

Flixborough, Bhopal, Piper Alpha, Deepwater Horizon, Buncefield— all are now synonyms for catastrophe. These names are inextricably linked with images of death, suffering, environmental damage and disastrous loss tied to the production of chemicals, fuels, or oils. An objective review of the world's industrial history reveals a story punctuated with infrequent yet similarly tragic incidents. Invariably, in the wake of such tragedy, companies, industries, and governments work together to learn the causes. Their ultimate goal is to implement the knowledge acquired through diligent investigation, which in turn can help prevent recurrence or mitigate consequences.

Investigations into catastrophic events have revealed something of major significance—the key to preventing disaster first lies in recognizing leading indicators rather than the lagging indicators. Leading indicators exist, and therefore can be uncovered, in incidents that are much less than catastrophic. They can even be seen in so-called near-misses that may have no discernable impact on routine operation. By examining abnormal/upset operations, near-misses, and lower-consequence higher-frequency occurrences, companies may identify deficiencies that, if left uncorrected, could eventually result in serious or even catastrophic events.

The two most significant roles incident investigations can play in comprehensive process safety programs are:

1. Preventing disasters by consistently examining and learning from near-misses (inclusive of abnormal operations, minor events, etc.) and;
2. Preventing disasters by consistently examining and learning from more serious accidents.

The Center for Chemical Process Safety (CCPS) of the American Institute of Chemical Engineers (AIChE) recognized the role of incident investigation when it published the original *Guidelines for Investigating Chemical Process Incidents* in 1992.

The first edition provided a timely treatment of incident investigation including:

- a detailed examination of the role of incident investigation in a process safety management system,
- guidance on implementing an incident investigation system, and
- in-depth information on conducting incident investigations, including the tools and techniques most useful in understanding the underlying causes.

The second edition, released in 2003, built on the first text's solid foundation. The goal was to retain the knowledge base provided in the original book while simultaneously updating and expanding upon it to reflect the latest thinking. That edition presented techniques used by the world's leading practitioners in the science of process safety incident investigation.

This third edition is a further enhancement of the second edition. Specific emphasis has been placed on updating investigation techniques and analytical methodologies, and applying them to example case studies where possible. Expanded topics include scientific validation of hypotheses, rigorous physical evidence documentation and examination, scientific analysis, hypothesis rejection and substantiation, learnings from repeat incidents, and means to institutionalize learnings within an organization.

1.2 INVESTIGATION BASICS

Successful investigations are dependent on preplanning, documented procedures, appropriate investigator training and experience, appropriate support from leadership, and necessary resources (personnel, time, and materials), to conduct a thorough investigation. It is imperative that operating organizations conduct careful and comprehensive investigations that are factual and defensible. Developing and following written procedures allows organizations to consistently respond promptly and effectively, establishes the basis for continuous improvement, and helps preserve a company's "license to operate".

1.2.1 The First Step in conducting a successful incident investigation is to recognize when an incident has occurred so that an Incident Management System (Chapter 4) can be activated. Linked with incident recognition are Initial Notification, Classification, and Investigation (Chapter 5).

It is important to use standard terminology when referring to incident investigation so that those investigating an occurrence all share a common language that efficiently and accurately supports their investigation objectives. Some investigators may define the terms presented below slightly differently or use other descriptive terms that have the same meaning. Some organizations may desire to further sub-divide these terms into different levels. Within the scope of this book, the following definitions for key terms will apply throughout:

1.2.1.1 Incident—*an unusual, unplanned, or unexpected occurrence that either resulted in, or had the potential to result in harm to people, damage to the environment, or asset/business losses, or loss of public trust or stakeholder confidence in a company's reputation. Some examples are:*

- *process upset with potential process excursions beyond operating limits,*
- *release of energy or materials,*
- *challenges to a protective barrier,*
- *loss of product quality control,*
- *etc.*

1.2.1.1(a) Accident—*an incident that results in a significant consequence involving:*

- *human impact,*
- *detrimental impact on the community or environment,*
- *property damage, material loss,*
- *disruption of a company's ability to continue doing business or achieve its business goals, (e.g. loss of operating license, operational interruption, product contamination, etc.).*

1.2.1.1(b) Near-miss—*an incident in which an adverse consequence could potentially have resulted if circumstances (weather conditions, process safeguard response, adherence to procedure, etc.) had been slightly different.*

For most occurrences, protective barriers prevent a resultant adverse consequence. Such occurrences are often referred to as near-hits, near-misses, or close calls. For every incident labeled a near-miss, more subtle precursors exist that, if investigated and understood, could provide valuable insights into factors that could be applied to mitigating or preventing other incidents.

1.2.2 The Second Step in conducting a thorough investigation is to assemble a qualified team (Chapter 6) that will determine and analyze the facts of the incident. This team's charter is to apply appropriate investigation tools and methodologies (Chapter 3) that will lead to the identification of the latent causes and application of remedies that could have prevented the incident or mitigated its consequence.

1.2.3 The Third Step in incident investigation is to gather information, separate facts from suppositions, analyze data, and determine what happened. Before conducting a cause analysis, a comprehensive and accurate understanding of what happened must first be completed. Witness management (Chapter 7), evidence management (Chapter 8), and evidence analysis and hypothesis testing (Chapter 9) are key concepts to be employed during the investigation process.

1.2.4 The Fourth step in incident investigation is to determine root causes for the failure(s) that initiated or failed to prevent the incident. Note that root cause is being used in this book in the traditional sense, i.e.:

Root Cause - *A fundamental, underlying, system-related reason why an incident occurred that identifies a correctable failure(s) in management systems.*

By this definition, a root cause is the most fundamental level in the cause determination, and there is no more fundamental level. Recommendations can be developed for root causes that will prevent, lessen the likelihood, and/or consequence, of the same **and** similar incidents from occurring. Whereas, causal factors are invariably contributory in nature and, for the purposes of this book, are defined as:

Causal Factor - *A major unplanned, unintended contributor to an incident (a negative event or undesirable condition), that if eliminated would have either prevented the occurrence of the incident, or reduced its severity or frequency.*

This definition implies that, if recommendations are based on causal factors, they would only prevent the same incident but not similar incidents from occurring. Therefore, recommendations should be based on root causes.

Once the most likely hypothesis is validated, determining root causes via a structured approach (Chapter 10) will help the investigation team determine all relevant factors. Understanding the impact of human factors is key to identifying root causes and is discussed in detail in (Chapter 11). Once

root causes have been identified, effective recommendations can be developed (Chapter 12).

1.2.5 The Fifth Step in incident investigation is preparing the investigation report (Chapter 13) which details the facts, findings, and recommendations prepared by the investigation team. Typically, recommendations are written to prevent incident recurrence by:

- improving the process technology,
- upgrading the operating or maintenance procedures or practices,
- improving compliance with existing organizational systems (operational discipline); and
- upgrading the management systems, (often the most critical area).

1.2.6 The Sixth Step in incident investigation is to implement and communicate the team's conclusions. After the investigation is completed and the findings and recommendations are issued in the report, a system is needed to implement and audit those recommendations (Chapter 14). This is not part of the investigation itself, but rather the follow-up related to it. Once a technological, procedural, or administrative corrective action is enacted, it is monitored periodically for effectiveness and, where appropriate, modified to meet the intent of the original recommendation. Learnings from an investigation can also be institutionalized and shared throughout the company and industry, particularly with those most affected by the incidents.

These six steps will result in the greatest positive effect when they are performed in an atmosphere of openness and trust. Management demonstrates, by both word and deed, that the primary objective is not to assign blame, but to implement system fixes and share learnings for the sake of preventing future incidents. This book helps organizations define and refine their incident investigation systems to achieve positive results effectively and efficiently.

1.3 WHO SHOULD READ THIS BOOK?

This book assists three target groups:

1. Incident investigation team leaders
2. Incident investigation team members
3. Corporate and site process safety managers and coordinators

This book provides a valuable reference tool for anyone directly involved in leading or participating on incident investigation teams. It presents knowledge, techniques, and examples to support successful investigations. This book offers a model for success in building or upgrading an incident investigation program.

Like previous editions, the book remains focused primarily on investigating process-related incidents. Most organizations find that integrating process safety with other types of investigations provides an opportunity to enhance any investigation. Readers will find that the methodologies, tools, and techniques described in the following chapters may be successfully applied when investigating other types of occurrences such as operational reliability, product quality, and occupational health and safety incidents.

1.4 THE GUIDELINE'S OBJECTIVES

Readers should be able to achieve the following objectives.

- Describe the basic principles behind successful incident investigations.
- Identify the essential features of a management system designed to foster and support high quality incident investigations.
- List detailed steps for planning and conducting incident investigations, including investigative tools, techniques, and methodologies for determining causes.
- Use the findings of an investigation to make effective recommendations that can reduce the likelihood of recurrence or mitigate the consequences of similar incidents (or even dissimilar incidents with common root causes).
- Plan an effective system for documenting, communicating, and resolving investigation findings and recommendations, including a method to track resolution of incident recommendations.
- Effectively share the learnings of investigations and institutionalize learnings to prevent the lessons from being lost over time.

1.5 THE GUIDELINE'S CONTENT AND ORGANIZATION

The summaries below provide an overview of the content and organization of the book chapter-by-chapter to assist in quickly locating a particular area of interest.

Chapter 2—Overview of Chemical Process Incident Causation

This chapter discusses the basics of determining incident causation, general types of incidents, and the linkage between causation theories, root causes, and management systems. Understanding incident sequence models, barrier analysis, and failure modes can greatly assist investigators in dissecting the anatomy of process incidents.

Chapter 3—An Overview of Investigation Methodologies

This chapter provides an overview of investigation methodologies, associated tools, and techniques that come together to form a modern structured investigate approach. An overview of the historical transition is provided along with description of methodologies and tools most commonly used by CCPS members.

Chapter 4—Designing an Incident Investigation Management System

This chapter provides an overview of a management system for investigating process safety incidents. It opens with a review of responsibilities from management through the workforce and presents the important features that a management system can address to be effective. It examines systematic approaches that start with notification, team structure, functional and agency integration, document control, team objectives, etc. The learning objective is to define a management system that supports incident investigation teams, root cause determinations, effective recommendation implementation, follow-up, and continuous improvement.

Chapter 5—Initial Notification, Classification, and Investigation of Process Safety Incidents

Timely reporting of incidents enables management to take prompt preventative or corrective measures to mitigate consequences. Many major process safety incidents were preceded by precursor occurrences (typically referred to as near-misses) that might have gone unrecognized or ignored because “nothing bad” actually happened. The lessons learned from any incident can be extremely valuable. However, this benefit is only realized when incidents are recognized, reported, and investigated. This chapter describes important considerations for internal reporting of incidents, the process of classifying incidents into categories, and means for determining appropriate levels of investigation to be conducted.

Chapter 6—Building and Leading an Incident Investigation Team

Personnel with proper training, skills, and experience are critical to the successful outcome of an incident investigation. This chapter describes team composition as a function of incident type, complexity, and severity, and includes suggested training topics. It also provides team leaders with a high-level overview of the basic team activities typically required in the course of conducting an investigation.

Chapter 7 - Witness Management

This chapter discusses techniques for identifying witnesses and effective interviewing techniques designed to obtain reliable information from them. Witnesses often hold the most intimate knowledge of conditions at the time of the incident, actions taken pre-incident and post-incident, process design and operations, etc. Effective management of witnesses is a crucial element of the investigation process. Issues related to witness interactions and interviewing techniques are covered in detail.

Chapter 8—Evidence Identification, Collection, and Management

Facts are the fuel that an investigation needs to reach a successful conclusion. This chapter addresses the methods and practical considerations of data-gathering and archiving activities. It describes plan development; priority establishment; different types and sources of data; data-gathering tools, techniques, and preservation; documentation requirements; photography and video techniques; suggested supplies; etc.

Chapter 9 - Evidence Analysis and Causal Factor Determination

This chapter provides practical guidelines for analyzing evidence, proving/disproving hypotheses, and developing causal factors. The use of a scientific methodology to sort out facts from collected data is explained, and techniques are offered for use during this iterative and overlapping process. Identifying causal factors is an intermediate step towards determining root causes, and implementing recommendations based on root causes should inherently address the causal factors as well.

Chapter 10—Determining Root Causes—Structured Approaches

This chapter addresses methods and tools used successfully to identify multiple root causes. Process safety incidents are almost always the result of more than one root cause. This chapter provides a structured approach for determining root causes. It details some powerful, widely used and proven tools and techniques available to incident investigation teams, including

timelines, fault trees, logic trees, predefined trees, checklists, and application of human factors. Examples are included to demonstrate how they apply to the types of incidents readers are likely to encounter.

Chapter 11—The Impact of Human Factors

This chapter describes human factor considerations in incident investigation. It provides insight and tools to identify and address applicable human factor issues throughout an investigation. Practical models are presented along with examples.

Chapter 12—Developing Effective Recommendations

Once the likely causes of an incident have been identified, investigation teams evaluate what can be done to help prevent recurrence or mitigate consequences. The incident investigation recommendations are the product of this evaluation. This chapter addresses types of recommendations, attributes of high quality recommendations, methods to document and present recommendations, and related management responsibilities.

Chapter 13—Preparing the Final Report

In the case of incident investigation, a major milestone is completed when the final incident investigation report is submitted. The incident report documents the investigation team's findings, conclusions, and recommendations. This chapter describes practical considerations for writing formal incident reports, and discusses the attributes of quality reports and differences among incident notifications, interim reports, and a final report. Considerations and associated practical techniques are provided for stating report scope, preparing preliminary notices, documenting the investigation process and results, developing a report format, and performing a quality assurance check that includes management review and approval.

Chapter 14—Implementing Recommendations

The recommendations generated from an incident investigation when implemented in a timely and effective fashion, decrease the probability of recurrence, and/or reduce the potential consequences of an event. This chapter begins with case examples that underscore key concepts, and then focuses on the critical aspects of effectively implementing recommendations. It addresses initial resolution of the recommendations, their full implementation, effectiveness of follow-up, and tracking.

Chapter 15—Continuous Improvement for the Incident Investigation System

The adage “if it ain’t broke, don’t fix it” does not apply to process safety management systems. A continuous improvement pillar is an integral part of the process safety management system. This chapter describes techniques that can help the incident investigation element of process safety remain strong and viable in an ever-changing technical, business, and regulatory environment. It includes considerations for assessing existing incident investigation programs as well as approaches for implementing continuous improvement.

Chapter 16—Institutional Knowledge

Sharing lessons learned, not only across the organization but also across industry and related agencies, is an extremely effective way to learn from the occurrences of others. This chapter focuses on how to obtain and critically analyze incident information and share core learnings, and provides examples.

Appendices

The appendices provide a wealth of supplemental information on the subject of incident investigation. Topics include:

- A. Photography Guidelines for Maximum Results
- B. Example Protocol – Checking Position of a Chain Valve
- C. Process Safety Events Leveling Criteria
- D. Example Case Study
- E. Quick Checklist for Investigators
- F. Evidence Preservation Checklist– Prior to Arrival of the Investigation Team
- G. Guidance on Classifying Potential Severity of a Loss of Primary Containment

Glossary

The glossary provides definitions of terms used throughout the book. To the greatest extent possible, definitions are consistent with the CCPS Process Safety Glossary.

(<https://www.aiche.org/ccps/resources/glossary>).

References

An extensive list of references is assembled to allow the reader to obtain the source reference papers and reports for investigation methodologies.

1.6 THE CONTINUING EVOLUTION OF INCIDENT INVESTIGATION

Like all the elements of process safety management, the incident investigation element continues to evolve. The AIChE Center for Chemical Process Safety assists this evolution by providing information to help companies safely operate process facilities. To this purpose, CCPS and the contributing authors offer this third edition of this guidebook on investigating process safety incidents.

2 OVERVIEW OF CHEMICAL PROCESS INCIDENT CAUSATION

For an investigation of a chemical process incident to be effective, the investigation team should apply a systematic approach that identifies the root causes of the incident, as defined in Chapter 1. As a rule, the benefits of this systematic approach result from:

- Applying a consistent and effective investigative effort, and
- Implementing sound process safety management principles.

The investigation team should apply an approach based on basic incident causation concepts. When a system or process fails, it may be difficult to trace the reasons for its failure. Based on available historic incident data, the makeup of a major incident is rarely simple and rarely results from a single root cause. Serious process safety incidents typically involve a complex sequence of occurrences and conditions that can include, but are not limited to:

- equipment faults or faulty design,
- latent unsafe conditions,
- environmental circumstances, and
- human errors.

Understanding the concepts of incident causation is essential to comprehensively investigate incidents and prevent their recurrence or mitigate their consequences through implementation of effective recommendations.

Numerous theories and models of incident causation have been developed over the years (Heinrich, 1936; Gibson, 1961; Recht, 1965; Haddon, 1980; Peterson, 1984, etc.). These theories and models may appear at first to be diverse and disparate, but they do contain a number of common themes and concepts. As a result of this research, industry best practices in incident investigation have evolved significantly over the last few decades, based upon a number of key incident causation theories.

This chapter discusses models that illustrate how a process safety incident can develop in a staged manner, often as a result of weaknesses in the management system. It also provides a brief overview of key causation

concepts such as loss of primary containment, linkage between root causes and the management system, involvement of human factors, and multiple root causes.

2.1 STAGES OF A PROCESS-RELATED INCIDENT

Experience from systematic analyses of past process safety incidents has allowed researchers to develop incident models that display the makeup of a process-related incident using a conceptual framework.

2.1.1 Three Phase Model of Process-Related Incidents

The progression of any process-related incident could be described as occurring in three different phases or stages (DoE, 1985):

1. Change from normal operating state into a state of abnormal (or disturbed) operation, i.e. a deviation from intended safe operation.
2. Loss of control of the abnormal operating phase, which may involve a breakdown of a barrier function. A barrier function is a safety feature such as a shutdown valve or containment system, a procedure, or the communication system. When safety systems fail, the incident can evolve from an undesirable occurrence to a near-miss and, if enough barriers fail, the incident could progress to an operational interruption or accident, depending upon the consequences or circumstances.
3. The severity of subsequent consequences is influenced by [the impact of] loss of control of energy accumulations. Process safety incidents can involve different hazardous energies, such as chemical, mechanical, electrical, thermal and pressure.

This model introduces the general concept that there is typically a sequence of events leading to a process safety incident. Understanding the sequence of events, and the barriers that have failed can help investigators to understand the progression of an incident.

2.1.2 Event Tree

An event tree model is an example of a more structured conceptual framework encompassing the three phases of a process-related incident. Figure 2.1 illustrates an example of an event tree of incident causation.

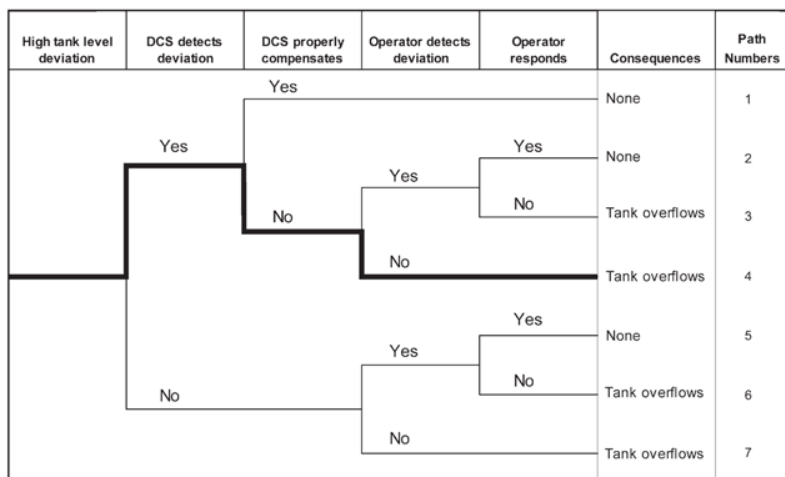


Figure 2.1 Event Tree for a Process-related Incident

In the Figure 2.1 example, there is:

1. Deviation from normal operation into abnormal operation. An example is the tank level deviation, which could be caused by various events or conditions, such as: operator error, faulty instrumentation, etc.
2. Breakdown of control of the abnormal operation. An example is the distributed control system (DCS) not compensating properly. Another example is the operator not detecting the deviation.
3. Loss of control of energy. An example is the operator not responding, which allows the tank to overflow.

This example has three contributors to incident causation in each of the three phases: equipment, process systems, and human. Under different circumstances, the organization, the environment and/or external factors may also contribute. There are two detection systems and two intervention opportunities. Depending on the success or failure of each, there are three potential paths that result in no adverse consequences and four potential paths that lead to failure, with overflow as the immediate consequence. Note that sometimes there are more opportunities for things to go wrong than to go right and the event tree clearly depicts the specific paths that can lead to an undesired event.

This example illustrates that event trees can be useful models of an incident sequence because they provide a graphical, logic-based depiction of the various potential consequences that could occur, depending on the pathway of an event. This is a more structured sequence model than the three-phase model, but it does not fully address the weaknesses in barriers and the management systems behind them.

2.1.3 *Swiss Cheese Model*

Another way to represent the staged events and conditions that result in an incident is by using the Swiss Cheese model (Reason, 1990). This model takes one of the failure paths defined in the event tree that leads to a consequence of concern. The protective barriers (safety systems) are represented by parallel slices of Swiss cheese. These barriers represent the equipment, procedures/practices, and people that comprise elements of the management system for the facility.

Ideally each barrier should be robust, but like the holes in Swiss cheese, all barriers have weaknesses (Figure 2.2) resulting from:

- Active failures (e.g., equipment failures, unsafe acts, human errors, procedural violations, etc.).
- Latent failures (e.g., design/equipment deficiencies, inadequate/impractical procedures, time pressure, unsafe conditions, fatigue, etc.) – see Section 2.1.4 below.

These weaknesses can lead to management system failures resulting in a process safety incident (see Section 2.2.2 below).

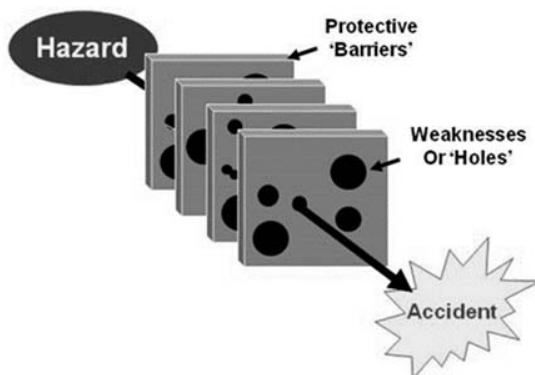


Figure 2.2 Swiss Cheese Model

In reality, the holes or weaknesses are not static; they are dynamic and continually open and close. For example, one personnel shift may be more experienced and diligent than another, so that some barriers begin to degrade further at shift change. Each barrier may not work when needed, and is fully dependent on management system implementation to ensure a reasonable probability of working on demand.

If a weakness occurs in one barrier, there may be one or more other barriers that can provide sufficient protection and, while the weakness may have an undesirable outcome, it is unlikely that a significant incident will occur. However, most process safety incidents involve a combination of multiple active and latent failures. Therefore, investigators should understand that *no layer of protection is perfect*, and look for weaknesses in all barriers.

2.1.4 Importance of Latent Failures

The Swiss Cheese model introduced the concept of latent failures (also known as latent conditions). Historic incident data show that latent failures have played an important role in incident causation (Reason, 1990). The term latent failure implies the condition is dormant or hidden. Normally the latent failure can be revealed before an incident occurs, through testing or auditing during typical operations within the process, as shown in Figure 2.3.

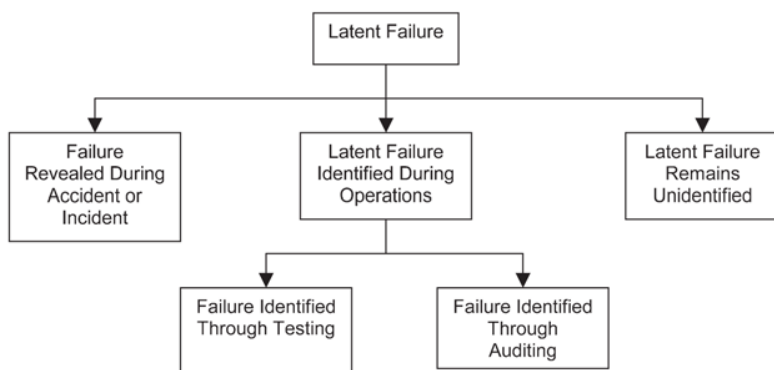


Figure 2.3 Latent (hidden) Failure

There is always a possibility, however, that a latent failure may remain hidden during testing. There are several reasons a latent failure may not be detected, including, but not limited to:

- It was not activated by the test used.
- The test was deficient, gave wrong results, or did not test the system properly.
- The test activity itself activates failure upon the next use of the process.

It is important that investigators understand the concept that latent failures can contribute to an incident, in addition to more obvious active factors, such as unsafe acts and spontaneous equipment failure. Latent failures may involve organizational influences, inadequate supervision, human error and equipment/system preconditions that were hidden from, or unknown to, personnel responsible for the process.

2.2 KEY CAUSATION CONCEPTS

Some of the common concepts from incident causation theories that are relevant to the investigation of process safety incidents are:

- There is potential or actual loss of containment or energy,
- There is a direct linkage between root causes and the management system,
- Most incidents involve human factors,
- Each incident will likely have multiple root causes,
- Events are not root causes, and
- Risk is not reduced until effective remedies are implemented.

Each of these causation concepts and a number of avoidable pitfalls that incident investigators should be aware of are discussed below.

2.2.1 *Loss of Containment or Energy*

A process safety incident involves a loss of containment of a hazardous chemical or a loss of control of energy. The chemical or energy is a hazard that, if released, has the potential to cause harm to people, the environment, or property. Even if no harm occurs, a thorough investigation of the root

causes for the loss of containment or energy and implementation of appropriate remedial actions can prevent a more serious outcome in the future.

Appropriate remedial actions are likely to follow Inherently Safer Design (ISD) principles such as the measures listed in Figure 2.4 to prevent, control, and mitigate incidents (based on Haddon, 1980).

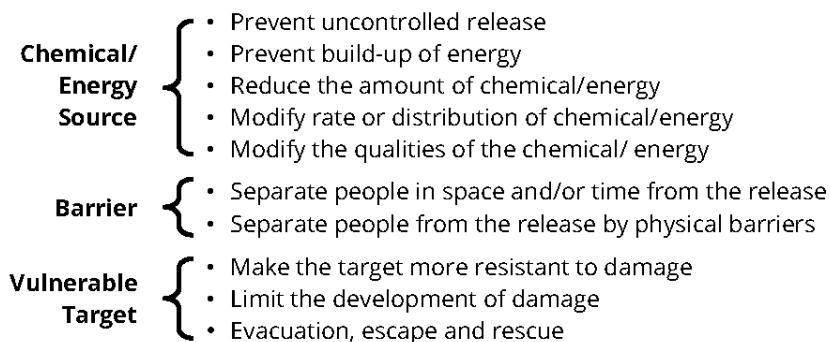


Figure 2.4 Incident Prevention Strategies

Haddon recognized that not all hazards (chemical/energy sources) can be eliminated, and to protect vulnerable receptors (e.g., people), most remedial actions will likely reduce risk by applying additional safeguards or improving the management of existing safeguards. This is consistent with CCPS guidance on Inherently Safer Design (ISD), which recommends a hierarchical and iterative approach covering first order (hazard elimination) and second order (reduction of severity or likelihood) ISD approaches (CCPS, 2007b).

It is also important to consider why the magnitude of the consequence of an incident was, or under slightly different circumstances could have been, as severe. The potential consequence of an incident is often a function of the following five factors:

1. *Inventory of hazardous material*: type and amount
2. *Energy factor*: energy of a chemical reaction or material state
3. *Time factor*: the rate of release, its duration, and the warning time
4. *Intensity-distance relation*: the distance over which the hazard may cause injury or damage

5. *Exposure factor*: a factor that mitigates the potential effects of an incident

Therefore, incident investigators should consider not only what went wrong, but also corrective actions based on second order ISD principles that could be taken to minimize the impact of future incidents.

2.2.2 Management System Failure

Most active failures and latent failures, whether they are equipment deficiencies, human errors, or unsafe acts/conditions, are the result of weaknesses, defects or breakdowns in the management system(s). Consequently, there is a strong link between root causes and management systems. Causal factors are unplanned contributors (negative events or undesirable conditions) to an incident, that if eliminated would have either prevented the incident, or reduced its severity or frequency. Therefore, a strong link also exists with causal factors, as these negative events and undesirable conditions involve some of the active and latent failures that contributed to the incident.

On rare occasions, an individual may deliberately damage a chemical process to cause an incident, but even then a management system weakness (such as facility security or employee fitness for duty) may be involved.

Risk is a measure of human injury, environmental damage, or economic loss in terms of both the incident likelihood and its severity. One reason the management system concept has received broad recognition relative to chemical incident investigation is that it builds directly on fundamental process safety principles. To manage risk, appropriate management systems need to be in place to ensure that the barriers against incidents remain intact. These preventive, error detection, and mitigation management systems make up the bulk of process safety efforts. Examples of these include the 20 elements of CCPS's process safety management system (CCPS, 2007a), such as operating and maintenance procedures, effective training, control of up-to-date process safety information, management of change, performance measurement, auditing, etc.

As most root causes are associated with weaknesses, defects, or breakdowns in the management system(s), investigators should look for weak barriers. These weak barriers could be associated with various aspects of the management system, including, but not limited to, the attributes in Table 2.1.

Table 2.1 Attributes of a Management System

Management System Attributes
Policies, Practices, Procedures, Standards, Instructions
Design and Technical Specifications
Competency Requirements, Training
Resources (Equipment, People, Funding)
Specific Tasks
Assignment of Authority, Accountability, Responsibility
Communications (Verbal, Electronic, Paper)
Documentation
Monitoring (Audit, Metrics)
Modifications for Changes and Deviations
Follow-Up and Continuous Improvement

2.2.3 Human Factors

Although root causes are generally related to management system weaknesses, most incidents involve people, even if the incident is an equipment failure. However, human error is **not** a root cause; rather it is important to understand which work environment or management system failure created the opportunity for human error to occur.

A recent study highlighted human and organizational errors as a major contributor to equipment failures in the process industries (Kidama, 2013). Examples of typical contributions related to equipment failures in this study include, but are not limited to:

- Equipment degradation through poor/incorrect design or maintenance,
- Poor design of human machine interface (HMI),
- Use of an unsafe/inadequate procedure,
- Failure to follow procedures,
- Poor contractor management,
- Poor management and supervision,
- Lack of planning,
- Poor competency (lack of knowledge, skills and abilities),
- Human error, including simple misjudgments,
- Inadequate physical/mental condition, and
- Poor behavior.

Although these are the result of actions or inactions by people, this does not imply that people are to blame. In reality, human factors are a contributing or intermediate causation, but it is weaknesses in the management system(s) that have allowed contributions, such as those listed above, to exist.

2.2.4 Multiple Causation

We are too much accustomed to attribute to a single cause that which is the product of several, and the majority of our controversies come from that.

Marcus Aurelius

Incidents are generally not the result of a single cause or act, unless an individual deliberately decides to work unsafely or damage/sabotage a chemical process. Even in such extreme deliberate acts, engineering and management controls that might have minimized the probability and/or consequence of the act should be considered as part of security vulnerability assessments.

Most incidents have multiple root causes, and certain combinations of those causes can give rise to accidents or near-misses. Some of these causes may have resulted in near-misses or minor incidents on previous occasions, i.e., less severe precursors such as scenarios when a barrier failed but the event did not propagate to adverse consequences. A thorough investigation of these types of events will not only find the root causes of the subject incident, but will also find other root causes that were near-misses. It is therefore an avoidable mistake to stop an investigation after identifying only one root cause. If the near-misses are not investigated, they may cause a future incident even if the root causes of the subject incident are corrected.

2.2.5 Events vs Root Causes

An event (including a non-event, i.e., an omission) cannot be a root cause because it is either a causal factor or the consequential result or symptom that follows a root cause. For example, *the operator opened the drain valve* is an event that led to a spillage of hazardous material. In this case, the root cause is related to **why** the operator opened the drain valve – was it due to inadequate training, human error, or another cause? Similarly, *failure to follow procedure* is not a root cause. It is a symptom of an underlying cause.

Sometimes it can be difficult to distinguish between events, symptoms, and actual root causes. If an event or symptom is identified as a root cause, the investigation has been stopped too soon. If the investigation’s recommendations only address events or symptoms, the real root causes will remain unresolved, and the incident may recur.

2.2.6 Controlling Risk

Because the management system concept builds on basic principles, it can be applied not only to process safety incident investigation, but also to reliability, quality, and business loss investigations. In process safety, as in all other systems used to control risk to a business, there are three basic keys to controlling the risk (see Figure 2.5):

1. **Understanding Risk:** Assessing the level of risk is accomplished by identifying potential incident scenarios and predicting their severity and likelihood using Hazard Identification and Risk Analysis (HIRA) studies (CCPS 2007a). The result is an understanding of the specific barriers necessary to control the risk to a tolerable level.
2. **Management Systems:** Management systems need to be in place to ensure the barriers remain sufficiently robust to manage the risk, as described in Section 2.2.1, above.
3. **Analyzing Weaknesses:** Continuous improvement of management systems is needed to prevent incident recurrence by implementing incident reporting and investigation practices to identify and correct weak barriers.

Figure 2.5 illustrates the relationship of these three keys.



Figure 2.5 Universal Concept for Controlling Risk (Kletz)

Neither prediction of potential incident scenarios nor management systems to prevent incidents will be perfect (although that should be the goal), so it is important to learn from incidents, even near misses, and to correct any weaknesses in the barriers. It is important to use a structured approach to incident investigation that builds on proven and recognized techniques, which makes it easier to develop consistent understanding from incidents and to communicate insights and results from investigations effectively. However, it is imperative to recognize that the risk of repeat incidents remains until remedial actions are properly implemented. Simply formally writing an investigation report and discussing it afterward does not reduce the risk.

It is essential that the investigation's recommendations address the root causes and are rigorously implemented, if repeat incidents are to be prevented. If remedial actions are impractical to implement immediately due to, for example, procurement delays on long-lead items of equipment or other reasons, additional interim safety measures may be appropriate until the remedial actions are fully implemented.

2.3 SUMMARY

In order to conduct an effective incident investigation and prevent incident recurrence, it is important to identify the fundamental underlying causes of the incident, i.e., root causes. Understanding models of incident sequences and the concept of barriers (and how they can fail) can assist the investigator's root cause analysis. Investigators should also take care to avoid potential pitfalls in applying principles of causality, such as calling negative events root causes, blaming the human, and stopping at an equipment or procedural failure rather than identifying the underlying management system weaknesses.

3 AN OVERVIEW OF INVESTIGATION METHODOLOGIES

Best practices in incident investigation have evolved substantially, particularly since the 1970s when structured methodologies for process safety incidents were virtually non-existent. Investigators now recognize that, for every incident, there are likely multiple root causes. To identify and understand these root causes and how they interacted to result in that incident, an investigator collects evidence and conducts an analysis of that evidence. Today, organizations use a variety of methodologies to investigate incidents, using combinations of various investigation tools.

This chapter provides a brief overview of investigation tools in simple, generic terms and demonstrates the benefits of using a structured approach. A number of public and proprietary methodologies employ generic tools that are readily available to users.

The following terminology is used throughout this chapter:

Tool—*A device or means used at a discrete stage of the incident investigation to facilitate understanding of event chronology, causal factors, and/or root causes.*

Technique—*The manner in which an incident investigation tool is applied.*

Methodology—*The use of incident investigation tools to analyze the evidence, develop and test hypotheses, identify causal factors, and determine the root causes of an incident.*

When choosing the tools and analysis methodologies to be used in an incident investigation, it is important to recognize that no single tool does everything. Good methodologies use combinations of tools to counteract their individual weaknesses. The choice of methodologies depends on the existing culture within the organization, the specific investigation leaders, level of training resources available, and complexity of the incident.

It is important to understand that the various tools use different types of logic to arrive at the result. These types of logic are intuitive, inductive, deductive, or a combination. Most of the tools described in this guideline are intuitive or deductive.

- Intuitive logic relies on the experience and knowledge of the people involved to identify causes. Brainstorming utilizes intuitive techniques, while structured brainstorming utilizes a combination of intuitive and deductive techniques.
- Inductive logic is characterized as “forward search strategies” for identifying the impact of potential process deviations. Inductive tools can support incident investigation and are especially useful when the evidence and facts of an incident have been exhausted or are not attainable. The team must then rely on inductive reasoning to determine where to search for more information to fully understand the causes and occurrences of the incident.
- Deductive logic looks backward in time to examine the preceding occurrences necessary to produce a specified result. Deduction is reasoning from the general to the specific. In a deductive analysis, it is postulated that a system or process has failed in a certain way. Next, an attempt is made to find out what modes of system, component, operator, or organizational behavior could have contributed to the failure. A typical general application of deductive reasoning to the incident investigation might be: What instrumental or human failures contributed to the over-pressurization of the process reactor? Most of the logic trees are deductive.

The disciplines of engineering and quality control have long recognized the principles of root cause analysis. Some process safety tools for root cause analysis have been borrowed from these disciplines. For example, fault tree analysis was developed as an engineering tool, but its “logic tree” structure has been adapted to meet process safety requirements.

The overall investigation approach within the process safety field is similar across many of the available methodologies. However, differences arise in the particular emphasis. Some methodologies focus on management and organizational oversights and omissions, while others consider human performance issues in more depth. Users may wish to have more than one methodology available and choose the methodology that will be most helpful for a particular incident, depending on circumstances of the incident.

Investigative tools should be practical and relatively easy to use. Investigators may make adaptations to selected tools based on the size, complexity, and needs of the investigation effort. Figure 3.1 provides an overview of investigation tools spanning from unstructured, informal

approaches to structured, committee-based, multiple cause, system-oriented approaches. The following sections of this chapter describe these tools and their history for the categories that are depicted in Figure 3.1.

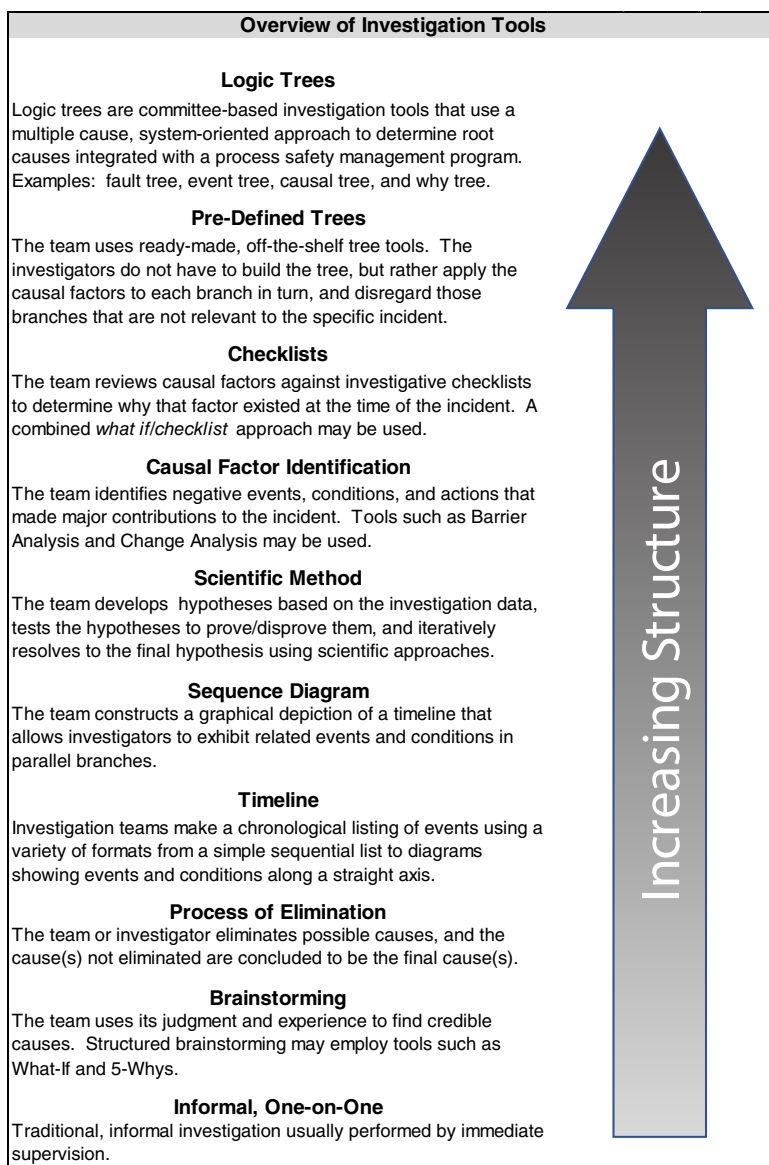


Figure 3.1 Overview of Investigation Tools

3.1 HISTORY OF INVESTIGATION METHODOLOGIES AND TOOLS

Investigation methodologies for process safety incidents have evolved over time, becoming more systematic, objective and scientific. It is relevant to review the history of investigation methodologies to learn from the weaknesses of historical methods and appreciate the approaches in modern methods.

3.1.1 *One-on-One Interview*

The historical approach to investigating incidents was an informal, one-on-one interview, typically between the person involved in the incident and his or her immediate supervisor. This approach has generally been less effective than structured investigation methodologies for process safety incidents, especially complex incidents resulting in, or having the potential to result in, serious or catastrophic consequences. Informal one-on-one interviews are still often used as an approach for investigating low severity incidents, including minor occupational injuries.

The focus of informal, one-on-one investigations has often been limited to determining the immediate remedies that would prevent an exact repeat of the incident circumstances. For example, a common finding may have been that *an operator failed to follow an established procedure*. Based on that finding, the investigator might have proceeded to evaluate how best to motivate this *specific* operator to follow the procedure as a recommendation to prevent recurrence. This informal type of investigation required little time or training, but the weakness of this approach for significant process safety incidents is that it does not determine the fundamental reason for the occurrence of the incident in the first place. If the fundamental reason (root cause) is not identified, then measures cannot be taken to address this fundamental reason, and the incident, or a very similar one, may recur.

3.1.2 *Brainstorming*

Brainstorming is essentially an unstructured tool, but it can provide more perspective and experience than one-on-one investigations. Brainstorming brings together a group of people from diverse backgrounds to discuss the incident and intuitively determine the causes of the incident. The group will typically understand the sequence of occurrences that led up to the incident through a timeline or sequence diagram. The group may also have identified causal factors, and typically focuses on establishing barriers to reduce the risk (probability or consequences) of recurrence.

The disadvantage of unstructured group brainstorming is that the discussion may be dominated by individuals who are not shy about stating an opinion and who may or may not be experts on the subject. Each person may also enter the discussion with a bias that can lead the thinking toward incorrect conclusions. The results of group brainstorming are very dependent on the collective experiences of the group, which may be incomplete if the group is lacking in critical knowledge or a competency skill set. Two different groups may reach two different conclusions as to the cause of an incident. Additionally, unstructured approaches are frequently inadequate for investigating process safety incidents because they produce incomplete and inconsistent results, and often do not determine all the root causes.

While brainstorming has weaknesses as an investigation tool by itself, it has an important role in more structured investigation methodologies. Brainstorming is useful to encourage all investigation team members to express their ideas and opinions, particularly following the guideline to brainstorming that no idea is disallowed. This can be a productive exercise to develop hypotheses based on evidence and observations, which is an inductive reasoning approach. It remains to determine whether hypotheses are true or false through various analysis techniques.

3.1.3 What If Analysis

A slightly more structured brainstorming tool uses What-If Analysis (CCPS, 1992), which involves the team asking “What if?” questions that usually concern equipment failures, human errors, or external occurrences. Some examples are: *What if the procedure was wrong? What if the steps were performed out of order?* The questions can be generic in nature or highly specific to the process or activity where the incident occurred. Sometimes these questions are prepared in advance by one or two individuals, which may also potentially bias the discussion.

3.1.4 5-Whys

The 5-Whys tool is another brainstorming tool used to add some structure to group brainstorming. The tool utilizes a logic tree approach without actually drawing the logic tree diagram. The group questions why unplanned, unintended, or adverse occurrences occurred or conditions existed. Typically, the group asks “why?” about five times in order to reach root causes; hence the name. Judgment and experience are required to use the 5-Whys tool effectively to reach management system failures. The level

of analysis is up to the group and does not always ensure reaching root causes.

3.1.5 Process of Elimination

Process of elimination is another tool that can be used after brainstorming, as well as in structured approaches, to arrive at causal factors. Process of elimination is an integral part of scientific methodologies. It is valid to eliminate (disprove) hypotheses based on information obtained during an investigation. However, it is not sufficient to conclude that the one remaining hypothesis, for which there is no support, is the cause just because all other hypotheses have been eliminated (NFPA 921, 2017). Any hypothesis must have a factual basis including evidence, observations, analysis and testing. Readers are cautioned that process of elimination alone is not sufficient to reach a cause determination.

3.1.6 Timelines

Most methodologies make use of a chronological list of events and conditions leading up to the incident. While a variety of formats have been used by investigation teams, the basic concept of a timeline remains unchanged (see Section 6.2.1).

3.1.7 Sequence Diagrams

Several investigative tools employing graphic displays of incidents have been developed, but only a few are used in the chemical industry. Although diagrams and charts had been in use before 1970 to depict a sequence of events, the National Transportation Safety Board (NTSB) introduced Multilinear Event Sequencing (MES) concepts in the early 1970s to analyze and describe incidents. Another method is the Sequentially Timed Events Plot (STEP) (Benner, 2000; Hendrick, 1987). MES and STEP were originally developed for incidents other than process incidents and are discussed in more detail below.

Multilinear Events Sequencing (MES)

When applying the MES tool, investigators convert observed data into events and arrange the events on a matrix with time and actor coordinates. An event is defined as one actor plus one action. Actors can be people or things, and actions are what the actors did. As data defining an actor and what the actor did are acquired, each new event is positioned on its actor row on the matrix and positioned horizontally under the time it started. This displays what

people or things did in the appropriate sequence, showing time and precede/follow relationships.

The MES matrix can be located on a wall, board, large paper or computer. The investigators use cards or sticky notes to record a layout of the events. Often investigators transfer the display to a computer for further processing. As new information becomes available, the investigators simply update the original card or insert a new card on the matrix.

As events are added, the investigator also adds arrows to link interacting or coupled events. By convention in MES, arrows always flow from the earlier event (causal events) to the later events (effect events) and from left to right. The linking arrows show the flow of the interacting events, or causal flow, from the earliest to the final event on the display. Gaps define data that are still needed. Question marks are used to show uncertainties for data which are needed, or for which no valid data can be developed. A final necessary and sufficient logic test determines the completeness of the display. The tested display is then the best description and explanation of what happened that can be developed by the investigation. Problems and potential changes to improve performance are identified and defined by examining the real relationships within each coupled event pair or set. Each potential change is noted on the matrix with "recommended action diamonds" to indicate where in the accident or incident process improvement opportunities exist (see Figure 3. 2).

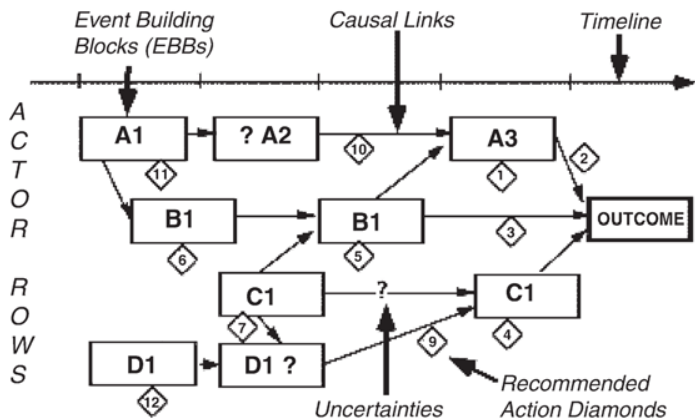


Figure 3.2 Schematic of an MES display (Benner, 2000)

Various interpretations of MES concepts are known as Events & Causal Factor Charting (E&CF) (Buys, 1978), or Causal Factor Charting for short (Johnson, 1980). The E&CF chart displays, in a logical progression, the necessary and sufficient events and conditions required for an event to occur, and has been adopted as one of the tools of several methodologies for process safety incident investigation.

Sequentially Timed Events Plot (STEP)

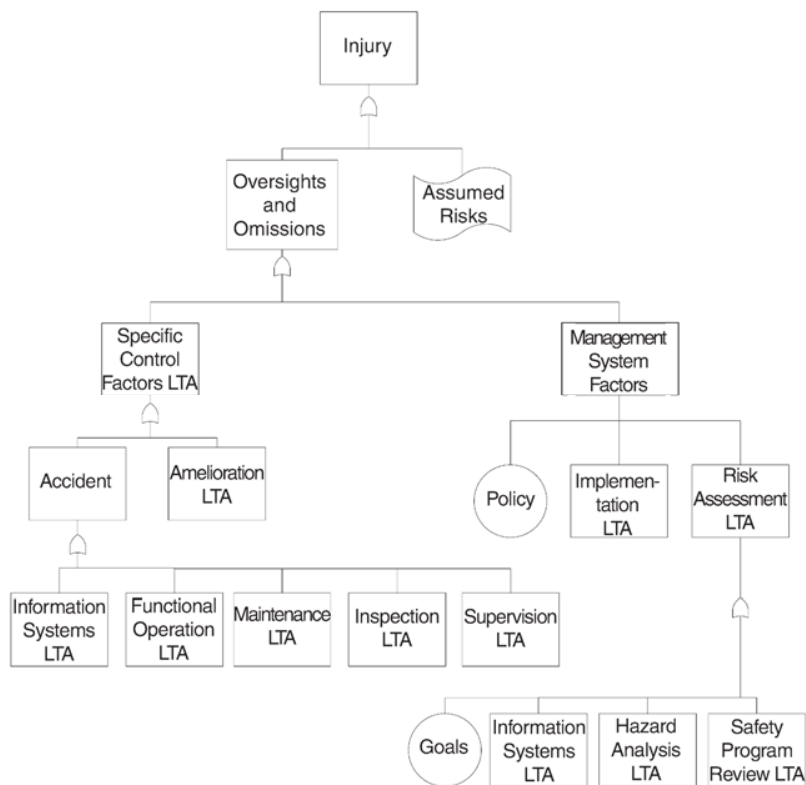
Sequentially Timed Events Plot (STEP) (Hendrick, 1987) is a multilinear events sequence-based matrix display. It evolved from the 1975 MES concepts, but only events are displayed because conditions or states are changed by actions. The matrix entries focus on the behaviors or actions, which produced the undesired outcomes that would have to be changed to improve future performance. The STEP procedures are part of the latest MES investigation process.

3.1.8 Predefined Trees

The Management Oversight and Risk Tree (MORT) tool was developed by the Department of Energy (DOE) for the investigation of occupational incidents at DOE sites (Buys, 1977). A simpler Mini-MORT variation was subsequently developed to reduce complexity (Ferry, 1988). Although MORT is loosely based on fault tree analysis (FTA) logic, it represents one of the earliest predefined trees. Many of the process safety incident investigation tools used in the chemical and allied industries today are based upon concepts similar to MORT.

The MORT diagram starts with the incident, which is equivalent to the top event in FTA. The second step consists of an OR-gate, and the investigator must choose between *assumed risk* or *management oversight and omissions*. The next decision point, another OR-gate, separates *what happened* from *why* it happened. The *what happened* category addresses the controls that should be in place, while *why* considers general management system factors. Eventually, the tree breaks down each of these factors until root causes are reached, which could take up to 13 levels of the tree.

An example of a segment of the Oversight and Omissions portion of the MORT tree is shown in Figure 3.3. Today, there are several versions of the MORT predefined trees available from public and proprietary sources.



Note: LTA = less than adequate

Figure 3.3 Top Portion of the Generic MORT Tree

3.2 TOOLS FOR USE IN PREPARATION FOR ROOT CAUSE ANALYSIS

A number of tools are used before commencing the root cause analysis. These tools include timeline and/or sequence diagram development, the scientific method, and, if using a predefined tree, causal factor identification. These tools are introduced below.

3.2.1 Timelines

An early phase of an incident investigation involves developing a preliminary timeline or chronological description of the sequence of occurrences that led to the failure. This requires collecting evidence through interviewing

witnesses and examining all relevant evidence (equipment, documents, process data, surveillance video, etc.) to piece together the circumstances of the incident in chronological order. This timeline development can range from a simple list of occurrences in sequence to diagrams showing occurrences and conditions along a straight axis.

Development of the timeline should start as soon as facts emerge about the incident. By starting early, the investigator will become aware of gaps in the sequence of occurrences and investigate further to resolve the gaps. Construction of the timeline is an iterative activity in which the timeline is refined and adjusted as the team gains a more complete and accurate understanding of the actual incident scenario and sequence of occurrences leading to it.

Timelines alone do not identify the causal factors or root causes of an incident. They are best used in conjunction with other tools, described in the following sections. See Section 8.4 for guidance on how to organize data with a timeline.

3.2.2 Sequence Diagrams

Sequence diagrams are a more elaborate graphical depiction of a timeline, and they allow the investigator to present related events and conditions in parallel branches. These sequence diagrams are also known as *causal factor charts*. Sequence diagrams show not only the timeline of events but also the connections between events, actors, and conditions using a worksheet. - Typically, sequence diagrams construction starts at the end and works backward, identifying the immediate contributing events first. Like timelines, construction of a sequence diagram may start as soon as facts emerge about the incident to identify gaps for resolution. It is important to choose a format that may be easily updated and revised as new evidence is gathered, such as using sticky notes on which a single event or condition is written. Like timelines, sequence diagrams do not identify root causes, and therefore they should be used in conjunction with other tools. The mechanics of these tools are relatively easy to learn, but the investigator should avoid locking into a preconceived scenario. See Chapter 8 Section 8.4 for guidance on how to organize data with a sequence diagram.

3.2.3 Scientific Method

The scientific method is a general problem-solving method used in many scientific fields in which a problem is first identified, and observations,

experiments, or other relevant data are then used to construct or test hypotheses that purport to solve it. Emphasis on the use of a scientific approach in investigations has increased due to court rulings in the United States that require experts to have a scientific basis for their opinions. NFPA 921, the *Guide for Fire and Explosion Investigations*, has incorporated the scientific method as the key approach for fire and explosion investigations (NFPA 921, 2017).

As an overview, the scientific method involves developing hypotheses based on investigation data including witness accounts, observations, measurements, recorded data and analyses. Hypotheses are then tested to determine if the hypothesis is true or not. Multiple hypotheses are considered. The process is often iterative with findings from one hypothesis suggesting an alternative hypothesis. The process is complete when all hypotheses have been tested and either proved or disproved. The final hypotheses provide the basis for identifying causal factors. Chapter 9 describes the scientific method in detail as it is used most extensively with evidenced analysis.

The scientific method does not replace the use of timelines or sequence diagrams. Rather, the scientific method is complementary to the use of timelines and sequence diagrams.

3.2.4 Causal Factor Identification

When using a predefined tree methodology for root cause analysis, once the evidence has been collected and a timeline or sequence diagram developed, the next phase of the investigation involves identifying the causal factors. These causal factors are the occurrences and actions that made a major contribution to the incident. Causal factors can involve human errors, equipment failures, undesirable conditions, and failed barriers that led to the incident. Causal factors point to the key areas that need to be examined to determine what caused that factor to exist.

There are a number of tools, such as Barrier Analysis (Dew, 1991; Trost, 1985) and Change Analysis (Kepner, 1976), that can assist with the identification of causal factors. The concepts of incident causation encompassed in these tools are fundamental to most of the investigation methodologies. The simplest approach involves reviewing each unplanned, unintended, or adverse item (negative event or undesirable condition) on the timeline and asking, *“Would the incident have been prevented or mitigated if*

the item had not existed?" If the answer is yes, then the item is a causal factor. Process safety incidents often involve multiple causal factors.

Causal factor identification tools are relatively easy to learn and easy to apply. A challenge is ensuring that one or more causal factors are not overlooked, which would ultimately lead to missed root causes. A potential mistake is that an inexperienced investigator could potentially assume that suppositions are causal factors, when the supposed event or condition did not actually occur.

3.3 STRUCTURED ROOT CAUSE ANALYSIS METHODOLOGIES

Once preparations for root cause analysis are complete, there are various ways to determine root cause using the timeline/sequence diagram and, if applicable, identified causal factors. The modern approach to root cause investigation is to use a more structured and comprehensive team approach when identifying root causes. Scientific principles and concepts are applied to determine root causes and to develop recommendations to prevent recurrence. Effective investigations use tested data analysis tools and methodologies to seek the identification of multiple causes. The investigation should use a systematic approach, which may also be prescriptive. An organization may specify the approach that they feel best suits their manufacturing processes, organization and culture. As a rule, application of a systematic approach results in:

- Implementing sound process safety management principles, and
- Applying consistent and accurate investigative effort.

The root cause analysis tools include checklists, predefined trees, and team developed logic trees. Chapter 10 provides a comprehensive treatment of root cause analysis. An overview of root cause analysis methods is provided below to give readers a basic understanding before reading the chapters on organizing an investigation and collecting data.

3.3.1 Checklists

Checklist analysis tools can be a simple means to assist investigation teams as they conduct root cause analysis (CCPS, 1992). Each causal factor is reviewed against the checklist to determine why that factor existed at the time of the incident.

The advantage of checklists is that they are simple to use and the investigation team does not require a lot of training to use them. The checklist provides structure to the investigation team and keeps the team focused. Another advantage is consistency among investigations (e.g., different teams would reach the same conclusion). With consistent application of checklists, the results of investigations can be easily trended using the standard categories (and subcategories) on the checklist to identify recurring problems at a facility.

A disadvantage is that a checklist may allow an investigation team to jump to conclusions and does not provide the opportunity to think “outside the box.” Checklists cannot envision every conceivable circumstance, and investigators may find that they need to add a causal factor not contained in the checklist they are using. It is also tempting to use the checklist too early in the investigation, before all causal factors have been identified. Determining *what* happened and *how* it happened is done **before** determining *why* it happened. Otherwise, the team will think that it has identified the right root causes, when in reality, not all of the root causes have been determined.

Checklists should be used carefully because, to the casual observer, they can imply blame. This is contrary to the intent of discouraging blame-seeking in a root cause investigation.

Checklists may also be used to supplement other tools; for example, checklists on human factors may be used in conjunction with logic trees. Similarly, checklists may be used in combination with structured brainstorming tools such as What If/Checklist and Hazard and Operability (HAZOP) Analysis (CCPS, 1992). It is also a good practice to apply a tool like the 5-Whys to the root causes identified from the checklist to verify whether they are truly root causes.

3.3.2 Predefined Trees

There are several predefined tree tools available from public and proprietary sources. Some of the predefined tree tools are listed in Table 3.1. Most of the predefined tree tools are prescriptive and list potential root causes for consideration among their branches. This offers the investigator a systematic method of considering the possible root causes associated with an incident. A strength of this approach is that it encourages investigators to contemplate a wide range of causal factors, not just those that come to mind through brainstorming. The investigator does not have to build the tree, but

rather applies the causal factors to each branch in turn and identifies those branches that are relevant to the specific incident.

Like checklists, the comprehensiveness of the various predefined trees varies. Some are very detailed with numerous categories and subcategories, whereas others may not fully reach root causes. This is hardly surprising, as the predefined trees are essentially a graphical representation of numerous checklists, organized by subject matter, such as human error, equipment failure, or other topics. The more comprehensive techniques were developed from many years of incident experience and management system experience across the chemical and allied industries.

The advantages of predefined trees are that they may bring expertise into the investigation that the team does not have, and, by presenting all investigators with the same classification system, greater consistency is encouraged among investigators. Largely, the technique ensures a comprehensive analysis and simplifies statistical trend analysis of the collected data. A disadvantage of predefined trees, as with a checklist, may be a tendency to discourage lateral thinking if the incident involves novel factors not previously experienced by those who developed the original tree.

The use of predefined trees, overall, requires fewer resources and less prior training than the non-prescriptive techniques involving team-developed trees that are discussed below. Some organizations have taken a generic, predefined tree and structured it along the lines of the company's management system. The effectiveness of a predefined tree is dependent on how well the tree models the data and system of dealing with the incident. When choosing a predefined tree, the user should confirm that the tree models the technology and system of the user.

3.3.3 Team-Developed Logic Trees

Logic tree analysis is a top-down, analysis in which an undesired state of a system (e.g., injury, fire, explosion, or toxic release) is analyzed using Boolean logic to combine a series of lower-level events. Logic trees can vary over a wide range from simple trees to complex fault trees. Most start at the end occurrence (e.g., injury, fire, explosion, or toxic release) and work backward until a point is reached at which the team agrees it would be unproductive to go further.

Logic trees are best developed using a multi-discipline team. Starting at the end event, the discussion is guided by asking "Why?" and recording the results in a tree format. The general approach encourages investigators to

contemplate a wide range of causal factors but relies on group discussion. This makes its success dependent upon the experience and knowledge of the team. These tools recognize that incidents have multiple, underlying causes, and the investigation attempts to identify and implement system changes that will eliminate recurrence not only of the exact incident, but of similar occurrences as well.

There are five main strengths to a logic tree approach.

1. It provides the ability to separate a complex incident into discrete smaller events (segments) and then to examine each piece individually.
2. It allows the investigation team to understand how the causes worked together to allow the incident to occur.
3. It improves the quality of investigations by directing the focus past the immediate surface causes to the underlying root causes and management system failures, and mandating a search for multiple causes.
4. It offers a clear record that the investigation team understands the incident through the logic diagram/tree.
5. It provides an opportunity to include human factors in the incident investigation process.

The disadvantages of logic trees center on their dependency on the cumulative expertise within the assembled investigation team and the team's ability to compile facts related to the incident. No technique can be a substitute if the team does not have the requisite knowledge and experience. Logic trees can also be somewhat time-consuming to develop and may not use a consistent set of categories and subcategories, making trend analysis of recurring problems difficult.

Examples of logic trees—Why, Causal, Event, and Fault Trees—are discussed below in order of increasing rigor.

Why Tree

The Why Tree provides a simple method for depicting the logical relationship between causes and effects of an incident (Nelms, 1996). The process starts by displaying all direct causes and associated consequences in separate boxes. A drill-down question that asks “why?” challenges each box. Plausible explanations are entered into new boxes attached by straight lines to the

subject or receptor box above. Ultimately, the page will fill up with several boxes attached by straight lines.

Unlike a formal fault tree, this method is empirical and does not require logic gates to be established. All boxes are scrutinized to determine their validity. If the content of a box is refuted by facts, it is crossed off with an appropriate explanation. Otherwise, the boxes are left connected to show the logical progression upward toward an incident.

The tree development process ceases at the base of the why tree where fundamental management systems are identified. The investigation team should then focus its efforts on the rigor and quality of the management systems that could have prevented the incident. Recommendations are developed to address system deficiencies and these are tested against the why tree.

Causal Tree

Causal Trees were developed in an effort to use the principles of deductive logic found in Fault Tree but make it more user-friendly. Causal tree methods rely on group discussion among experts from different fields, including workers, witnesses, supervisors, process safety specialists, and subject matter experts. Starting at the end event, and working one level of the tree at a time, the group asks three questions:

1. What was the cause of this result?
2. What was directly *necessary* to cause the end result?
3. Are these factors (identified from question 2 above) *sufficient* to have caused the result?

In recognition that most incidents have multiple root causes, the team is generally required to identify a minimum of three factors; one from each of the following categories: organizational, human, and material factors.

Causal trees may be drawn from top to bottom, left to right, or right to left. Connectors such as AND- and OR-gates are often omitted. Some methods use only AND-gates.

Event Tree

Another type of logic tree, the event tree, is an inductive technique. Event Tree Analysis (ETA) also provides a structured method to aid in understanding and determining the causes of an incident (CCPS, 1992).

Each event, such as equipment failure, process deviation, control function, or administrative control, is considered in turn by asking a simple yes/no question. Each is then illustrated by a node where the tree branches into parallel paths. Each relevant event is addressed on each parallel path until all combinations are exhausted. This can result in a number of paths that lead to no adverse consequences and some that lead to the incident as the consequence. The investigator determines which path represents the actual scenario. Generally, a qualitative event tree is developed when used for incident investigation purposes.

Since inductive reasoning is used to construct the event tree, not all pathways will lead toward a true conclusion. Simply because a pathway is included in an event tree does not mean that it is a correct pathway. The scientific method should be applied to disprove or prove each pathway. Chapter 2 contains an example of an event tree in Figure 2.1.

Fault Tree

Fault Tree Analysis (FTA) provides a structured method for determining the causes of an incident (CCPS, 2008; Browning, 1975; Arendt, 1991; Vesely, 1981). The fault tree itself is a graphic model that displays the various combinations of equipment failures and human errors that can result in an incident. While the fault tree starts at the undesired event and works backward to identify root causes, the event tree looks forward to display graphically the progression of various combinations of equipment failures and human errors that result in the incident.

The undesired event appears as the top event and the tree is drawn from top to bottom. Two basic logic gates connect event blocks: the AND-gate and the OR-gate. The facts dictate the structure of the incident diagram and limit the influence of presupposed conclusions invariably drawn by team members before all of the facts are identified and logically matched. Logic rules are used to test the tree structure.

The term *fault tree* means different things to different people. Some use the term to describe trees that have frequency terms included. These quantitative trees can be solved mathematically to provide a frequency of the incident. However, for incident investigation, the term commonly refers to a qualitative tree, albeit a tree that rigorously follows logic rules.

3.4 SELECTING AN APPROPRIATE METHODOLOGY

As mentioned previously, no single tool does everything. Methodologies often use combinations of tools to address all facets of an investigation and counteract the various individual weaknesses of the tools involved. Table 3.1 provides an alphabetical listing of the various methodologies and types of tools they offer. Livingston (Livingston, 2001) provides a review of many of the techniques that may be helpful in choosing a methodology.

Methodologies are chosen based on the:

- organizational culture,
- experience and expertise of the incident investigators, and
- nature and complexity of the incident.

There are a number of common generic features shared by most investigation methodologies, which are presented in Figure 3.4.

Table 3.1 Some Characteristics of Selected Public Methodologies

Methodology	Tools						
	Brainstorming	Timeline	Sequence Diagram	Causal Factor Identification	Checklists	Pre-Defined Tree	Team Dev. Logic Tree
Cause Effect Logic Diagram (CELD) (*Mosleh, 1988)	X	X		X			X
Kepner and Tregoe (Kepner, 1976)	X			X			
Management Oversight Risk Tree (MORT) / mini-MORT (Johnson, 1980), (Buys, 1977)		X		X		X	
Multilinear Event Sequencing (MES) / (Benner, 2000)		X	X				
Multiple-Cause, Systems-Oriented Incident Investigation (MCSOII) (Dowell, 1990) (Anderson, 1991)	X	X		X			X
Schematic Report Analysis Diagram (SRAD) (Toft, 1987)			X				
Sequentially Timed Events Plot (STEP) (Hendrick, 1987)		X	X				
Systematic Accident Cause Analysis (SACA) (Waldram, 1988)					X		
5-Whys	X						

- ✓ **SYSTEMATIC** – Provides a systematic and thorough approach that is applied in an organized and logical fashion.
- ✓ **CONSISTENT RESULTS** – Similar teams working with similar information will be able to produce similar results, not overly influenced by team composition and individual team experience factors.
- ✓ **GRAPHIC DIAGRAM** – Most root cause methodologies apply some type of graphic illustration/diagram to record the specific events, conditions, and relevant facts. This may be a logic tree, cause diagram, or other graphic. In some instances, the logic diagram is combined with the chronology tool (for example, Causal Factor Charting). Causal relationships are applied in constructing and examining the diagram, such as the *necessary and sufficient* tests.
- ✓ **CHRONOLOGY** – Most root cause methodologies call for arranging the facts, evidence, and events in chronological order to be able to understand the scenario.
- ✓ **ROOT CAUSE TEST** – Most root cause methodologies will provide a specific definition of the term root cause and will require examination for confirmation that the causes that have been identified as root causes are indeed root causes.
- ✓ **MULTIPLE CAUSES** – Most current methods recognize the concept of multiple root causes.
- ✓ **HUMAN FACTORS** – Most current root cause methodologies will address the human reliability and human performance aspects that are involved in the occurrence.
- ✓ **MANAGEMENT SYSTEMS** – Most current root cause investigation techniques emphasize the need for examining the administrative management systems that were involved in the occurrence, and will evaluate these systems for any inherent weaknesses or defects.
- ✓ **CHECKLISTS** – Root cause investigation methods often include a set of integrated and comprehensive checklists (or accompanying reference documents) to ensure that common generic causes and issues are considered.
- ✓ **QUALITY ASSURANCE** – A comprehensive root cause methodology will often include a component to ensure that the method is being applied properly.

Figure 3.4 Common Features of Investigation Methodologies

To ensure effective incident investigation and identification of root causes, addressing three key challenges can guide the overall investigation strategy to be selected:

1. *“What” happened?*
A component for describing and schematically representing the incident sequence and its contributing events and conditions.
2. *“How” it happened?*
A component for identifying the critical events and conditions (causal factors) in the incident sequence.

3. "Why" it happened?

A component for systematically investigating the management and organizational factors that allowed the critical events and conditions to occur (root causes identification).

Finally, in selecting an appropriate incident investigation methodology, consider whether the method facilitates the identification of management system and organizational inadequacies and oversights. The methodology should specifically identify factors that influence and control an organization's risk management practices and procedures.

3.4.1 Methodologies Used by CCPS Members

The Center for Chemical Process Safety (CCPS) conducted a survey of its membership and other chemical processing companies in preparation for the second edition of this book in 2003. Based on the responses, some general observations can be made about incident investigations:

- Companies reported using an average of two or three different methodologies for both major and minor incidents. The surveyed companies used both public domain and proprietary tools and methodologies.
- The most popular methodologies use different combinations of the tools described in Table 3.1 as well as proprietary tools.

The methodologies used today provide improved results over simplified techniques such as informal, one-on-one interviewing. Most current methodologies have adopted a battery of tools for application at particular stages of the investigation process. As a minimum, a tool representing the incident sequence is used prior to identifying causal factors (also known as critical factors), to which root cause analysis is subsequently applied.

In general, the companies surveyed use one of two approaches to determine root causes. The first involves timeline construction followed by logic tree development. The second involves timeline construction, identification of causal factors, followed by the use of predefined trees or checklists.

4 DESIGNING AN INCIDENT INVESTIGATION MANAGEMENT SYSTEM

This chapter describes how to build and implement a practical management system for investigating process safety incidents. The ultimate goal of incident investigation is to prevent future incidents by communicating and applying the learnings from present investigations. The quality of lessons learned is dependent upon the knowledge and experience of the investigation team. Effective incident investigation can best be accomplished by establishing an investigation management system that assists in achieving the following seven objectives:

1. Encouraging employees to report all incidents, including near-misses.
2. Ensuring that investigations accurately determine what happened.
3. Ensuring investigations accurately identify causal factors and root causes.
4. Ensuring investigations identify and recommend preventive measures that reduce the probability of recurrence and/or mitigate as appropriate for the potential consequences.
5. Communicating the investigation findings.
6. Ensuring follow-up actions are taken to resolve all recommendations.
7. Establishing continuous improvement practices that evaluate effectiveness of recommendation implementation and the overall management systems.

The items in this list are essential to maintaining a well-designed incident investigation program. A high priority should be to promote reporting and investigation of near-miss incidents, to learn from these events, and improve performance *before* a substantial loss occurs.

The incident investigation management system should be described in a written document that defines the roles, responsibilities, protocols, and specific activities to be carried out by personnel performing an incident investigation. This chapter highlights the importance of leadership and management's responsibilities with regard to the incident investigation system. This chapter also discusses management system content and proven methods for implementing a management system.

Figure 4.1 depicts a typical view of the management system model used throughout this book.

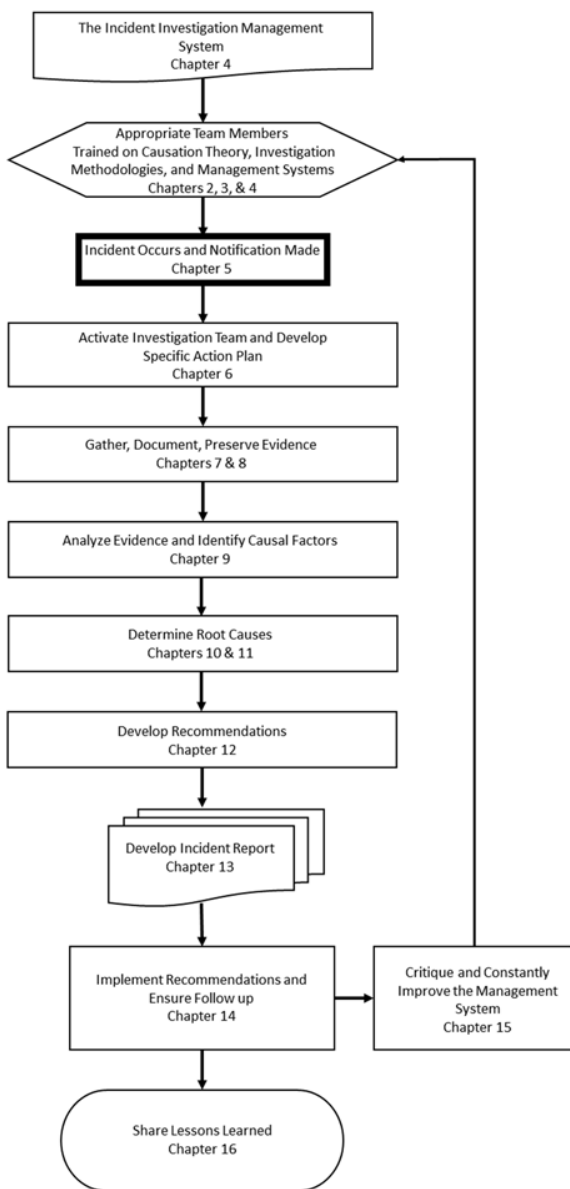


Figure 4.1 Management System for Process Safety Investigation

4.1 SYSTEM CONSIDERATIONS

4.1.1 *An Organization's Responsibilities*

Incident investigation is only one of the many elements of a process safety management program (CCPS, 2007), and is notably one that plays an essential role in identifying overall management system weaknesses on a continuous basis. Establishing a high quality incident investigation program begins with management's support, commitment, and action. To demonstrate support, it is common practice to establish a written policy regarding incident notification, investigation, and dissemination of findings; to communicate this policy to the workforce; and to sustain the policy over time by committing resources for continuous improvement (see Chapter 15). This is often expressed in a formal statement written to achieve the following goals.

- Communicate management's commitment to prevent recurrences by determining causal factors and root causes, evaluating preventive measures, and taking follow-up action.
- Recognize the importance of implementing investigation findings as a strategic risk control mechanism.
- Strongly support reporting and investigating near-misses.
- Clearly focus on finding causal factors, root causes, and management system weaknesses, while avoiding assignment of blame.
- Endorse sustained commitment of resources for the investigation program, including training team members. This supports employee participation in the investigation program and the appropriate and timely implementation of recommendations.
- Emphasize the value and necessity of communicating and sharing the lessons learned from the investigation to all that could reasonably benefit.
- Support a system to ensure that all recommendations and findings are resolved and that decisions and actions are documented.
- Establish a mechanism to foster continuous improvement.

Management demonstrates support for this policy by nurturing an atmosphere of trust and respect that encourages openness in reporting incidents throughout the organization. Failure to achieve this positive atmosphere may result in hidden incidents and low or no reporting of near-misses, which results in lost learning opportunities that could have potentially led to avoidance of future accidents.

4.1.1.1 *Management Commitment*

Management demonstrates commitment to an investigation process by visibly re-affirming the value of the company's reporting and investigation policies, recognizing individuals who support the system, and applying continuous improvement practices. Periodic reviews and reevaluations of the incident investigation management system are necessary to ensure that it continues to function as originally intended and achieves the desired results. Periodic reviews provide:

1. Verification that team composition was suitable and effective.
2. Verification that investigations are identifying correct causal factors and associated root causes.
3. Verification that all action items resulting from recommendations are completed, documented, and effective.
4. Assurance that documentation exists explaining why a recommendation was rejected, modified, or replaced after its original inclusion in an incident investigation report.
5. Early detection of both positive and negative trends. An example would be increased number (or frequency) of near-misses (actual, as well as those not reported) in a particular area or process.
6. Verification that lessons learned are shared as appropriate.
7. Opportunity for continuous improvement for the investigation system itself.

4.1.1.2 *The Benefits of Management's Commitment*

Management's commitment to a systematic incident investigation system results in benefits such as:

- fewer or less severe worker injuries and illnesses,
- fewer or less severe environmental issues,
- reduced worker and corporate risk,
- greater return on investment capital,
- increases in process capability and uptime (less business interruption),
- improved product quality,
- reduced costs, and
- an enhanced image in the eyes of employees, industry, and the public.

These benefits will be realized with a proactive, dedicated, and sustained commitment of resources. The incident investigation management system should help managers:

- develop a clear understanding of the organization's commitment,
- understand the specific responsibilities of each level of the organization in regard to the management system,
- proactively address near-misses,
- recognize, accept, and address root causes, and
- persistently follow up on recommendations to ensure their effective resolution.

Participation of upper-level managers helps promote a sense of sponsorship and assists in establishing investigations as a normal task within a manager's or supervisor's duties. Promoting sponsorship reduces the tendency to perceive investigations as primarily the domain of a narrowly focused group of full-time investigators. For example, one company requires that a senior business unit manager (a refinery manager or chemical plant manager) lead any fatality investigation with the support of a specially trained root cause analyst. At that company, all business unit managers receive a minimum level of training in the conduct of these investigations—*no exceptions*.

Management's continuing endorsement and approval of the program is essential. It is beneficial to reaffirm that management understands and values the concepts of incident investigation on a periodic basis since changes in company leadership may affect the level of awareness and emphasis on incident investigation.

4.1.2 Workforce Responsibilities

Employees should understand the provisions of the incident investigation management system and relevant standards, procedures, guidelines and practices. Where specified, employees should attend training programs and drill exercises.

Employees and contractors involved in, or learning of an incident, should be required to report details of the incident immediately to their supervisor. The supervisor would customarily be responsible for initiating further action to mitigate the immediate hazards, initiate incident notification, and begin investigative actions.

4.1.2.1 Notification

Notification should follow the company protocol to report details of the incident internally or externally to specific individuals or organizations. The circumstances of the incident and the progress of the investigation should also be communicated via the company's incident reporting system and/or the incident management/emergency response system.

The term *report* can have several meanings. Sometimes, the term could mean a verbal initial notification or communication to alert the organization that an incident has occurred. The term also refers to the final, formal written incident investigation report. The term report still causes confusion when discussing regulations. For example, US OSHA requires a notification report within 8 hours following a fatality incident or within 24 hours for in-patient hospitalization, amputation, or eye loss. The reporter should make a written documentation of any verbal communication, noting the time, person involved, extent of information disclosed, and any special instructions or requests made by US OSHA at the time of notice. US OSHA further requires a written *report* for each work-related injury or illness that is severe enough to be recordable (29 CFR 1904, OSHA, 2000).

Many regulatory agencies require *immediate notification*. However, the application of the term is inconsistent. Some jurisdictions require formal notifications for certain levels of injuries within a specified period of time. Other jurisdictions require immediate notice when certain quantities of hazardous materials are released.

Regulatory requirements vary by community, locale, state, and country. The specific extent (number of agencies), format, and timing of all external notifications should be identified beforehand, including contact information, and incorporated into the incident investigation and/or other applicable management systems. With this information readily at hand, the proper notifications may be made quickly and accurately when an incident occurs. Records of notifications and any follow-up communications should be preserved.

Internal notifications, sometimes called alerts or *flash reports*, are trigger mechanisms for starting specific portions of the incident investigation management system and for decision making. Obviously, medical treatment of injured personnel and stabilization of the incident site always takes priority over other activities if there is a conflict regarding the use of available resources during the early stages of an incident. These notification alerts may

be initiated for incidents such as those which result in serious injury or illness, spill or release with consequential damage, or public exposures.

Initial notifications (see Chapter 5 for details) should be part of the company's emergency response plan, but given the nature of notification requirements, updates may extend into the incident investigation stages. The incident investigation management system should address how to handle these communications and how to coordinate with facility emergency response plans.

4.1.2.2 Notification Recipients

Notifications may include the following.

Internal

- Within the facility to summon emergency responders
- Within the site to start administrative response
- To the company headquarters and administrative departments to start the investigation, advise in-house counsel, and initiate other responses

Typical management systems include guidelines for external notification and communications. Coordination may be required to address each respective parties' investigative needs.

External

- Resources for mutual aid emergency response
- Neighboring facilities
- Neighboring community, as needed
- Family members of impacted personnel
- Regulatory agencies, as required
- News media where appropriate
- Insurance carriers

4.1.3 Role of the Management System Developers

One way to achieve the support of management is to include managers in development activities. Developers lead teams to establish an entire incident investigation management system or to upgrade one that is already in place. In either case, developers need top management's support. System

developers prepare their team by researching the basic incident investigation principles and priorities. This book is a good resource for orienting a development team. Developers can provide leadership to help the team determine which investigation methodologies best fit the particular culture of their organization.

4.1.4 Integration with Other Functions and Teams

An active incident investigation will touch other functions within the organization. Preplanning for this interaction begins during the development stage of the management system by identifying known areas of mutual interaction. The management system developers should review other existing management systems such as those listed below to identify opportunities for integration and communication.

- Crisis Management
- Emergency response
- Environmental protection
- Employee safety
- Security
- Regulatory compliance
- Insurance interactions
- External media communications
- Corporate legal policies and procedures
- Engineering design and risk reviews (such as process hazard analyses or management of change reviews)
- Accounting and purchasing practices
- Quality assurance
- Hazard Identification and Risk Analysis (HIRA)

One approach is to mesh all investigation and root cause analysis activities under one incident investigation management system. Such an integrated system should address all four business drivers: (1) process and personnel safety, (2) environmental responsibility, (3) quality, and (4) stakeholder interests. This approach works well since techniques used for data collection, causal factor analysis, and root cause analysis, can be the same regardless of the type of incident or business sector (i.e. not just petroleum or chemicals). Many companies realize that causal factors and root causes of a product quality or business continuity, etc. incident may also share a commonality with occupational or process safety incidents.

An integrated approach also helps to avoid redundancy regarding assignment of responsibility, authority, or priorities. It also makes it easier to report occurrences, as the reporter does not need to know the occurrence classification in order to determine who to notify. While an integrated management system can have several benefits, the components shown in Figure 4.1 are considered a best practice and thus should remain as the foundation.

4.1.5 *Involvement by Regulatory Agencies*

Regulatory and legal considerations should be addressed in the management system and such issues need to be monitored for changing requirements. Government agency attention to industrial incidents has steadily increased in a number of jurisdictions due to new and revised safety and environmental regulations. The global regulatory landscape varies widely by country and region. Some have very specific requirements for reporting, documentation, and investigation. As with all regulatory and legal issues, it is best to ensure the management system provides provisions and procedures for legal counsel throughout the investigative process.

In some circumstances, outside organizations and agencies that have the authority and responsibility to enforce safety or environmental legislation will carry out their own investigation. Inspections or subsequent enforcement may be inevitable. Enforcement may be civil or criminal. This depends on incident severity and whether there are allegations regarding failure to comply with regulations. A facility where a process safety incident occurs can face multiple agency inspections, such as overlapping federal and state/provincial agencies, or worker safety and environmental protection agencies. Where an incident has resulted in serious injury or death or significant environmental damage, government prosecuting agencies could also decide to become involved. Finally, there is also the potential for civil litigation, particularly by contractors or members of the community surrounding a facility where an incident occurs.

Companies have specific legal rights during investigations by government agencies. Legal counsel can help companies to determine their rights and obligations, and can assist in preparing for investigations and on-site inspections. The incident investigation team should consult legal counsel to determine work processes that will ensure all parties' concerns are addressed. As a minimum, the legal department should be consulted at the beginning and the end of the investigation process for all significant accidents. One issue common to both the regulatory and legal concerns is the additional

responsibility a corporation assumes once it has increased knowledge of a hazard or remedy. Failure to act on this knowledge may result in much more significant legal and regulatory consequences.

The management system can include actions for companies to take when preparing for an agency inspection. Whether or not to consent to an immediate entry by government inspectors in the aftermath of an incident is a difficult question to answer in any situation. It is impossible to answer generically. Consider involving legal counsel in these situations. Remember that the incident site and evidence may come under regulator control. Facility managers should be aware of the company's rights with regard to unreasonable searches and seizures. A government entry into and search of a facility in the wake of an incident may be unreasonable. It may be appropriate to refuse to consent to entry in some cases. In others, it may be appropriate to consent to the government entry under specific conditions. The conditions might include limits on the scope and duration of the inspection or specific agreements about the taking and sharing of photographs and interviews of employees. Of course if the visitors have one, the terms of a government agency warrant must be followed. In general, cooperating with an agency seeking to perform an investigation is the best approach. In the long term, this approach can help forge a good working relationship with the agency.

Whether or not the agency is admitted to the facility by the consent of the facility or under a warrant, the agency's purpose should be kept in mind. That purpose may not be the same as that of the company incident investigation team. The company seeks to identify the factors contributing to the incident and the underlying causes. The agency also seeks to identify regulatory violations and evidence that may lead to an enforcement action. A regulator's approach to incident investigation has to be different from the company's as "proof beyond a reasonable doubt" is required if a criminal case is justified. Of course, both parties want to ensure that lessons are learned to prevent future incidents. Especially when an accident causing death or personal injury has occurred, government investigators are likely to assume that a preventable condition caused the incident, that the condition violated a statute or regulation, and that regulatory penalties should be imposed.

Agency involvement presents challenges from the facility's perspective. Facility personnel need to manage the incident and its aftermath, but may also be asked to divert resources to accommodate agency personnel. Personnel should cooperate with authorities but should avoid volunteering unnecessary or unconfirmed information. Plant staff may be asked

questions that are premature or outside the scope of their knowledge or experience.

The government agency will seek to interview employees. Unless subpoenaed to testify, employees may not be required to submit to interviews. Moreover, employees are entitled to have counsel, either company counsel or their own, present during agency interviews. The company should inform employees of these rights in a factual way that does not obstruct the government's investigative process. Consider involving legal counsel in these situations.

In addition to conducting interviews, the government agency may also seek documents and physical evidence. Without a warrant, government investigators may or may not be authorized to take documents. Consider involving legal counsel when the governmental agency requests documents. Generally, a facility should allow reviewing and copying those documents that the facility is required to keep and make available to the agency. Such documents may include copies of process hazard analyses, prior incidents, and prior compliance audits. Requests for other documents should be accepted in writing and considered by management and counsel. Procedures should be implemented to track any documents supplied to an agency.

Many chemical processing facilities use nonproprietary technologies that present common hazards. This allows for meaningful sharing of incident investigation findings throughout the industry. The management system should address methods for sharing incident causes and lessons learned through appropriate channels so that others can benefit. It is often a challenge for a company's management to share the details of investigations due to litigation concerns. However, when similar facilities might benefit, finding a way to share displays a company's interest in driving improved industry safety performance. In addition to litigation issues, practical logistics sometimes make it difficult to communicate lessons learned within and between companies. Determining which people or companies have a potential interest in the incident and learnings can sometimes be problematic. Despite these challenges, broad communication of investigation findings is a recognized good practice.

4.2 TYPICAL MANAGEMENT SYSTEM TOPICS

As stated in the introduction, the incident investigation management system is a written document that defines the roles, responsibilities, protocols, and specific activities to be carried out by personnel performing an incident investigation. The management system may include a purpose statement, definitions, incident classifications, and investigation responsibilities. It provides the structure for activities such as evidence gathering, witness interviewing, and data control as well as standard practices for notification, reporting, and follow up. The following sections summarize the recommended elements of a management system for incident investigation.

4.2.1 *Classifying Incidents*

When developing an incident investigation management system, it is important to define common terms and classifications (ASSE Dictionary, 1988). Several incident categories can be used to develop a classification system. Classification has three main purposes:

1. Determining the significance of the incident and the resulting consequences. This often dictates team leadership, size, composition, and investigative techniques.
2. Determining how investigation results will be communicated and to whom (including regulatory-required communications).
3. Provide consistent data for trending and other analytics.

The system should describe specific mechanisms for deciding to activate an investigation team and the team composition for each incident classification. There should also be a mechanism that describes required internal and external notification. This is usually captured in a procedure and associated routing forms. The incident investigation management system should specify:

- Who will make the notification
- Who is to be notified
- How and when they are to be notified

Chapter 5 provides descriptions, incident classifications, and examples of functions and organizations that might need to be notified.

4.2.2 Specifying and Managing Documentation

The management system should specify documentation requirements for interim data and work products of the investigation. The company's legal staff may have a valuable opinion on this guidance or they may offer case-by-case opinions. For example, the legal department may wish to be involved with witness interviews and physical evidence collection and management. Certain documents or evidence may need special attention due to potential litigation.

It is important not only to document investigation activities appropriately, but also to properly manage all documents and evidence developed by the investigation team. The team needs to develop a control system to track all documentation and evidence. A log should be developed, and every piece of evidence or documentation should be given a unique identifier number/code and entered into the log.

Legal counsel should also be consulted on the scope of distribution lists of documents that are prepared by the team. If the investigation is being conducted under attorney-client privilege, counsel will determine the scope of those who need to be on distribution lists. Do not forward any documents, emails, communications or information to any other person unless expressly permitted by legal counsel. Otherwise, such distribution may waive attorney-client privilege and/or work product. It is important to keep control of preliminary copies and draft reports issued for team review and comment. A good practice is to include a full distribution list on each copy, so that receivers of the document know who else has been copied. This is especially important on sensitive documents related to accidents. In addition to the use of headers and footers noting confidentiality, expert investigators include DO NOT COPY on some documents and always use the pagination style that notes the identification "*this is page x of y*" markers on certain documents. A chain of custody should be maintained for all evidence that is moved to a different location or transferred to a different party. It is likely that items could be sent for examination by interested parties for testing by a specialist. It is essential to preserve the condition and quality of the evidence as well as to know precisely where it is at any given time.

Incident investigation document retention is another important issue to consider. Lawyers and investigation team members are likely to disagree about which documents to keep and how long to keep them. Retained documents may be useful to maintain corporate memory; however, retained documents may also create increased legal liability. Each organization must

develop and implement its own policy. In addition, there may be regulatory requirements. In the United States, EPA and OSHA have established certain retention requirements for those facilities subject to process safety management regulations. Under these regulations, incident investigation reports must be retained for five years.

Other important documentation issues include:

- the minutes of team deliberations,
- official notifications to external agencies,
- the method for tracking documents and evidence requested, received, or issued by the team,
- the final report,
- resolution of findings, and
- retention of institutional knowledge (lessons learned).

4.2.3 Legal Considerations

The investigation management system should emphasize that the team needs to conduct a thorough and effective investigation while minimizing legal implications. Preplanning and a well-designed incident investigation management system using the guidance provided above will help to manage legal issues that may arise during the course of an investigation.

To help protect the confidentiality of an incident investigation, as needed/appropriate, a request should be made by the company (either to an in-house or outside legal counsel), for legal advice on matters arising from, or related to, the incident. The lawyer should then direct the activities to be undertaken, making it clear that the information is to be provided to counsel for the purpose of providing legal advice to the company or preparing for litigation, or both.

Key points to remember are listed below.

- Get an attorney's advice at the beginning of the investigation and decide early if the attorney-client privilege /work product doctrine is to be used. If so, ensure that all investigation team members are trained on how to manage documentation in accordance with these provisions. Be aware of potential litigation issues.
- Use a good document management system. Utilize the principles of careful communication; stress to the team that almost any document generated could become part of the public record.
- Have good procedures for managing the handling and chain of custody of all evidence.

- When appropriate, discuss employee interviews and potential discoveries with an attorney before and after the interview to properly provide legal protection.
- Have a plan in place for how to interact with outside agencies, including the media.

4.2.3.1 *Use and Limits of Attorney–Client Privilege*

Some documents created by an incident investigation team may be subject to disclosure to:

- government agencies under their regulatory authorities, and
- plaintiff’s lawyers under the rules of discovery that govern litigation.

Communication with counsel is critical as there are a variety of issues that counsel may be dealing with that the investigator is not. The appropriate use of the attorney–client privilege during an investigation can help promote frank and open communication between the incident investigation team and legal counsel, and through legal counsel to management. The primary advantage of the attorney–client privilege is to allow and legal analysis of the situation to be protected. If outside experts are needed to assist in the investigation, legal counsel will be responsible for retaining the expert. The experts may then assist counsel in the defense of any legal actions that may follow. When documents are prepared at the request of counsel or when communications are transmitted to counsel in order to obtain legal advice, the extent of protection afforded by Attorney-Client Privilege depends on the legal jurisdiction. The attorney–client privilege exists so clients can communicate frankly with their attorney. Usually, the attorney can provide sound representation without the substance of those communications becoming public. In most European countries, however, the concept of privilege is extremely narrow and in the United States, judges may apply privileges sparingly. Therefore the investigation team should ensure they have clear guidance from the counsel on how to conduct communications in accordance with privileges appropriate for involved jurisdictions.

Note that, if a document is considered privileged information, the organization may want to severely restrict access to that document to maintain that privilege. Because there are many attacks on the use of the attorney–client privilege, each investigation team member should treat any

note, email, report or communication as if it would become a public document available to the press, government or the public in general, including competitors. Regulatory requirements may dictate that reports on process safety are to be shared with workers, depending on jurisdiction and type of incident.

Other protections that may apply include *The Work Product Doctrine* and *The Self-Critical Analysis Privilege* (Adams, 1999). The work product doctrine was created to protect materials prepared in anticipation of litigation from discovery. Although technically speaking a lawyer might not have to be involved for material to acquire work product protection, attorneys may need to be involved for several reasons. First, some rulings have favored the involvement of a lawyer. Second, involving a lawyer suggests the matter should not be considered ordinary course of business. Third, the lawyer's involvement emphasizes that the work is being done in anticipation of litigation.

4.2.3.2 Recording the Facts

There may be a perceived conflict between the need of the investigation team to gather information quickly and record observations versus the legal risk the company could face from hastily prepared notes or erroneous preliminary conclusions. Haste in making notes without clearly distinguishing between factual observations and speculation can cause unnecessary legal risk to the company. The company could spend a great deal of time and money trying to explain the hasty notes in litigation or enforcement actions. The investigation team should take accurate notes and record only facts. Any opinions or speculation should be clearly noted as such. Facts cannot be altered, but conclusions can change as the investigation continues. In some cases, the legal counsel should review documents that are prepared by the investigation team for outside distribution as well as the final official reports as they are drafted. The guidance by legal counsel can help to limit unnecessary liability. Typical guidance to investigators regarding note and report writing may include:

- Using header and footer designations to identify official incident team internal documents. Legal counsel may recommend adding statements such as, "Privileged and Confidential—Attorney–Client Privileged Information" or other designators on each page of certain documents
- Refraining from use of superlatives and inflammatory language; rather, use factually accurate statements
- Refraining from use of judgmental words with special legal

- meanings such as *negligent, deficient, or intentional*
- Refraining from assigning or implying blame
 - Refraining from offering opinions on contract rights, obligations, or warranty issues
 - Refraining from making broad conclusions that are not supported by the facts of this investigation
 - Avoiding unsupported opinions, perceptions, and speculations
 - Refraining from *overly* prescriptive recommendations; that is, allowing for alternative resolutions of the problems and weaknesses found
 - Following through on each recommendation and documenting the final resolutions, including why a recommendation was rejected or modified
 - Reporting, investigating, and documenting near-misses as well as accidents to demonstrate the company's commitment to incident prevention
 - Refraining from making personal notes or any other information unrelated to the incident investigation

4.2.4 Describing Team Organization and Functions

The incident investigation management system should include a description of how a team is organized and how it functions. The team organization, composition, and functions should be structured to provide flexibility based on the particular incident and the management system should emphasize that fact. The system may describe an investigation team's basic objectives and priorities. When establishing the charter for a major investigation, it is important to remember that the team members are not full-time, professional investigators. Some team members may only serve on such a team once during their entire work career.

The team leader's responsibilities should be explicit. Normally a team leader chosen for more serious or more complex incident investigations will be independent from the operation or facility where the incident occurred. Actual team composition may vary significantly based on the nature of the incident, chemical process involved, and the degree of technical sophistication used to control the process. This flexibility of team composition is an important feature of a well-designed incident investigation management system.

The investigation process generally follows a problem solving process sequence as described in Chapter 3. Once the team has developed the

specific investigation plan, evidence is gathered. These two activities consume much of the team's time.

The management system may define some specific team functions and responsibilities. Some examples are listed below.

- Selecting and developing an incident investigation plan defining the scope of the investigation
- Identifying support resources
- Developing evidence handling procedures
- Establishing communication channels both within the company and with outside groups
- Conducting witness interviews and gathering/analyzing evidence
- Summarizing findings and recommendations in a report
- Evaluating the initial containment actions.

Implementation, and associated follow-up on resolution of all recommendations, is an essential component of a management system. As written, it should specifically address the assignment of responsibility for follow-up. In rare cases, the incident investigation team will retain responsibility and authority for the final resolution of the recommendations. However, in most cases the primary responsibility will shift to a designated member of management who is not a member of the incident investigation team. If management rejects or significantly modifies the recommendations from an incident investigation team, management has the responsibility to discuss these changes with the team to determine if the team needs to clarify their recommendations.

4.2.5 *Electronic Process Data and Control Systems*

Electronic systems monitoring, recording, and controlling chemical and petroleum processes have evolved immensely and rapidly in just a short time. The operations reliance and complexity of these systems justifies special considerations when formulating team structure and functions.

The investigation management system should include provisions for the following considerations:

- Assignment of an electronic instrumentation and data processing specialist as a team member
- Assignment of an operator capable of interrogating stored data and producing trends of process conditions
- Pre-arranged assistance from vendors, contractors, and consultants

- Priority preservation of raw (uncompressed, unaltered buffer) data on an expedited basis, i.e., before memory capacity causes overwriting data or averaging data to a historian archive
- Preservation of data related to operator control input and associated control element movements
- Preservation of data logs, e.g., alarm, programmable logic controller action, safety instrumented system functioning, set point excursions, etc.

Specific electronic evidence identification and preservation suggestions are contained in Chapter 8.

4.2.6 *Defining Training Requirements*

Management proves its commitment by action. Management committed to learning from incidents will establish a high-quality incident investigation training program. This helps to ensure that the management system is understood and implemented as designed. Each job position's training on the incident investigation system will vary in the level of detail and scope. Persons assigned to lead roles on incident investigation teams should be targeted to receive the most concentrated training. Periodic refresher training is an opportunity for management to reinforce commitment, demonstrate support for the organization's policy and philosophy on incident reporting and investigation, and discuss modifications and improvements in the investigation process based on lessons learned from performing investigations.

Typical training agendas for management and employees who may report an incident but are not intended to be designated investigative team members, can be brief. Special training may be indicated for those employees and functions that will interface with the incident investigation team during an investigation. These may include, for example, emergency response teams, fire brigade, maintenance, security, site safety, site industrial hygiene, public relations, legal, and environmental. Table 4.1 describes general guidelines for the content of training sessions for various functions.

Table 4.1 Suggested Training for Effective Implementation

Complex Incidents Investigation Team Leader Training	Moderate/Minor Incident Investigation Team Leader Training	Incident and Near-miss Reporting/ Notification	Awareness Training
<p>These leaders will handle the most complex incidents (top 10% or less)</p>	<p>These leaders will handle low to moderate complexity incidents (90% or more of the incidents)</p>	<p>All operations and maintenance staff; appropriate purchasing, accounting, and other staff</p> <p>Individuals who are expected to identify and report all incidents, including near-misses.</p> <p>Some of these individuals may become team leaders or members or may be interviewed during an investigation.</p>	<p>All staff individuals may fill any role in the system; this is the starting module of training</p>
<p>Training Agenda</p> <ul style="list-style-type: none"> • Investigation planning • Data protection • Data collection • Causal factor determination • How to fill gaps in data • Root cause identification • Writing recommendations • Using the incident database • Programmatic issues such as reporting, communication, legal issues 	<p>Training Agenda</p> <ul style="list-style-type: none"> • Data collection • Causal factor determination • Root cause identification • Writing recommendations • Using the incident database 	<p>Training Agenda</p> <ul style="list-style-type: none"> • Near-miss definitions and examples • The learning value of incidents • No blame approach • Root causes are management system failures • Incident reporting system 	<p>Training Agenda</p> <ul style="list-style-type: none"> • What is changing in how you approach incidents? • What can each person do to help the system work? • Expected impact to most jobs

The management system should describe minimum initial training and refresher training. High quality training for potential team leaders, members, and supporting personnel helps ensure success. The level of detail contained in the management system may vary. For example, it may provide a brief summary and then refer to a training management system document or position curricula for the detailed training information. A summary of training topics for each group is provided below:

Management

This group needs to be familiar with the concepts, policies, and extent of commitment from executive management; specific assignments of responsibility and resource commitments associated with process safety incident investigation; the employer's incident investigation management system; and report content, including what constitutes clear actionable recommendations.

Site - Management

"Management" topics above should be supplemented with basic investigation concepts, investigation methodologies, causation concepts, fact-finding vs. fault-finding philosophy, general internal legal protocols, and media relations/communications policies and practical exercises.

All Employees

This group includes operators, mechanics, first-line supervisors, auxiliary staff groups such as technicians and engineers, and middle-level management. These are employees that are in a position to first notice an incident and may provide support activities vital to the success of an investigation team. They should be trained on how to differentiate an accident from a near-miss. They should also be educated on the requirements of employer's investigation management system, with a focus on what to do once an incident is identified, and the site's incident reporting procedure.

Investigation Team Members (Including Team Leader)

This group is intended to be a designated pool of specifically trained investigators to be called into service as needed. Additional training focuses on the support functions of an investigation, particularly on how to effectively gather and preserve data. For instance, team members would be trained on how to preserve evidence, interview peers, develop test plans, and develop sampling procedures. Depending on their role in the investigation, some team members may need training in data analysis and the use of specific

investigative tools. It is a good practice to identify internal and external resources available to assist with these tasks. Suggested topics include:

- An overview of the company incident investigation management system
- Incident investigation concepts, including the fact-finding, not fault-finding philosophy
- Specific investigation techniques used by the organization
- Interviewing techniques
- Gathering evidence
- Developing and testing hypotheses
- Identifying Causal Factors
- Using tools to determine causal factors and root causes
- Writing effective recommendations
- Documentation and report requirements
- The roles of the team members
- Confidentiality of the investigation

Team member training may also include “role playing” for activities such as witness interviews, conflict resolution, and confidentiality issues. Team members should understand that they are not expected to perform at the level of full-time professional investigators. They should feel free to request help or training as soon as they recognize a need. After initial training and accreditation, brief periodic refresher-training sessions or tabletop role-playing drills are a good way to reinforce the training objectives. Summary training topics may include:

- Site-specific incident investigation plan
- General roles and responsibilities
- Specific assignments for team members such as interviewing, photography, and other roles
- Evidence preservation and handling protocols
- Locations for evidence storage
- Controlling communications from team members

Investigation Leaders

Some organizations break this training into two or more levels, with team leaders given more training if they will lead investigations of higher level or complex incidents. Leaders learn how to determine the appropriate investigation methodology, how to gather data, how to analyze data for causal factors, how to determine root causes, and how to develop effective recommendations and reports.

Leader training deserves special attention. Training for leaders could include role-playing for witness interviews, conflict resolution, applicable laws, regulator powers, and confidentiality issues. They should feel free to request help or training when needed, especially at the early stages of an investigation. Other investigators may handle low to moderate complexity incidents. Leader training for low to moderate complexity incidents usually consists of classroom training plus experienced coaching during their first few investigations. These individuals can also benefit from participating as team members on an incident investigation led by an experienced leader. Low complexity incidents may require one helper (team member) to support the leader in data gathering and analysis. Individuals who will lead major or complex investigations should be able to handle almost any incident within the company. The training for this level usually consists of considerable experience leading low to moderate complexity incidents and additional classroom training and coaching by a more experienced investigator during their first few major investigations.

In some cases, employees, rather than supervisors, lead investigations for lower level incidents. Companies have found it beneficial for employees to feel ownership of the investigation results. This philosophy helps encourage workers to report more near-misses by reducing the fear caused when a supervisor leads the investigation. Most incidents are low complexity. Many of these are near-misses and benefit from investigation by persons who are closest to the process.

Chapter 6 provides details on the selection, and organization of incident investigation teams.

4.2.7 *Emphasizing Root Causes*

Identifying causes is a major objective of the investigation process, and this should be specified in the management system. Initial selection (or custom development) of the root cause determination process will require special attention to the concept of multiple causes and to underlying system-related causes. The approach should emphasize finding management system weaknesses and failures versus placing blame on individuals. Some employees may need to adjust to this approach, particularly if past methods did not encourage discovery of causal factors and associated root causes. Everyone involved in the resolution process for recommendations needs to understand the concept of multiple root causes of an incident.

Chapter 10 describes methods to determine root causes. The management system should include information on the root cause approaches that the company has adopted, which could vary depending on incident classification. Training in the selected root cause approaches is needed for investigation team members who will facilitate a root cause analysis.

4.2.8 *Fostering a Blame-Free Policy*

Fault-finding and disciplinary action should not be part of the investigation process. The management system for investigation should ensure that a blame-free policy is clearly stated and enforced. The team should look beyond human error for the associated performance management system weaknesses that failed to prevent the error.

Disciplinary action may be appropriate if negligent, malicious or criminal intent is positively identified. An example would be when an investigation reveals horseplay, practical jokes, fights, or even sabotage was among the causes. These activities have no place in any workplace and are especially undesirable in the chemical processing industry. It is most likely that a company's employee handbook, human resources documents, or union contract addresses these situations and communicates the policy in advance of an incident. In short, the investigators determine the facts, analyze to identify root causes, and make recommendations. Managers then may react to those recommendations. When human actions such as discussed above are called into question, discipline might be appropriate, consistent with the company's Human Resource policies.

4.2.9 *Developing Recommendations*

Identifying and evaluating practical recommendations are critical team activities. The management system should include attention to evaluating proposed recommendations. For example, recommendations should be effective in eliminating the root causes of the incident or near-miss while being practical, cost-effective, and within the control of the organization. Ineffective recommendations may only serve to transfer the hazard or even create a new hazard that was not present before the initial incident. The management system for incident investigation needs a built-in mechanism to require safety analyses of the proposed recommendations. A tie should exist between the facility's incident investigation management system and their management of change (MOC) and PHA program. The investigation team needs to evaluate whether proposed recommendations

are practical and will adequately address the root causes. Additionally, site management should ensure that any changes to equipment or procedures as a result of recommendations are properly evaluated before implementation.

The space shuttle *Challenger* disaster is a classic example of the need to evaluate proposed recommendations. Before the *Challenger* incident, NASA was aware of the poor performance (Winsor, 1989) of the ring joint seal systems from previous near-miss incident investigations. In a well-meant effort to improve the safety margin, a decision was made to increase the pressure test from 100 to 200 psig (6.8 to 13.6 atmospheres) after the ring joints were reassembled. In reality, this recommendation actually decreased the integrity and reliability of the ring joint seals by increasing the deformation of the sealing putty. An effective MOC analysis might have uncovered this increased risk.

Chapter 12 provides guidance for formulating effective responses to investigation findings.

4.2.10 Recommendation Responsibilities

The incident investigation team has the responsibility to develop practical recommendations and submit them to management. The investigation team may include comments on resuming normal operations and/or suggesting recommendations to be implemented before restarting the process. It is then the responsibility of management to:

- review the recommendations;
- approve them as written or ask for clarification, revisions, or alternative solutions;
- establish process safety re-start and ramp-up (normal capacity), criteria (CCPS, 2007)
- approve the final recommendations;
- assign action item priorities and target completion dates;
- allocate resources; and
- track implementation status and effectiveness.

Regulatory agencies usually take special interest in the status of previous recommendations made at the same facility or similar recommendations made across the organization. Lawyers give this issue significant attention. The assumption is that prudent and responsible managers should promptly

apply lessons learned from an incident, not only at a facility level, but also across the organization.

Employees are affected by the recommendations. Their responsibilities include:

- Using new or modified equipment properly.
- Abiding by procedural improvements.
- Giving feedback to management when something is not working as expected.
- Sharing their knowledge when they find a better or safer way to address the problems identified in the investigation

In summary, developing the recommendations is a responsibility of the incident investigation team. Accepting and implementing the recommendations is a management responsibility. The inclusion of the elements of the recommendation in daily work practice is the responsibility of each individual affected by the recommended action.

4.2.11 Implementing the Recommendations and Follow-up Activities

Resolving recommendations and following up on their effectiveness is a cornerstone of all management systems. Once a recommendation has been accepted for implementation, a clear, auditable document trail should be established and maintained. The recommendations should not only be implemented but also, they need to be sustained. For lasting results, it is wise to audit implemented recommendations periodically to ensure that they are continuing to achieve the intended objectives.

It is the prevailing opinion of many regulatory agencies that any changes in the originally accepted recommendation should be thoroughly documented. If a recommendation is modified in scope or time commitment, or is otherwise not implemented as originally planned, then the basis for this decision should also be documented. The concept of an auditable trail is mentioned in regulatory and legal activities. If a recommendation is rejected or modified, the basis for the rejection or change should be thoroughly documented after review with the investigation team. These requirements should be reflected in the incident investigation management system and should be emphasized when personnel at all levels are trained.

The management system should indicate the importance (priority) of the recommendation, assignment of responsibility, and method for verifying and

documenting its resolution. Management should acknowledge observations and endorse findings expressed in the team's written report.

4.2.12 Providing a Template for Formal Reports

Reports that document incident investigations are different from most business and technical reports. Business reports traditionally only address financial considerations. Process safety incident reports, however, can contain a full range of elements: serious injury, fatality, flawed management systems, financial aspects, as well as complex technical issues. Although most business documents could become legal documents, the incident report has a higher likelihood of legal disclosure.

Generally speaking, reports should include enough information to allow a person with no prior knowledge of the incident (but a reasonable level of process knowledge) to understand what occurred, the causal factors/root causes that were identified, and the recommendations made. Consideration should also be given to legal requirements for report content.

The intended distribution and required approval levels should be addressed in the preplanning stages, and should be clearly identified in the written management system description.

Additional specific suggestions are provided in Chapters 12 and 13.

4.2.13 Management System Review and Approval

The management system should be reviewed, approved, and fully implemented by the appropriate company personnel. Investigations can have significant interaction with several other company functions. Each of these groups needs the opportunity to participate in the development of the initial management system through review and comment.

4.2.14 Planning for Continuous Improvement

The management system should promote continuous improvement by including a process for feedback. Each investigation provides an opportunity to evaluate the management system effectiveness. The lessons learned strengthen and refine the management system. It is also valuable to recognize and share the positive aspects of those investigation activities that were especially successful.

To ensure continuous improvement, an evaluation after each investigation should include:

- Team thoroughness in the investigation.
- Team effectiveness in applying the techniques.
- Team preparedness in advance of the investigation.
- Equipment performance during the investigation.
- Supply logistics and quality.

To ensure that the management system continues to provide the intended results, periodic reviews and updates are necessary. This action recognizes that organizations are dynamic, ever-changing, and evolving. Consider the following critique questions.

- Were the investigation techniques applied correctly and fully?
- Did the team accurately determine what happened?
- Did the team find the management system failures that led to the incident (that is, did they get to root causes)?
- Was the team documentation adequate?
- Were the right skills available within the team?
- What other resources could be used next time?
- What should be changed next time?
- Is there evidence to suggest that near-misses are being reported?
- Have there been any repeat events?

Chapter 14 provides guidance on recommendation implementation effectiveness, and Chapter 15 details proven methods for enhancing an incident investigation system.

4.3 MANAGEMENT SYSTEM

Implementing a new or upgraded management system normally begins with training employees, supervision, and management in their respective roles in the investigation program. Implementation also includes development and refinement of the incident data management systems. The data management system should allow users to easily develop consistent reports

and perform queries of incident data to spot systemic trends. Additionally, the management team's endorsement of the incident investigation management system is important when introducing a new or revised system.

4.3.1 Initial Implementation— Training

Implementation of a new or revised management system often begins with presenting training for the four groups described earlier in this chapter.

1. Management
2. All employees in a position to notice and report all incidents (including near-misses)
3. Incident investigation team members
4. Incident investigation team leaders

4.3.2 Developing a Specific Investigation Plan

The incident investigation management system should include guidance on how to develop a specific investigation plan for an incident. The specific plan should include leader and team selection, a designated mechanism for documenting the team activities, deliberations, decisions, communications, and a record of documents requested, received, or issued. The objective of the investigation plan should not be limited to identifying physical causes but extended to underlying management system issues.

The primary objectives of a process safety incident investigation plan should include:

- Identification of the physical causes—process and chemistry
- Identification of the PSM-related multiple root causes,
- Identification of recommendations to prevent recurrence, and
- Assistance in interpreting the recommendations or auditing their implementation as needed

Figure 4.2 offers a typical checklist to use during the planning stage of an investigation of a major complex incident. Low complexity incident investigations do not always call for a formal plan.

The team leader sometimes makes a brief orientation visit and considers numerous factors in developing an investigation plan including the magnitude of potential outside interest in the investigation. Outside interest in the investigation includes three aspects:

1. Legal issues,
2. Contractual issues, such as insurance coverage, and
3. Regulatory issues.

<ul style="list-style-type: none"><input type="checkbox"/> Clarify and confirm priorities<ul style="list-style-type: none"><input type="checkbox"/> Rescue and medical treatment<input type="checkbox"/> Secure incident to mitigate further consequences<input type="checkbox"/> Environmental concerns<input type="checkbox"/> Evidence preservation/Secure the site<input type="checkbox"/> Evidence collection (including interviewing witnesses)<input type="checkbox"/> Regulatory notification protocols<input type="checkbox"/> Legal counsel considerations<input type="checkbox"/> Plan for witness interviews<input type="checkbox"/> Team leader selection<input type="checkbox"/> Team member selection, training, and organization<input type="checkbox"/> Initial orientation tour/visit<input type="checkbox"/> Initial photography<input type="checkbox"/> Plan for evidence identification, preservation, and collection including special handling of time sensitive material such as query control system logs<input type="checkbox"/> Plan for documentation<input type="checkbox"/> Plan for coordination and communication with other functions<input type="checkbox"/> Identify and plan for procurement of team supplies and equipment<input type="checkbox"/> Plan for any special or refresher training needed by team<input type="checkbox"/> Establish checkpoints, timetables, and schedule of progress
--

Figure 4.2 Checklist for Developing an Incident Investigation Plan

The initial site visit is the first opportunity to establish the physical boundaries of the investigation. The team leader should:

- ensure that access to the area is minimized as much as possible, and
- verify that the personnel who enter the incident area are aware of evidence preservation considerations.

One of the most critical issues is clearly establishing which groups have responsibility for which activities and areas. These responsibilities may change during the investigation. The incident investigation team leader needs to ensure that these responsibilities are clear to all groups to avoid duplication of effort or omission of critical activities.

Management's charter to the team should include expectations for accurately reporting investigation outcomes. However, assigning blame or recommending disciplinary actions should not be part of a team's charter. A high performance team should be as independent and autonomous as possible, and the leader should encourage this awareness. This helps to establish an unambiguous signal to all contributors that the investigation process will be implemented impartially. If there is a perception, either rightly or wrongly, that the team is in any way inhibited or intimidated by outside influences, participants and reviewers may question the quality, quantity, and credibility of the information collected.

It is particularly helpful to have an hourly employee from the same (or an adjacent) plant on the team to not only get their valuable input, but also to establish credibility with a wider workforce. There has been a tendency in the past to select staff engineers as incident investigation team members and ignore operators and technicians. Operators and technicians may know what really happens better than others, and their involvement on the team can produce facts that would otherwise not become known. Personnel closest to the incident occurrence, however, may also be those with a personal agenda, so this potential conflict of interest should be considered.

5 INITIAL NOTIFICATION, CLASSIFICATION AND INVESTIGATION OF PROCESS SAFETY INCIDENTS

Timely reporting of incidents, including near-misses, enables management to take prompt preventive or corrective measures to prevent another incident. Depending upon the actual (and potential) incident severity, it may also be necessary for management to notify key stakeholders so that resources can be mobilized to mitigate any adverse effects of the incident, to conduct timely reporting to regulatory agencies, and to initiate the incident investigation.

This chapter describes important considerations for internal reporting of incidents and the process of classifying incidents into categories, which helps employees to determine which stakeholders need to be notified and the type of investigation to be conducted.

5.1 INTERNAL REPORTING

The term *report* can have several meanings. Sometimes the term could mean a verbal initial notification or communication to alert the organization that an incident has occurred. The term also refers to the final, formal written incident investigation document. In this chapter, *reporting* refers to the initial communication that an incident has occurred.

Reporting incidents, including near-misses, is critical to improving safety in the workplace. If incidents are not reported, they cannot be investigated, and corrective actions cannot be implemented. The insights from even minor incidents allow site management to identify where actions and additional resources are required to avoid more serious incidents in the future. When more incidents (including near-misses) are reported, more data is available to identify negative trends in management system and human performance.

It is therefore essential that **all** incidents, including near-misses, are reported to line management as soon as possible by the individual discovering the incident. Leadership plays a key role in creating and sustaining a positive culture of workforce involvement, which promotes incident reporting and drives improved safety performance. If line

management responds promptly and effectively to reports of incidents, the workforce will realize that their concerns are taken seriously. This will encourage continued incident reporting and drive a positive safety culture.

The supervisor, when informed of an incident, would customarily be responsible for initiating further action to alert management, investigate the incident, and take required action. First notification may also need to follow company protocol to report details of the incident to specific individuals or organizations internally or externally including regulatory agencies (see Section 5.3 below).

Not only does incident reporting allow management to initiate remedial measures, it can help to instill a sense of vulnerability to keep the workforce alert to potential hazards and their proper management. Furthermore, the lessons learned from incidents can be shared more widely within the company, and, if appropriate, externally.

All incidents and near-misses should be entered into the company's incident reporting system (such as a database or log). As a minimum, the database or log may record the type of incident, date/time, description, and circumstances of the incident. Additional information could include the stakeholders notified and the incident classification. Other fields may be left blank at this time if the information is not yet available. Examples of types of incidents that may be recorded include, but are not limited to:

- Injury (e.g., first aid, non-disabling, disabling, etc.)
- Fatality
- Occupational illness
- Release of hazardous material from primary containment, i.e., vapor release, liquid spill, solid release (including dust)
- Fire
- Explosion
- Process upset (e.g. flaring, off-spec product/effluent, etc.)
- Property damage (at or above a certain cost level)
- Environmental damage
- Security (trespass, theft, bomb-threat, etc.)
- Community complaint (odor, noise, etc.)
- Near-miss
- Challenge to a safety system (e.g. relief valve discharge or safety trip)

5.2 INCIDENT CLASSIFICATION

Classifying incidents can assist decision-making regarding their management and investigation. Classification systems can vary depending on the company and the site organization. There is no perfect one-size-fits-all system of classification. Traditionally, classification systems assign a category to an incident based on the type of incident or its actual (or potential) severity. In some cases, it may be useful to assign a category based on the nature and complexity of the incident (rather than only its severity) to facilitate the selection of lead investigators and team members with the most appropriate skill sets. In a few cases, the local jurisdiction may mandate a specific approach to incident classification as well as the depth of the investigation. Table 5.1 shows various incident classification schemes.

The incident classification system selected should preferably:

- Be easily understood,
- Include clear examples,
- Detail specific mechanisms to authorize an investigation and who may do so,
- Help identify the investigation approach/methodology, and
- Help determine the composition of the incident investigation team.

In practice, whatever method is used, there may be gray areas in every system. Discovery of new information or changes in perspective during the initial stages of an investigation may lead the team or site management to change the incident classification during the course of the investigation. For example, the team investigating an incident may determine that an actual (or potential) consequence was more severe than first recognized. The management system should provide guidance on how to make changes in incident classifications when appropriate.

Table 5.1 Common Classification Schemes

By System Complexity	By Type of Incident	By Severity	By Local Jurisdiction
<ul style="list-style-type: none"> • High <ul style="list-style-type: none"> -nuclear materials -high pressure (>50 psig) -high temperature (>2000°F) -exothermic reactions -explosive environment -highly toxic -several relief devices -highly automated -several operators • Moderate <ul style="list-style-type: none"> -10–50 psig -100–2000 °F -minor reactivity/toxicity -low probability of explosions -single relief device -1–3 operators • Simple <ul style="list-style-type: none"> -ambient conditions -little/no reactions -nonexplosive environment -single/no relief valve -1–2 operators 	<ul style="list-style-type: none"> • Major release • Minor release • Explosion • Fire • Toxicity • Personnel harm • High potential incident • Safety permit violation • Failure of critical safeguard • Challenge last line of defense • Serious process excursion • Other <ul style="list-style-type: none"> -process upset -quality variation -downtime -offsite consequence -process safety vs. occupational safety 	<ul style="list-style-type: none"> • Multiple fatalities/serious injuries • Fatality • Injury <ul style="list-style-type: none"> -hospitalization -lost work day -recordable -first aid • Evacuation • Shelter-in-place • Reportable to government agency • Levels of business interruption/product losses • Levels of equipment / property damage <p>Note: Examples of the above include CCPS and API RP 754 tiers</p>	<p>Varies by jurisdiction, e.g. USA</p> <ul style="list-style-type: none"> - OSHA PSM, - EPA RMP, - BSEE SEMS, - DOT, etc. <p>Europe</p> <ul style="list-style-type: none"> - Seveso Directive - UK RIDDOR <p>Australia</p> <ul style="list-style-type: none"> - CMHF <p>Canada</p> <ul style="list-style-type: none"> - Environment Canada - Transport Canada - Provincial Regulations

5.2.1 Severity Classification

Classification of an event by actual severity is the most common classification system used by companies to establish when to initiate an investigation, the team composition, and the investigative technique to be used. The benefits of using actual severity to classify incidents include the relative simplicity of categorization and the availability of significant guidance on its use. The main disadvantage of classifying an incident using actual severity alone is

that it does not consider the potential worst-case consequences - what *could* have happened. Potential severity is much more difficult to determine. Hence personnel responsible for incident classification should be knowledgeable in process operations and receive classification training to ensure consistency between different personnel. A broad knowledge of other incidents across industry is also helpful. In addition, the actual severity may not adequately reflect the complexity of the system involved, which could impede selection of the most appropriate investigation team.

Examples of severity classification are illustrated below.

i. CCPS Guidance

CCPS developed guidance on the classification of process safety incidents in 2007 as an industry lagging metric that would become the benchmark across the chemical and petroleum industry for measuring process safety performance. The document (CCPS, 2011) was later updated to broadly align with the first edition of API Recommended Practice 754 published in 2010. Subsequently, API revised RP 754 (see Section 4.2.1.ii) in 2016 and CCPS updated their guidance to align with API (CCPS, 2018).

The CCPS guidance is based on a tiered approach representing the severity of the incident (referred to as “process safety event”) ranging from Tier 1 as the greatest consequence (i.e., lagging metrics) to Tier 4 as proactive performance evaluations (i.e., leading metrics). Tiers 1 and 2 cover process safety incidents with consequences affecting safety/human health, property damage, material release, community impact, and offsite environmental impact. The classification of Tier 1 incidents at four consequence severity levels is illustrated in Table 5.2. These consequence severity levels were selected primarily for reporting company and industry process safety performance purposes, and include a points system to indicate incident severity, which is additive if a single incident impacts several consequence categories.

Table 5.2 Tier 1 Process Safety Event Severity Categories (CCPS, 2018)

Severity Points	Consequence Categories				
	Safety/Human Health	Direct Cost from Fire or Explosion	Material Release Within Any 1-Hour Period	Community Impact	Off-Site Environmental Impact
1 point	<ul style="list-style-type: none"> Injury requiring treatment beyond first aid to an employee, contractor, or subcontractor. 	<ul style="list-style-type: none"> Resulting in $\\$100,000 \leq$ Direct Cost Damage $< \\$1,000,000$. 	<ul style="list-style-type: none"> Release volume $1x \leq$ Tier 1 TQ $< 3x$ outside of secondary containment. 	<ul style="list-style-type: none"> Officially declared shelter-in-place or public protective measures (e.g., road closure) for < 3 hours, or Officially declared evacuation < 3 hours. 	<ul style="list-style-type: none"> Resulting in $\\$100,000 \leq$ Acute Environmental Cost $< \\$1,000,000$.
3 points	<ul style="list-style-type: none"> Days Away From Work injury to an employee, contractor, or subcontractor, or Injury requiring treatment beyond first aid to a third party. 	<ul style="list-style-type: none"> Resulting in $\\$1,000,000 \leq$ Direct Cost Damage $< \\$10,000,000$. 	<ul style="list-style-type: none"> Release volume $3x \leq$ Tier 1 TQ $< 9x$ outside of secondary containment. 	<ul style="list-style-type: none"> Officially declared shelter-in-place or public protective measures (e.g., road closure) for > 3 hours, or Officially declared evacuation > 3 hours < 24 hours. 	<ul style="list-style-type: none"> Resulting in $\\$1,000,000 \leq$ Acute Environmental Cost $< \\$10,000,000$, or Small-scale injury or death of aquatic or land-based wildlife.
9 points	<ul style="list-style-type: none"> A fatality of an employee, contractor, or subcontractor, or A hospital admission of a third party. 	<ul style="list-style-type: none"> Resulting in $\\$10,000,000 \leq$ Direct Cost Damage $< \\$100,000,000$. 	<ul style="list-style-type: none"> Release volume $9x \leq$ Tier 1 TQ $< 27x$ outside of secondary containment. 	<ul style="list-style-type: none"> Officially declared evacuation > 24 hours < 48 hours. 	<ul style="list-style-type: none"> Resulting in $\\$10,000,000 \leq$ Acute Environmental Cost $< \\$100,000,000$, or Medium-scale injury or death of aquatic or land-based wildlife.
27 points	<ul style="list-style-type: none"> Multiple fatalities of employees, contractors, or subcontractors, or Multiple hospital admission of third parties, or A fatality of a third party. 	<ul style="list-style-type: none"> Resulting in $\geq \\$100,000,000$ of direct cost damages. 	<ul style="list-style-type: none"> Release volume $\geq 27x$ Tier 1 TQ outside of secondary containment. 	<ul style="list-style-type: none"> Officially declared evacuation > 48 hours. 	<ul style="list-style-type: none"> Resulting in $\geq \\$100,000,000$ of Acute Environmental Costs, or Large-scale injury or death of aquatic or land-based wildlife

Note: CCPS provides additional guidance on loss of containment, injury/death of wildlife, etc.

Some companies have used the tiered approach to classify incidents to determine the level of internal corporate notifications and the type of incident investigation required. Depending on the actual severity level, the company may elect to notify company executives of more serious Tier 1 incidents (e.g., consequence severity levels \geq single fatality) and adopt a more rigorous and detailed investigation approach than for less severe incidents. This is discussed in more detail in Sections 5.3 and 5.4 below.

While the consequence severity levels in Table 5.2 may be appropriate for oil refineries and petrochemical complexes *for reporting purposes*, the levels of direct costs associated with property damage and environmental impact may be inappropriate *for classifying incidents* in small chemical facilities, such as those comprising one or two process units. Small facilities may wish to use the Tier 2 definition (fire/explosion direct cost \geq \$25,000 to \$100,000) or reduce Tier 1 direct costs by an order of magnitude *for the purposes of determining the type of investigation*.

CCPS has also developed a mobile phone/device App (Process Safety Incident Evaluation Tool) that is aligned with API RP 754 and is available for free download on Apple and Android platforms. A desktop version of this tool with examples, Process Safety Incident Evaluation Tool (version 1.0.0), is also available from CCPS. Some companies may also choose to determine the potential severity of an incident and, depending on the potential severity, adopt a more rigorous and detailed investigation approach than that indicated by the actual severity. The UK Health and Safety Executive (HSE) states that:

*"It is the **potential consequences** and the likelihood of the adverse event recurring that should determine the level of investigation, not simply the injury or ill health suffered on this occasion" (HSE, 2004)*

CCPS guidance for Tier 3 process safety incidents discusses near-misses, and the opportunity of valuable data for improving process safety management systems. In particular, CCPS explains:

"When evaluating process safety near misses, consider the potential adverse impacts. The level of response to a near miss (i.e. investigation, analysis, and follow-up) should be determined using the potential as well as the actual consequences of the event." (CCPS, 2018)

The determination of potential severity can be complicated. It is recommended that personnel responsible for classifying incidents based on potential severity be trained in the classification methodology. CCPS's earlier document provided guidance on how to determine potential severity of a loss of primary containment (LOPC) of a hazardous material (flammable and toxic) (CCPS, 2011). See Appendix G for an extract from this publication addressing the potential chemical impact of Tier 1 process safety incidents.

i. API Recommended Practice 754

The American Petroleum Institute (API) developed a similar guide for process safety performance indicators, incorporating input from CCPS, and subsequently revised and published a second edition of the recommended practice (API, 2016a). The purpose of this document is to identify leading and lagging indicators in the refining and petrochemical industries to drive improved safety performance. API proposes indicators for use at both corporate and a site levels. In addition, API has published a guide for reporting process safety events (API, 2016b). Other industry organizations, including the European Chemical Industry Council (CEFIC, 2016), International Council of Chemical Associations (ICCA, 2016), and International Association of Oil & Gas Producers (IOGP, 2011), have adopted API RP 754, sometimes with minor variations. As discussed in Section 5.2.1.i, CCPS aligned its guidance with API RP 754 in 2018.

Although API RP 754 is intended for standardized reporting of process safety events (i.e., incidents), some companies have used it as a classifying tool for the purpose of determining the type and depth of investigation. As in the case of CCPS guidance, companies may wish to consider potential severity when determining the type of investigation, and small companies may reduce direct cost criteria as appropriate for their operations.

ii. Logic Tree

A few companies use a logic tree approach to determine incident classification and the type of investigation to conduct. An example logic tree is shown in Figure 5.1; it contains simple questions requiring yes/no answers. In this example, actual and potential serious injury and fatality incidents would receive a formal investigation. An unsafe act or behavior with injury and/or fatality potential would have an informal investigation, although at management discretion, it may receive a formal investigation. An unsafe act or behavior with no injury or fatality impact would not be investigated and would be recorded for trend analysis only, unless there is a trend worthy of investigation.

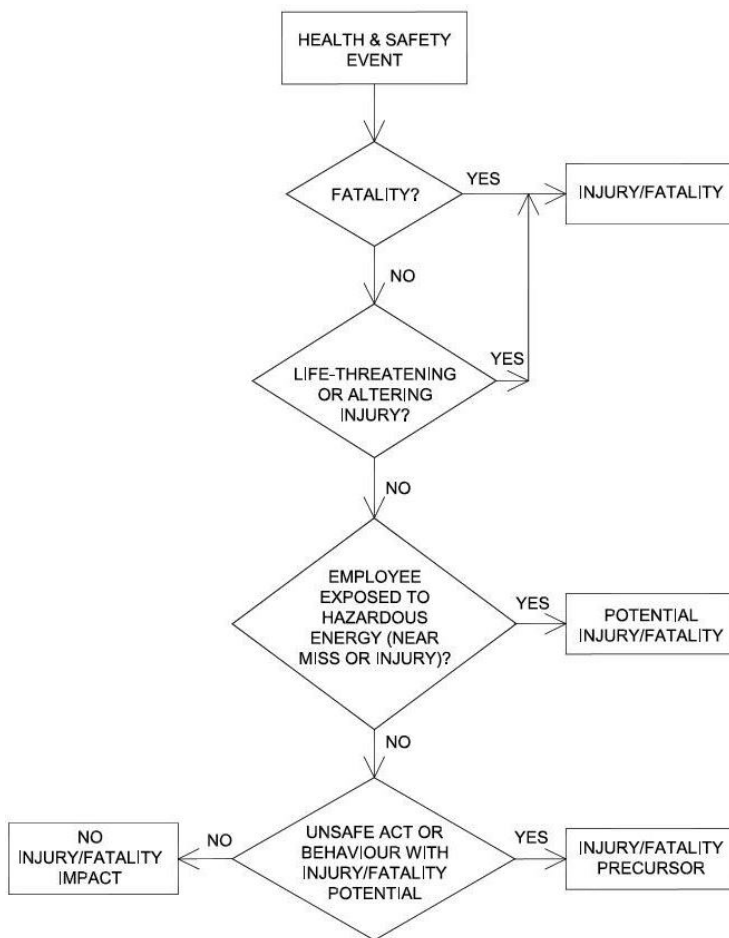


Figure 5.1. Logic Tree for Determining Incident Classification

An example of the criteria used in this logic tree as guidance to answer the yes/no questions is illustrated in a Process Safety Events Levelling Criteria table (Appendix C). This levelling document is used to determine the level of severity of a precursor or potential event that might result in serious injury or fatality in order to establish whether or not it should be investigated.

Typically these precursor and potential events relate to releases during:

- Safe Work Practices (e.g., energy isolation (LO/TO), confined space entry, line breaking, hot work, access control, etc.), and
- Chemical Handling.

ii. Risk Matrix

Another approach to incident classification uses a simple risk matrix (consequence severity vs. likelihood) to determine incident classification. The severity axis varies among companies, and the axis can reflect actual severity or potential severity, in broad sub-categories, for example, ranging from first aid/minor damage to fatality/major damage. An example of the likelihood axis contains an order of magnitude estimate of likely frequency of the incident ranging from once in history of the industry to once per year at the facility. Even for an actual incident, a ranking based on likelihood of recurrence can elevate the risk and classification, and hence the type and rigor of investigation. High severity/high likelihood incidents would receive thorough investigation and root cause analysis, whereas low severity/low likelihood incidents may involve a simpler approach. Figure 5.2 illustrates an example of a risk matrix used for incident classification. Table 5.3 provides the likelihood levels for Figure 5.2.

		Impact			
		4	3	2	1
Likelihood	4				
	3				
	2				
	1				

Figure 5.2 Example Risk Matrix for Determining Incident Classification

Table 5.3 Example of Likelihood Levels for Determining Incident Classification

Category	Description
1 Remote	Has occurred at least once within the industry
2 Rare	Has occurred at least once within the company
3 Unlikely	Likely to occur once in the life of the facility
4 Likely	Likely to occur once per year of the facility

5.2.2 Local Jurisdiction

If a particular regulatory agency becomes involved, additional classification and notification may be required. For example, in the United States, some incidents reportable to the Environmental Protection Agency (EPA) may result in another classification of an incident and require other mandated actions. Similarly, in Canada and Japan, pressure vessel/equipment failures are reportable to the local jurisdiction. The approval loop for the notification report may expand to include legal representatives and the investigation team composition may change to meet specific regulatory requirements or to provide stewardship of the company's interests.

5.2.3 Other Options for Establishing Classification Criteria

In addition to the approaches discussed above, companies use a variety of other means to classify incidents, including, but not limited to:

i. Direct Cost

The amount of direct monetary value of the loss, interruption, harm, or damage is sometimes used as a category. This is similar to CCPS/API's classification for property damage and environmental impact, but is often an internally established value related to insurance coverage deductibles or management financial authorization structure.

ii. Lead Investigator Experience

One alternative classification scheme simply specifies the experience level of the lead investigator based upon the severity of the incident, and then leaves the team composition to the leader. This approach depends upon the leader's experience and training to select the appropriate team members.

iii. Loss of Production

The loss of production may be used as a classification criterion and could be expressed in units of hours, days, or weeks of expected downtime. A further improvement is to estimate both the actual and *potential* severity of the impact of such incidents. Making such a determination is an imprecise effort, and organizations are best served when a decision is made quickly with the evidence at hand rather than waiting for more perfect data.

5.3 INCIDENT NOTIFICATION

Depending upon the severity and type of incident, various stakeholders may need to be notified that an incident has occurred. These stakeholders may be internal (e.g., corporate executives, key departments) and external (e.g., regulatory agencies, partners, local government, etc.). All external notifications should follow the company's policy and procedures for external communications.

Making initial notification in a timely manner can be challenging immediately following an incident. The format and timing of all external notifications should be identified and incorporated into the management system **before** an incident occurs. The corporate emergency response and/or the incident investigation management systems should address how to handle these communications, and how to coordinate with facility emergency response plans. A checklist with key contact names, titles, and phone numbers may be developed and kept up-to-date for this use. With this information readily at hand, the proper notifications can be made quickly and accurately when an incident occurs.

5.3.1 **Corporate Notification**

Initial notifications to the company's headquarters may alert executives and key departments (e.g., EHS, Legal, etc.) that an incident has occurred. Some companies only require notification for more severe incidents, while lesser incidents are simply entered into the company's reporting database. For example, some companies only require executives and corporate departments to be informed of CCPS severity level 1 and 2 incidents (see Appendix G). Such incidents may have implications for the company's reputation and its license to operate and may justify a more thorough investigation approach. Some companies require initial notification within a certain timeframe, typically 8 hours to 1 day.

These internal notifications can be trigger mechanisms for starting specific portions of the incident investigation management system and for other associated decision-making (see Section 5.4 below).

The initial notifications are often based on the actual severity classification of the incident. Sometimes there may be a delay in determining the potential severity until more information on the incident is available. In this case, if the potential severity is greater than the actual severity, a new notification may be required. Some companies require notification of 'high potential' incidents (e.g., CCPS/API Tier 1 \geq single fatality) even if the actual severity was less severe (e.g., lost-time injury or near-miss).

5.3.2 Agency Notification

Depending on the jurisdiction, the regulatory agency(s) may require verbal and/or written communication that an incident of a certain severity has occurred. A timeframe for this communication is often specified and typically varies, for example, 8 hours by US OSHA for a fatality and 24 hours for hospitalization or severe injury. In a few cases a longer timeframe is permitted. For example, in the UK under the RIDDOR regulations (HM Government, 2013), an accident resulting in a fatality or hospitalization of non-workers is required to be reported within 10 days.

In instances where a verbal notification by telephone is sufficient, it is advised that the individual reporting the incident make a written record of this verbal communication, noting the time, person involved, extent of information disclosed, and any special instructions or requests made by the agency at the time of notice. Some jurisdictions may use a recorded line, and the individual reporting the incident should keep a similar written record.

In some jurisdictions, the initial notification may also be the basis for the company to satisfy regulatory requirements on the timely initiation of the investigation process.

5.3.3 Other Stakeholder Notification

Initial notifications to other stakeholders may be appropriate depending on circumstances. These notifications may be managed through the relevant corporate and/or site management system, and include, but are not limited to:

- Family members
- Neighboring facilities
- Neighboring community

- News media (where appropriate)
- Insurance carriers

5.3.4 Other Notifications

Later, when the investigation is at an advanced stage or complete, other internal and/or external notifications may be appropriate, depending upon specific circumstances. At this point, such notifications should be managed through the incident investigation management system. External communications should follow corporate policy and procedures. Examples of later notifications could include follow-up to initial notifications and safety alerts based on interim or final investigation findings related to:

- Incidents that can potentially expose persons to safety risks, and
- Use of specific items of equipment, plant and machinery to help eliminate hazards associated with their use.
- Revised containment action based on new information gathered during the incident investigation

This information can be used to help prevent similar incidents at the subject workplace as well as other workplaces.

5.4 TYPE OF INVESTIGATION

Some companies have different investigation systems and/or different investigation approaches depending upon the type of incident or the incident classification. For example, a company may have different investigation systems for occupational safety, process safety, and equipment reliability. Alternatively, another company may have a more thorough and detailed investigation of a high severity incident than a loss of containment without harm to personnel.

5.4.1 Which Investigation System to Use?

Although some companies may have different investigation systems, the same investigative approach and training may work well for incidents in any facet of a business. There is merit in combining the systems and, in particular, in combining the incident databases since there will be a larger set of data for trend analysis, and common causal factors and management system deficiencies may be more readily identified. This approach can also help ensure that all aspects of an event are investigated appropriately.

A related consideration is that incidents can affect more than one aspect of a business. Table 5-4 illustrates this point for an example incident involving a 1000-lb release of cyclohexane from a decanter system at a polymer production facility. The occurrence did not harm any people and did not noticeably damage the environment, although reporting of the release to regulators was required. The occurrence and the actions taken after the release caused the process to be shut down for about 9 hours and caused 3000 lb. of product to be rejected. (The values in Table 5.4 are from a qualitative scale, where 10 would be very high impact and 0 would be very low or no impact.)

Table 5.4 Examples of the Impacts of a 1000-lb Cyclohexane Release

Business Aspect	Actual Impact of the Incident	Potential Impact of the Incident
Safety (harm to people)	0	10
Environment (harm to nature)	1	3
Quality (harm to product)	3	3
Reliability (harm to process efficiency)	5	10
Capital (harm to property, facilities, equipment)	1	10
Customer Service (harm to relationship with clients)	2	10

From the view of both actual and potential impact, the cyclohexane release affects all business aspects. The incident is a near-miss for safety and a minor or major incident for other aspects of the business. Performing six or more investigations would waste time and resources. Performing one investigation that meets the needs of all business aspects is a simpler and likely more effective approach.

5.4.2 Investigation Approach

Incidents classified as CCPS severity level 1 or 2 (e.g., one or more fatalities) may have implications for the reputation of the company and its license to operate, and may justify a different corporate response and investigation approach. Circumstances that may impact reputation include, but are not

limited to (i) location of the facility, (ii) prior incident history, (iii) media interest, and (v) deteriorating relationship with the government, regulatory agencies, and the local community.

After serious incidents, including fatality(s) and those that impact company reputation or license to operate, corporate executives may activate their crisis management system, involve their legal counsel, and select an investigation team leader and key team members who are independent of the facility that experienced the incident. Furthermore, the investigation may be significantly more thorough than an investigation for a less severe incident. For example, depending on circumstances, a more thorough investigation and root cause analysis may involve some of the following:

- Process sample analysis,
- Fire and explosion forensic analysis,
- Equipment inspection and testing,
- Process simulation,
- Metallurgical analysis,
- Chemical reactivity analysis, and
- Engineering studies.

Some companies manage lower severity incidents, such as those requiring first aid or CCPS level 3 or 4, within the facility and use a simpler, less rigorous investigation approach. Nevertheless, the approach should use proven techniques to identify the root cause(s). Although API Recommended Practice 585 (API, 2014) was written primarily as guidance for investigating pressure equipment integrity incidents, it contains useful guidance on how to investigate low, medium, and high severity incidents.

5.5 SUMMARY

It is important to develop a classification system for the purposes of reporting and also to assist in determining the type of investigation needed. There are various classification systems in use, the most common being those that take into account the actual or potential consequence. The choice of system may also be influenced by local regulatory agencies and industry reporting criteria. The classification criteria, and associated communication and investigation team requirements, should be incorporated into the incident investigation management system before an incident occurs.

6 BUILDING AND LEADING AN INCIDENT INVESTIGATION TEAM

A thorough and accurate incident investigation strongly depends on the capabilities of the assigned team, its organization, and its leadership. Each member's knowledge, technical skills, expertise, and communication abilities are considerations when building an investigation team. This chapter describes some approaches to selecting appropriate personnel to lead and participate in incident investigations and recommends methods to develop their capabilities and manage the team's resources.

6.1 TEAM APPROACH

Whether investigating a major process safety incident with a large team or a minor incident using one or two employees, all incident investigations benefit when the team is capable of applying the chosen investigative methods effectively and consistently. Organizations with effective incident investigation teams can realize benefits in other aspects of their business besides process safety. Performance can be enhanced in product quality, productivity, environmental responsibility, and morale. With each well-performed incident investigation, an organization can add to its accumulated knowledge to prevent future incidents.

The composition and mandate of an incident investigation team should relate to the type and severity of the incident, or, in the case of a near-miss, to its potential severity. Furthermore, the potential for significant learning from the incident investigation, irrespective of the severity of the incident, may also be reflected by the composition of the team. For example, it may not be necessary to assign the most experienced technical personnel to conduct the investigation of an incident involving a minor injury that did not require medical treatment. However, an organization may consider assigning more senior experts to a team investigating a minor gas leak if it highlights major deficiencies in an asset integrity system. Furthermore, if safety performance indicators reveal a *series* of relatively minor incidents that were precursors or may have similar causes, it may be appropriate to conduct a higher level of investigation. By contrast, a major incident involving a very simple process may not require as many investigators as a less significant

one involving a highly complex system. Team selection is dependent on the circumstances, complexity, and severity (actual or potential) of the incident.

Although highly experienced investigators may not be needed for every investigation, seasoned investigators can still support an investigation through consulting, quality assurance, and peer review. It may not be necessary for the lead investigator to be part of the line management team; however, it is important that the leader of the investigation be provided with adequate training, coaching, support and authority by management.

6.2 ADVANTAGES OF THE TEAM APPROACH

There are several advantages to using a team approach when performing incident investigations.

1. **Multiple technical perspectives assist in analyzing the findings**—A structured analysis process is used to reach conclusions. Individuals with diverse skills and perspectives best support this approach.
2. **Diverse personal viewpoints enhance objectivity**—In comparison to a single investigator, a team is less likely to be subjective or biased in its conclusions. A team's conclusions are more likely to be accepted by the organization than the conclusions of a single investigator.
3. **Internal peer reviews can enhance quality**—Team members with relevant knowledge of the analysis process are better prepared to review each other's work and provide constructive critique.
4. **Additional resources are available**—A formal investigation can involve a great deal of work that may exceed the capabilities of one person. Quality may be compromised if one person is expected to do most of the work.
5. **Scheduling requirements are easier to meet**—Deadlines set by management, outside parties, or the team leader may require several activities to be performed in parallel. This demands a team approach.
6. **Regulatory authority may require a team approach**—Specific regulations, such as OSHA's Process Safety Management regulations in the US, call for a team approach. Management needs to be aware of whether a facility falls under such regulations.
7. **Workforce involvement** – Participation in an incident investigation team provides an opportunity to engage with workers, for them to learn, as well as to contribute, and to build support for the recommendations with peer workforce members.

6.3 LEADING A PROCESS SAFETY INCIDENT INVESTIGATION TEAM

An effective incident investigation management system, as described in Chapter 4, depends on many factors, driven by management's commitment, support and actions. A management system that provides strong team leadership and organizational support will help the investigation team to succeed in understanding what happened, determining causal factors and root causes, developing plans to prevent recurrence, and sharing learning both inside and outside the company.

The selection of the team leader for an incident investigation will depend on a number of factors related to the incident, including:

1. Its actual (or potential) severity and complexity;
2. Its health, safety, environmental, or business interruption implications;
3. The anticipated complexity of the investigation.

Various approaches for determining the scope and size of the incident investigation are described in Section 6.5 and Figure 6.1, and the choice of team leader will be a function of the scale and type of incident. However, the general abilities of the investigation leader will be similar and should include the following competencies and qualities:

- Leadership abilities and experience, including process safety experience
- Communication skills with all levels in the organization and other stakeholders (verbal, written and presentation)
- Problem solving/ logical and systematic thinking
- Objectivity
- Planning and organization/ administration
- Commitment to safety
- Technical incident investigation skills
- Conflict management skills and experience
- Ability to handle information with confidentiality and sensitivity

The selection and training requirements for the team leader and the rest of the investigation team are detailed in Section 6.4. Investigation team leaders should be identified and trained for the appropriate investigation types or tiers to which they have been assigned. Ideally, the team leader should be independent of the incident itself, although this may not always be possible or practical, particularly with a lower tier investigation. For

example, the manager of a facility might lead an investigation, but the cause of the incident may be associated with management system problems for which the manager is responsible. Under these circumstances, the peer and senior management review should provide independent oversight and a path to further action, if required.

Often, the investigation team leader's first task is to systematically identify the resource requirements and recommend individuals and organizations that should participate. As with management's selection of the team leader, the leader's selection of the team members will be based on the severity and nature of the incident. The team leader may choose to involve experts on an as-needed basis, allowing them to focus on key areas without affecting their normal work schedule. These experts may be internal to the organization or be contracted from an outside source. Part-time and expert participation should be carefully managed to ensure the scope is defined and adhered to, competing priorities are considered, and costs are controlled.

The organization's incident investigation management system should specify the team leader's responsibilities and authority. Once selected, the team leader should meet with senior management to review and agree on all responsibilities and authority (e.g., selection of team members, financial and technical resources) associated with the investigation, which should then be clearly documented. Typical leader responsibilities may include:

- Ensuring incident investigation activities adhere to company, site, and scene safety practices
- Ensuring that restricted access zones are identified and access is controlled
- Ensuring that evidence is preserved
- Ensuring that the investigation team activities result in minimum disruption to the rest of the facility
- Directing and managing the team in its investigation, setting priorities, and ensuring the objectives and schedules are met
- Serving as principal spokesperson for the team and point of contact with other organizations and interested parties, including government agencies
- Preparing status reports and other interim reports documenting significant team activities, findings, and concerns
- Keeping upper management advised of status, progress, and plans
- Organizing team work including schedule, plans, and meetings
- Assigning tasks to team members in accordance with their individual skills, knowledge, capabilities, and experience

- Procuring and administering resources needed for the investigation
- Initiating formal requests for information, witness interviews, laboratory tests, and technical or administrative support
- Ensuring that proprietary information and other sensitive information is controlled
- Providing structured feedback to team members and their supervisors regarding their performance on the investigation, to help with their development and support continuous improvement (See Chapter 15, Table 15-5).

6.4 POTENTIAL TEAM COMPOSITION

The composition and mandate of a team will vary depending on the nature, type, and size of the incident. It may not be practical or desirable to preselect one team to investigate all incidents. Personnel should be selected to participate in investigations based on their specific skills, experience, availability, and the team roles that need to be filled for a particular investigation. Investigations are also opportunities to train other personnel how to investigate and develop future investigation team leaders. It can be beneficial to include personnel who have never been involved in an incident investigation. The investigation process can be a good opportunity for them to engage with the workforce and to convey the investigation learnings to the organization afterwards. Over time, this approach will produce a pool of trained and experienced employees familiar with the investigation process.

A typical incident investigation team may consist of the following:

- Team leader
- Process operator (at least one worker from the unit experiencing the occurrence)
- Process engineers
- Process safety specialist
- Maintenance/inspection specialist

Production and maintenance staff who were *involved* in the incident will be part of the investigation process as witnesses. However, it would not normally be appropriate to appoint them to be a core part of the investigation team, due to possible bias or inability to be objective.

At least one team member should be a competent facilitator for the investigative method that the team will use. This person does not necessarily need to be the team leader.

Other participants can be involved in a full- or part-time consulting role, depending on the nature of the incident. It is important to include people who know what happens in the field—not just those who know what is supposed to happen. The team selection should involve the appropriate competencies and roles to be credible with other stakeholders such as employees, departments, union representatives, community groups, regulatory agencies and legal departments.

Positions to consider should be based on the nature and scale of the incident and may include:

- Emergency response personnel such as fire chief
- Fire investigator—for expertise to help determine fire origin and cause
- Explosion investigator—for expertise in understanding the ignition source and physics involving explosion
- Process control (electrical/instrumentation) engineer / designer
- Computer software specialist
- Data recovery/ forensic data specialist
- Instrument technicians, inspection technicians, and maintenance technicians
- Maintenance engineer
- Civil or structural engineer
- Construction department
- Contractor participant
- Purchasing or stores department
- Original Equipment Manufacturer (OEM) representative—a factory or team services engineer
- Materials/ corrosion /metallurgist / failure analysis engineer
- Rotating equipment specialist
- Industrial hygienist
- Environmental scientist or specialist
- Chemist/ specialist testing lab services
- Quality assurance specialist
- Research technical personnel
- Human factors specialist
- Other technical consultant or equipment specialist
- Human Resources representative
- Recently retired employee with pertinent knowledge, skill, or experience
- Collective bargaining unit participant

Team members who come from another part of the organization, experienced contractors, and part-time staff may bring an unbiased, fresh, objective perspective to the investigation. Some companies choose to avoid selecting managers or supervisory personnel as team members, (at least from the same site or unit), since they may inhibit open dialogue among other team members and might bias the conclusions and recommendations.

The team leader should become familiar with each member's competencies and strengths. Team leaders should encourage team members to admit when they require help or if they do not have the competence needed for a task. Team members may not be forensic investigative professionals and should not be expected to contribute beyond their level of competence or experience. The team leader needs to be flexible in making and modifying job assignments.

Team size is also a consideration. Some companies recommend the core team consists of a minimum of two and a maximum of eight people for a workable size group, but significant or complex incidents may involve more personnel. However, large investigation teams are generally more difficult to manage and may require a longer timeframe to reach consensus and closure on findings and recommendations.

Some personal and technical characteristics to consider when selecting team members are provided below.

Select personnel with:

- Open, logical minds
- A desire to be thorough
- The ability to maintain an independent perspective
- The ability to work well with others
- Special expertise or knowledge regarding the technology or the facility
- Experience in technical troubleshooting
- Data analysis skills
- Writing skills
- Interviewing skills

Avoid selecting personnel:

- With preformed opinions on important issues
- Who are difficult for the team to work with
- Who identify causes of the incident before the investigation starts
- Who are too close to the incident, the

facility, or the injured and may be emotionally involved or biased

- Who are only offered because they happen to be available
- With conflicting work assignments or other job priorities
- Who have difficulty with logical or technical reasoning
- Who lack good communication skills
- With travel or schedule restraints that are not compatible with the investigation timing and location

Training requirements for persons assigned to the investigation team are discussed in Chapter 4, section 4.2.6.

Although they may not be part of the core team, senior management needs to play a part in the workings of the investigation team. A good practice is to request that a senior manager periodically review the work product and comment informally on the progress during the investigation. Furthermore, the investigation process should include a formal review by senior management that provides feedback to the investigation team. The practice of keeping senior management informed emphasizes the significance of the incident and the importance of the investigation. It can also assist in expediting responses to team requests. The team leader may work with senior management reviewers to determine the format for reviews.

In the example case study shown in Appendix D, management selected the following incident investigation team:

- Corporate Safety and Risk Analyst, Team leader
- Process Engineering Supervisor
- Safety Supervisor (trained and expert in the multiple-cause systems-oriented incident investigation methodology)
- Catalyst Production Supervisor
- Outside Operator
- Polyethylene Process Unit No. 1 Foreman
- Maintenance Foreman
- Corporate Legal Representative

6.5 BUILDING A TEAM FOR A SPECIFIC INCIDENT

Once an incident has been reported, the team activation section of a company's incident investigation management system should guide the user to assemble a team led by a trained investigator. Many companies have a system in place to match their resources to the type of incident involved. Classifying the nature of the incident is discussed in section 4.2.1.

6.5.1 Composition and Size of Investigation Team

The UK HSE guide on incident investigations (HSG 245, 2004) and API 585 (API RP 585, 2014), which is primarily aimed at investigations into pressure vessel integrity incidents, both provide guidance on the scope and size of investigation teams. A consolidation of the guidance from these two references is provided in Table 6.1 below, although the precise assignment of team members to investigation levels would vary according to incident classification, company policy, and regulation. A flexible approach to the exact composition of the investigation team may be more appropriate.

Table 6.1 Typical Investigation Team Composition and Scope

Investigation Level	Typical Incident Characteristics	Investigation Characteristics	Investigation Team	Initiation	Leadership/ Sponsor
Minimal	Near-miss or non-injury incident with minimal learning potential / minor consequences. Possibly API 754 Tier 3 PSE	Establish circumstances and any possible lessons to share to prevent future events.	Supervisor and operator/ technician	Within a few days	Line manager
Low	Minor leak or small fire with minimal consequence/ minor injury. Loss of a safety barrier / demand on safety system Possibly API 754 Tier 2 or Tier 3 PSE	Establish circumstances, causal factors and root causes to try to prevent a recurrence and to learn any general lessons. Possible use of less structured tools such as “What-if” or “5-whys”	Supervisor/ line manager trained in simple investigation techniques	As soon as practical – within 24 hrs	Area or section manager
Medium	Larger leak/ fire / explosion/ major injury/ environmental impact Possibly API 754 Tier 1 PSE with low severity points or Tier 2 PSE/ RIDDOR reportable	More detailed investigation, possibly using more formal/ structured methodology to establish the causal factors and root causes	Manager trained in investigation techniques, relevant supervisor/ line manager, health and safety adviser, employee representatives.	Freeze and collect evidence as soon as possible	Site management / Site safety, health and environment manager
High	Major leak/ fire/ explosion, possible fatality / major environmental damage Possibly API 754 Tier 1 PSE / with higher severity points / RIDDOR reportable	Thorough investigation, using subject matter experts, formal/ structured root cause analysis methodology/ logic trees/ cause and effect diagrams to establish the causal factors and root causes.	Leader trained and experienced in structured RCA techniques from another site, corporate process safety or external company, subject matter experts, local managers, health and safety advisers and employee representatives.	Freeze and collect evidence using formal approach and corporate/ external experts	Senior management / director with overall responsibility for process safety at the facility/ corporate safety department

6.6 TEAM ACTIVITIES

A complex or significant incident will involve a great deal of work by many people. It is unlikely that the team leader will have the opportunity to interact regularly with everyone who works on the investigation. For large scale investigations, it may be appropriate to organize the investigation team by function, and the team leader then needs to efficiently and effectively delegate these activities to key individuals and ensure there is effective communication between them. Examples of functional group activities would be forensic analysis and conducting personnel interviews. In this way, the team leader can interface with fewer individuals and more effectively manage the overall process. A designated point of contact between the team and outside groups can help minimize communication breakdowns, delays, and confusion.

The investigation discovery phase should follow a problem-solving process sequence. Investigation activities include interface and coordination with other groups, evidence preservation, evidence examination and documentation, evidence analysis and testing, and resolution of conflicts and gaps in initial information. Debate among team members is encouraged regarding causes, remedies, probable sequence of occurrences, scope of investigation activities, and sometimes even on process technical concepts. Active deliberation and open exchange of ideas, opinions, and experience are critical to the function of the team approach. In the early stages, most activity takes place in the field using specialized techniques and resources. As the investigation moves forwards, a more collaborative process is required and there will normally be a series of regular team meetings to:

- resolve questions,
- update members on new information,
- report on subtasks,
- conduct preliminary analysis for causes and possible remedies,
- establish new items and questions for resolution, and
- generate short-term action plans.

The length and complexity of these meetings will increase as the team considers the evidence and conducts an analysis of causal factors and root causes, before developing its findings. As the investigation progresses from information gathering to analysis of the results, the physical location of the team's activities may change. All core team personnel should be present when key points are discussed or debated and when the formal analysis of

logic is conducted. A dedicated conference room is often used to draw people together at predetermined times. The team will shift its focus toward activities in this room as the investigation reaches closure. Figure 6.1 illustrates the physical function of the team. The large central rectangle depicts those activities that engage the core team members. By contrast, the outside boxes depict activities that are carried out by individuals in support of the team.

The final phase of the team’s activities is preparation and presentation of the results and recommendations, usually in the form of a written formal report. In some cases, the incident investigation team (or selected members) may retain some responsibility and authority for the final resolution of the recommendations; however, responsibility typically shifts to the management team. If necessary, the investigation team can be reconvened at a future date to audit, evaluate, and report on the actual implementation of the recommendations. This would further capitalize on the insights gained by the team during the investigation.

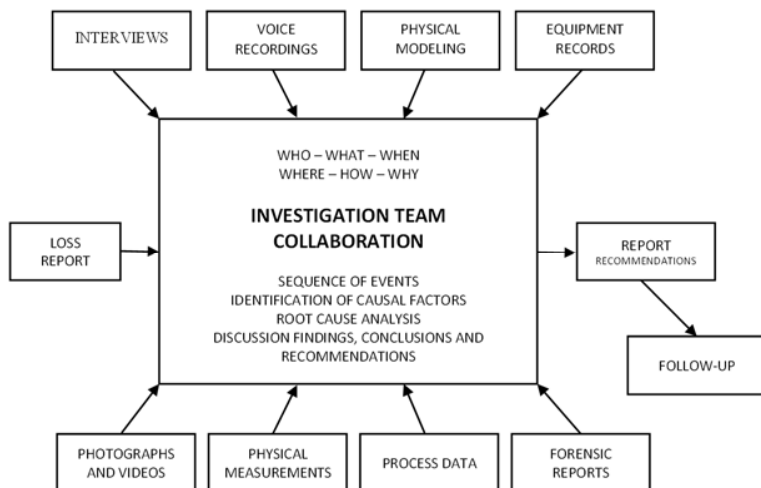


Figure 6.1 Investigation Team Collaboration

6.7 SUMMARY

Following incident notification, the next step in the investigative process is assembling a team. It is important to select the appropriate size and composition of the team commensurate with the actual (and potential) incident severity, the complexity of the incident, and other factors such as legal implications. For simple incidents, the team could be small. For more complex events, a larger team may be required, with specialists and incident support personnel included on an as-needed basis. Team leaders should have the necessary level of expertise and experience for the particular incident and need to be effective at delegating parts of the investigation to specific individuals, when required, while facilitating collaboration amongst the team members. Team members should be selected based on their skills, capability to work well with others, ability to be objective and unbiased, and to coordinate the wide range of activities. Training is important to develop and maintain an understanding of the investigation management system and the specific activities to be performed by various participants in the process. Training can include instruction on the management system, roles, and responsibilities as well as specific training on the tasks that each individual would be expected to perform in support of the investigation.

Once a team is formed, the next step is for the team to develop a plan to gather data. The next chapters discuss considerations for witness interviews and evidence collection.

7 WITNESS MANAGEMENT

Chapter 7 details the recovery of witness evidence and Chapter 8 describes methods and practical guidelines for gathering and archiving physical and electronic evidence.

In the immediate aftermath of an incident, there are likely to be a number of witnesses with information of great value to the investigation team. This includes knowledge of tasks and activities that were being undertaken prior to and at the time of the incident as well as sensory observations (what was seen, heard, smelled and felt). Identifying potential witnesses and obtaining information from them is part of the investigation process. The increased use of personal electronic devices means that witnesses, both inside and outside a facility, are often able to capture key, reliable evidence from the time of the incident.

Whether dealing with individuals' recollection of events, or information from personal electronic devices, the effective management of witnesses is a crucial part of the investigation process. This chapter provides practical guidelines and advice on how to manage witnesses and the information they can provide in order to maximize their value to the investigation process. Once collected, witness information is handled alongside the other physical and electronic evidence, as described further in Chapter 8.

7.1 OVERVIEW

The process shown in Figure 7.1 presents the overall evidence-gathering activities in the context of the management of witnesses and physical evidence. The objectives are to gather information for determining causal factors and root causes, and to support the development and implementation of recommendations.

The process is iterative, and as evidence is analyzed and hypotheses are tested, there is often a requirement to obtain more information from witnesses and other sources. It is common to conduct follow-up interviews to help confirm, refute, or clarify certain inconsistencies.

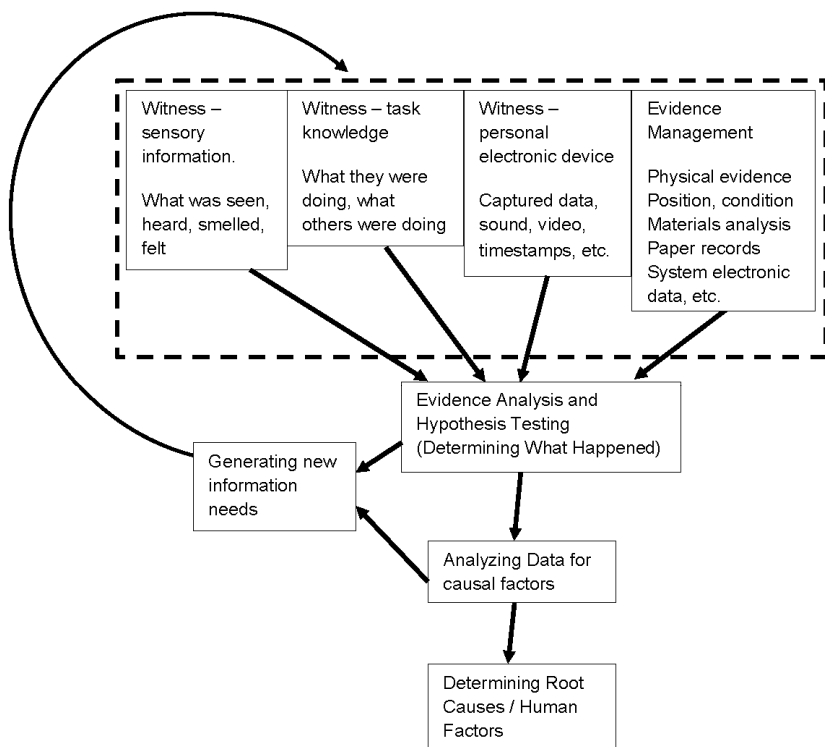


Figure 7.1 Iteration between Witness and Physical Evidence Collection and Analysis

7.1.1 Witness Issues Following a Major Occurrence

Following a major event, such as an explosion or large fire, the investigation environment can present significant challenges, including the identification and handling of witnesses. Witness information is time-sensitive since memories will fade or change rapidly; however, access to witnesses immediately following an event can be limited.

Some critical witnesses may be initially unavailable; some may be in the hospital, and some who were on duty at the time of the incident may be at home recovering from long, traumatic hours spent during the emergency response. Other witnesses could be involved in making the plant safe and/or the initial inspection of the plant and equipment affected by the event. Following a major event, there may be a requirement for psychological

counselling of employees. The mental health of witnesses should be considered when planning the interviews including the use of interviewers with experience in handling traumatized people, if appropriate.

Witnesses might be pressured by the press or others to make statements and respond to questions. The site may be under the control of a regulatory agency (e.g., OSHA in the US / EPA or HSE / EA in the UK). Witnesses may be asked by these agencies to provide statements. The various social media platforms provide an opportunity for sharing both accurate and inaccurate (or speculative) information concerning the details of the incident and possible causes. This information can alter the perception of witnesses and potentially lead to less reliable statements.

The investigation of a major incident could last a number of months. During this period, emotions of personnel may evolve from shock, to disbelief, to sadness, to anger or resentment - especially if the incident involved fatal or permanent injuries. People may also be concerned about their job security. Sometimes there is uncertainty as to whether or not the plant will be rebuilt or reopened.

These and many other issues are important considerations when managing witnesses to an incident, in order to maximize their benefit to the investigation process. Therefore, recognizing the possibility for limited access to witnesses and the potential for changing witness memories over time, it is important to make scheduling witness interviews a high priority in the investigation.

7.1.2 Investigation Team Priorities for Managing Witnesses

The incident investigation team has a number of priorities to coordinate concerning examining the incident scene and identifying and recovering physical evidence, some of which will be time-sensitive. However, information from witnesses is also time-sensitive and the need for early intervention to recover this knowledge and information cannot be overstated; it will be of significant benefit to the overall investigation process.

Witnesses should be identified as soon as possible and individually encouraged to provide initial statements while the incident details are still fresh. Discussions between witness should be avoided as this may result in alteration of some individuals' recollection of events; either consciously or subconsciously. In some cases, the initial statements may be written out by witnesses or taken by immediate supervisors/managers when speed, rather

than thoroughness is a priority. More detailed and structured interviews can be arranged by the investigation team at a later time.

7.2 IDENTIFYING WITNESSES

Any person who may have information relating to an incident is considered a potential witness. This concept extends beyond those individuals traditionally identified who were direct participants or eyewitnesses to the occurrence. Indirect witnesses who are outside the operations team often contribute valuable information. Examples include workers from maintenance, the laboratory, janitorial service, shipping, delivery companies and contractors. They may routinely visit the process unit, be familiar with some aspects of normal operations, and could have noticed some unusual condition, remark, or actions.

Increasingly, people are recording events on personal electronic devices such as mobile phones. These witnesses may have been on or off-site at the time of the incident, and the information they possess can be extremely helpful. They may also have shared the details on social media and could be contacted to provide further details.

Emergency response personnel may also be interviewed. During their emergency response activities, they may—unavoidably—disturb, alter, or destroy evidence. The interview can attempt to determine the original positions and status of equipment and items. Firefighters may be able to comment on many important observations such as flame patterns, areas of fire, location of victims before rescue, whether fires are pool or jet fires, which equipment was already damaged upon their arrival, and any equipment that suffered damage in a secondary fire or explosion.

Personnel who are off-shift, who were on the previous shift, or whoever last ran the process should be contacted. Recently retired or transferred employees are potential sources of valuable information about the plant and systems involved. They often have unique knowledge based on many years of experience with the particular systems and equipment involved in the incident. Examples of such knowledge include:

- Actual operating practices or changes not included in the written operating procedures
- Insights on little-known failure modes and anomalies in system behavior
- Process control system response to various upset conditions

- Subtle changes in process variables
- Unexpected relationships between certain parameters
- Reliability of specific instrumentation
- Unexpected problems and associated changes in the process made during the initial startup of the system
- History of previous problems and actions taken to avoid/rectify problems

If a similar incident occurred in the past, it might be appropriate to re-interview those witnesses involved to gain insights into this investigation.

A list of potential witnesses is provided in Figure 7.2.

Employees	Contractors and Third Parties
On-shift operators	Statutory compliance officer/ Safety, Health and Environment officer/ Fire engineer/officer
Off-shift operators	First responders/emergency response personnel
Maintenance personnel	Contract maintenance
Process engineers	Manufacturer's representatives
Operations management	Personnel previously involved in operation/ maintenance of the system, including former employees and personnel involved in the initial start-up of the system
Maintenance management	Personnel involved in previous incidents associated with the process
Chemistry and other laboratory personnel	Janitorial, delivery, and other service personnel
Warehouse personnel	Original design/installation contractors or engineering group
Procurement personnel	Security force (roaming guards or sentries)
Quality control personnel	Off-site personnel and visitors
Research scientists	Members of the community

Figure 7.2 List of Potential Witnesses

Drafting a list of potential witnesses at the start of the investigation is helpful, as the list can be modified as the investigation progresses and more witnesses come to light.

Sources of information on possible witnesses include:

- List of people associated with the facility
- Operator's and other logs
- Permits to Work
- Work schedules
- Computer access records
- Employee and visitor sign-in sheets
- Names of personnel on work orders and procedures / risk assessments
- Purchasing records
- Design and drawing documentation
- Training documentation
- Organizational charts
- Lockout/tagout records
- Audit records
- Hospital admission records
- Phone logs or records
- Referrals made by current witnesses
- List of personnel responding to the emergency
- Contact with people outside of the facility
- Responses to public advertising for the need for anyone with related information to come forward, possibly including people who have posted on social media

7.3 WITNESS INTERVIEWS

7.3.1 *Human Factors Related to Interviews*

Humans are unable to record and playback occurrences in perfect detail. Eyewitness accounts should be considered incomplete. Most of us have received little formal training in observation techniques. The common optical illusion amusements in Figure 7.3 remind us that our minds will often complete the expected or anticipated picture or image, even if it is not necessarily present. Consider the text in Figure 7.3. Most people will miss the repeated extra word. Similarly, witnesses may fill in data that are missing from their recollection of an occurrence or overlook data due to oversight or

other distractions. In most cases, the witnesses are not trying to provide false data; they are usually trying to provide an account of what happened as best as they can recall it. In some cases, witnesses may be emotionally upset after incidents that were particularly serious. These human performance characteristics are often at the root of apparent inconsistencies and conflicts generated from comparing witness testimony.

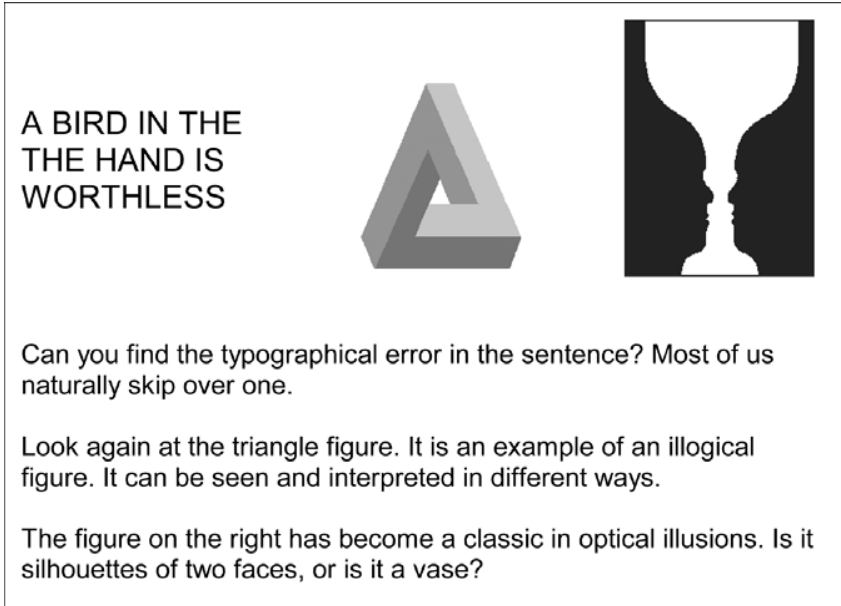


Figure 7.3. Illustration of Human Observation Limitations

Although humans have a remarkable capacity to observe, interpret, recall details, and then articulate this information, humans are not computers. No single witness has a complete view or comprehension of the entire occurrence; each person experiences a unique perspective. Discrepancies in descriptions of the incident may be due to different perspectives or even different experiences of the individual witnesses. In one way, this concept could be compared to each witness seeing an instantaneous vertical slice or “snapshot” view of a large, moving, panoramic occurrence. All incoming information is processed and filtered by the brain as part of the cognitive comprehension process. The information is again processed and “filtered” as it is articulated and transmitted to others.

A classic example of this “filtering” concept is the fable of four blind men who encounter an elephant as they walk down the road together. Each blind man encounters a different part of the elephant and tries to communicate to his associates what he has found. The first man touches the trunk and believes they have met a boa constrictor. The second man grabs the tail and thinks it is a rope. A third who has encountered a leg begins to argue saying that both of his friends are wrong and that the thing is a tree trunk. The last man, who has hit the side, insists they have hit a wall of some sort. Each blind man was basing his conclusion on the information available combined with his previous experience. The entire picture is not accurately interpreted until the composite information is assimilated. The task of the incident investigation team is to put these four stories together and realize that the men have encountered an elephant and not a snake, rope, tree, or wall.

Another natural human characteristic is to recall events, actions, observations, etc., out of chronological order. The human ‘replay’ mechanism does not function in order like a video player. This characteristic is one reason why retelling their account of what happened several times may help individuals remember additional details.

Sometimes, witnesses may choose not to tell the complete story. A witness may have several motives for purposely modifying statements or choosing not to tell the incident investigation team all of the relevant information they have. The most significant of these influences is fear of punishment, either for themselves or a friend or colleague. When evaluating witness statements, the investigation team may need to consider the possibility that a statement given in an interview might be incomplete or modified. The strategies for dealing with fear of punishment are similar to those for encouraging the reporting of near misses. The focus of the investigation is on fact finding, not fault-finding. Although some incidents may be a result of horseplay, negligence, or malicious/criminal acts of sabotage, these causes are, by far, the exception. The root causes of the vast majority of incidents are associated with management-system or organizational failings. This message should be clearly communicated to everyone involved in the investigation, particularly to the witnesses.

It is important for witnesses to understand that the purpose of the investigation is to determine the root causes of the incident to prevent a similar occurrence. In cases that involve a failure to follow safety or operational instructions, personnel may have thought that the rules are unnecessary, incorrect, or an inefficient use of time and it was in the best interest of the individual and the organization to perform the task in another

way. Perhaps the supervisors and management were aware of these types of issues prior to the event and could have done something to correct them. If the investigation reveals that staff routinely fails to follow procedures, this may be indicative of more fundamental cultural issues that require addressing by management.

For example, an operator may skip a pre-operational check of a system because he believes the check will not discover any problems and takes valuable time that could be used to produce product. In other words, the operator believes the check is a waste of time. Perhaps the operator had skipped the preoperational check many times, and it had never caused any problems. His supervisor may have known he normally did not perform the preoperational checks but had said nothing because it resulted in increased production. Skipping the checks was not a malicious act or act of sabotage or even an act of negligence; it was an 'accepted' practice. However, this time when the operator skipped the check, the system failed and a release of process chemicals occurred. Will the operator tell the incident investigation team that he skipped the preoperational check? What motivation would there be? What potential punishments are there? Unless the operator believes that it is in his own best interest to divulge the information, he probably will not. Unless boisterous play, negligence, or sabotage are clearly involved, individuals should not be punished for the information revealed during incident investigation interviews. If witnesses are aware of this, they are more likely to openly share the information they have. The investigation team's responsibility is to gather facts and draw conclusions. Punishment is not part of the investigation process. This philosophy should be emphasized as part of the training requirements, as outlined in Chapter 4. Any disciplinary action arising from an investigation is part of a separate process involving Human Resources personnel/policies.

Cultural issues, including company culture and country/regional culture, should also be considered. This may include factors such as a tendency to agree with whatever is said by someone perceived to be in authority or a more senior position, and an unwillingness to divulge information that could reflect poorly on a co-worker.

7.3.2 *Collecting Information from Witnesses*

The accuracy and extent of witness information is highly dependent on the performance of the interviewer. The interviewer's ability to establish rapport and create an atmosphere of trust affects the quality and quantity of information disclosed.

Promptness in gathering information is critical. Information from people is among the most fragile form of evidence, (i.e., it is easily forgotten, distorted, or otherwise influenced by personal conflicts.) For most people, short-term memory for retaining and recollecting details degrades rapidly. The second reason for promptness is rooted in the fact that contact and communication with others can significantly affect our “independent” recollection of occurrences. It is best to prevent any exchange of information among witnesses, if possible, immediately after an event. In most cases, complete isolation is not practical, so as a minimum, the witnesses should be asked to refrain from discussing the incident with anyone until their initial interview. The use of social media makes this a challenge.

The interaction among witnesses causes modulation of details and changes emphasis both consciously and subconsciously. Recollection is affected by our emotions, by perceived unfairness, by fear of embarrassment, by fear of becoming a scapegoat, and by preexisting motives, such as grudges and attitudes. Many people are so reluctant to be identified as betraying their peer group that they may withhold information if they perceive the peer group would desire them to do so. There is often value in repeating portions of the interview; a witness might be stimulated by reviewing his or her own initial testimony.

Investigations involving complex human performance problems can benefit from simulations. Process simulators are often used for operator training. In some cases, these process simulators can be excellent tools for learning more about human error causation. The incident investigation team can expose operators to simulated process upsets and gain valuable insights into the operator’s response to rapidly and accurately diagnose the problem and execute the proper action.

The talk-through exercise is a technique sometimes used by investigators to gain insight and to verify conclusions drawn from verbal testimony. This technique, often used by human reliability analysts, has particular application for learning more about specific tasks or occurrences. It is a method in which an operator describes the actions required in a task, explains why he or she is doing each action, and explains the associated mental processes. To be effective, such exercises must be planned by the investigator. The actual talk-through itself is seldom very time-consuming, but the burden is on the investigator to take good notes and observe any potential problem areas. When the procedures call for the manipulation of a specific control or for the monitoring of a specific set of displays, the operator and the investigator approach them at the control panels and the

operator points out the controls and displays in question. If the performance is simulated, the operator touches the manual controls that would be operated and describes the control action required.

A talk-through of control room operations can reveal previously undisclosed information. In a control room analysis, an operator and the investigator actually follow the path taken by the operators during the performance of the procedure being analyzed.

A good example of the talk-through technique is when reactive chemistry is involved. The witness would relate his actions, sequence, addition rate, volumes, etc., without referring to the batch or log sheet. This is not an effort to cause him to make a mistake but rather an effort to discover if his field actions match what he documented. Sometimes tasks become so routine that they are done without much thought, or an interruption might occur, and it is easy to write one thing and do another. Furthermore, if a witness is having trouble recalling the order of things they observed or did, it may help to ask them if the action or observation has happened before or after some other notable/significant event or action. This will sometimes help the witness remember the order more clearly.

7.3.3 Initial Witness Statements

The initial witness statements address three needs. First, the incident investigation team cannot interview all the witnesses promptly. It takes time to work through the list of all the witnesses. The initial witness statement helps to capture the basic thoughts of each witness before too much time passes. Secondly, these statements help the incident investigation team prioritize the witness interviews, so those with the most fragile and valuable information are contacted first and those with the least fragile and least valuable information are last. Finally, the statements can be used to trigger the witnesses' memories when the interview is actually performed.

When documenting initial witness statements, it is a good practice to request the witnesses to separately and simultaneously write down their observations and recollections in a narrative statement. Focusing on the sequence of events that occurred and first-hand observations may help the witness to clarify and focus their thoughts. However, some people do not like to write and may prefer to talk into a recording device for transcription later. Others may find such devices intimidating or are self-conscious about speaking into a recorder. The investigator needs to be aware that most eyewitnesses are not trained or accustomed to giving such statements,

potentially resulting in unclear and incomplete passages. The interviewer should insert narration into the audio record when appropriate to clarify what is physically happening during the interview. For example, if the witness points to a chart or a diagram, the interviewer should narrate, "Mr. Witness is pointing to Reactor K-13 on Chart XYZ," so that listeners, or those reading a transcript, will be able to follow the dialogue.

Because there is a high degree of variability in length, amount of detail, clarity, etc., in the statements, they can provide a misleading perception of value of the information a witness holds. When establishing interview priorities, the investigation team should consider not only the statements but also the value of their content and other relevant factors such as work assignment at the time of the incident, etc.

7.3.4 Conducting the Interview

An overview of the interviewing process is shown in

. The interviewing techniques discussed in the following section are generic to any interviewing activity but have been modified to incorporate specific issues unique to incident investigation.

7.3.4.1 Selecting an Interviewer

The most important consideration when selecting an interviewer is good interviewing skills, many of which are described in the list of things an interviewer "should" and "should not" do during the interview (see 7.3.4.9). It is helpful if the interviewer is someone with whom the witness will feel comfortable. This person could be an individual at a similar level in the organization. In a major incident, it may be necessary for company interviewers to come from another facility, or for a third party to be involved. Good interviewing skills can often overcome hurdles associated with being an "outside" person. Although familiarity with the system involved and the terminology used in the facility can be beneficial, someone from outside may be more far-reaching with their inquiries due to a lack of understanding. In some cases, the operations and maintenance personnel from the investigation team can be of assistance with the interviews of other operators and maintenance personnel. However, there is a risk that by being too close to the incident or the person being interviewed, they could "lead the witness." On the positive side, they may have an established rapport with these individuals, thus leading to more information being gathered during the interview.

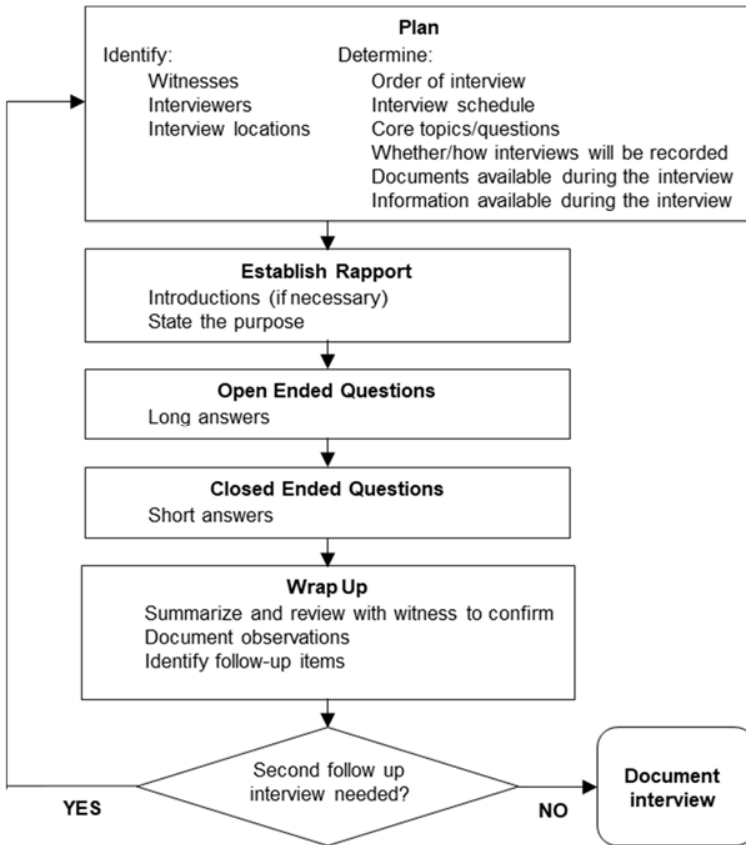


Figure 7.4 Overview of Interview Process

Not every witness will be comfortable with the same interviewer. It could simply be a matter of personality types. Having more than one interviewer available may be helpful to avoid a poor match between interviewer and interviewee.

7.3.4.2 Limiting the Number of Interviewers

Select the interview style to maximize results from witnesses. During the initial interview, a one-on-one or two-on-one interview style is best. By limiting the number of interviewers to one or two, the stress level for the witness is lowered and the interview seems less like an inquisition. If two interviewers are present, one can lead the interview by asking questions and interacting with the witness, while the other interviewer plays a background

role, primarily serving as a note taker. This division of tasks allows the primary interviewer to concentrate on listening and asking questions. Having a secondary interviewer also speeds up the interview because less time is spent waiting for notes to be completed. This approach also prevents the witness from feeling intimidated or becoming defensive, which can occur when multiple interviewers start asking questions.

For follow-up interviews and general information gathering (fact-finding type meetings), the interviewer to interviewee ratio is less critical. Later in the investigation, it may be acceptable to have multiple witnesses present as details and inconsistencies are resolved. A group interview can come across as more open, honest, and less covert. A team atmosphere can be created. The team will have to make this judgment based on the specifics of the occurrence and the workplace atmosphere.

7.3.4.3 *Avoid Influencing the Witness*

There is sometimes a tendency for the witness to relay what he thinks the interviewer is expecting (wanting or waiting) to hear. There is also a corresponding possibility for the interviewer to “lead the witness” by inadvertently sending various response signals or asking leading questions. Sometimes the interviewer is not even aware that they are leading or steering the discussion. Leading questions contain some hint of the answer in the question. For example, consider the question “After you check the pressure you then adjust the inlet valve, right?” This wording implies to the witness that the correct action is that the inlet valve was adjusted, although the witness may believe otherwise. The witness may answer yes, just to satisfy the interviewer.

Interviewers can also influence responses by repeatedly asking about the same issue or topic. For example, if the interviewer always asks multiple questions about a procedure, the witness will start to relate all his answers to the procedure because he realizes that this is important to the interviewer. Such questions might include:

- “Is that consistent with the procedure?”
- “What does the procedure say next?” and
- “Is that in the procedure?”

Questions asked by the interviewer should be carefully worded to be as neutral, unbiased, and non-leading as possible. A common, core group of questions, such as those in Table 7.1 below, should be asked of all witnesses to provide a control sample and to obtain confirmation of key information.

The interviewer's comments made in response to statements by the witness can also influence what the witness says next. For example, assume a mechanic admits taking a shortcut in the lockout / tagout process and the interviewer says, "Wow, no kidding! You did what?" This response could influence the information the witness communicates during the remainder of the interview.

Even the nonverbal reactions of the interviewer can influence the witness. If, for example, the witness admits making an error in performing an operation and the interviewer grimaces or lets out an exasperated sigh, the interviewer has communicated, using body language, a perception that the operator has performed poorly. Interviewers must remain constantly aware of the potential influence they can have on a witness.

7.3.4.4 Maintaining Confidentiality of the Interviews

In most cases, it is unrealistic to tell witnesses that the information provided during an interview will remain confidential. The team should make reasonable efforts to protect the identity of each witness and the information provided by each witness. For example, in reports, the names of witnesses should not be used. However, the report should document the sequence of events, and the identity of witnesses may therefore be apparent to personnel at the facility. The notes from each witness should not be shown or released to anyone outside the incident investigation team, except where legally required.

A list of the individuals interviewed may be included in an appendix of the report to show the thoroughness of the data collection/analysis effort; however, generic titles rather than names of the personnel interviewed could be used to preserve anonymity for the individuals who provided data. Again, there is no reason to distribute this list widely, as most individuals can determine the general level of effort by examining the remainder of the report.

7.3.4.5 Selecting Interview Locations

A neutral interview location that is reasonably familiar to and convenient for the witness will usually allow the witness to feel more relaxed. Avoid locations that may be uncomfortable or stressful such as the office of a high-level manager. Choose a room that is in a quiet, low traffic area if possible. Possible interview locations include a meeting room, a training room, and an office. The witness's work location is usually not a good choice due to distractions within the work space (e.g., phone, computer, people dropping by) and visibility to others.

As part of the interview, it may be beneficial to visit the incident scene as it is less formal and the visual clues may help the witness remember information. This location also provides the opportunity for the witness to walk around and point out equipment, which may further ease tension and elicit more information than would be obtained in a different setting (for example, the witness may be able to describe the position of a valve or its distance from an instrument). Disadvantages of conducting the interview at the scene include potential distractions (such as other people, repair activities, demolition activities, the presence of other potential witnesses, and unsafe conditions), poor weather conditions (if the incident scene is outdoors), and emotional distress for the witness, especially if a colleague was seriously injured or killed. For these reasons, interviews at the scene are usually best as a follow-up interview.

7.3.4.6 Arranging the Interview Room

Arrange the room to be welcoming to the witness. Have the witness sit on the same side of the table or desk as the interviewer; conducting the interview across a table or desk may create a more formal atmosphere. If using a scribe to take notes, have the scribe sit to the side so that the witness can see and focus on the interviewer, and not be distracted by the scribe taking notes. If any other persons are attending the interview (e.g., union representative, spouse, colleague), arrange the seating so that those individuals are out of the line of sight between the witness and interviewer to prevent gestures and body language of these individuals from influencing the witness.

Have reference information readily available (for example, flow diagrams, plot plans, procedures, and work orders). This will give the witness something to point to and something to do during the interview, making him more relaxed and willing to talk. Be careful not to inundate the witness with documents, but have them available so they can be referred to as they come up in conversation or are requested by the witness.

Eliminate other distractions from the room if possible. Close the door to create a private atmosphere, so the witness can speak freely and others will not overhear the discussion. Do not allow the witness to see any documents developed by the investigation team, such as causal factor charts or fault trees, showing the incident investigation team analysis of the occurrence.

Hand-drawn sketches (regardless of the artistic quality) are a valuable tool in the interview process and should be encouraged by the interviewer. It is a good practice to have paper, flip charts, and pencils in the interview room

for use by the witness. It may also be helpful to display information such as photographs, videos and drawings on a large computer screen. Having extra copies of plot plans, aerial photographs, P&IDs and other documents that the witness can mark can be helpful for the witness to communicate their recollections. A witness should not be shown diagrams marked by another witness, to avoid possibly influencing the current witness.

7.3.4.7 *Scheduling Interviews*

The first witnesses to be interviewed should be those with the most critical (detailed, fragile) information. To the extent possible, schedule interviews at a convenient time for each witness. Make appointments with witnesses through appropriate channels, such as through managers, union and contract personnel, etc.

Attention to minor practical details such as arranging transportation home for the witness and providing overtime meals or refreshments can help to reduce the stress of a witness.

In some companies, union workers have a right for a union representative to be present with them at the interview, and the union representative will have to be allowed to attend the interview if the witness so desires. Alternatively, it may be helpful for a colleague or safety representative to be present. In the example case study (Appendix D), two members from the investigation team, the safety supervisor plus one other person, as available, were present for the interview. When another individual accompanies the witness, the interviewer can inform this person that the purpose of the interview is to obtain first-hand information from the witness, and request that the additional person not interject in the interview.

Despite the best efforts of the investigation team, they may be faced with witnesses who are less than cooperative. It could take considerable time and effort to obtain information from uncooperative witnesses, which could delay interviewing other witnesses. If significant resistance from a witness is encountered, it may be better to interview the other witnesses and come back to the uncooperative witness at a later time.

Although it is undesirable, witnesses will talk to each other about the occurrence and about the interviews they have had, resulting in contamination or blending of information. The incident investigation team can avoid this by selecting a schedule that minimizes contact between witnesses. For example, schedule each initial interview for 30 minutes. Allow 30 minutes between interviews to complete the documentation of the

previous interview and prepare for the next one. If possible, do not have witnesses waiting in a common area for their interviews. Adjust the schedule and interview list based on information that is learned during interviews, as appropriate.

Do not exceed the witness's interview time without the witness's consent. If more time is needed, consider scheduling a follow-up interview if continuance is inconvenient for the person being interviewed.

Telephone interviews may be appropriate as an initial interview to determine if a face-to-face interview will be required. For example, a telephone interview may precede an interviewing trip. It may also be appropriate to conduct an interview by telephone if the witness:

- is not readily available,
- will primarily provide factual information related to the chain of events,
- has little information related to contributing and root causes, or
- is not key to the occurrence.

7.3.4.8 Developing a List of Core Topics and Issues

Develop a list of specific topics to cover and issues to resolve during the interview. These will be best addressed and resolved by the use of open-ended questions. The list of specific topics and issues can be developed from the questions and data needs identified using the analysis techniques described in Chapter 9. Typical questions for an interview are listed below in Table 7.1.

Table 7.1 Example Questions for Witnesses and Emergency Responders**Example Basic Information Questions**

- Name
- Position
- Length of service with company
- Time in current position
- Normal work shift
- Overtime worked recently

Example Questions for Witnesses

- What do you remember about the incident?
- What did you see?
- What did you hear?
- Did you feel or smell anything unusual?
- What were the initial conditions?
- What were you doing/where were you just before the occurrence?
- What were you doing/where were you during the occurrence?
- What was the timing of occurrences?
- What indications did you have of the occurrence?
- How did you know what to do when you saw _____?
- What communications did you have with others in the area?
- What other individuals were in the area?
- Where were they?
- What were they doing?
- What were the environmental conditions?
- What was different this time?
- Did you notice any equipment that did not operate properly?
- Do you know if they were trained on the equipment?
- Do you know if the job had been prepared properly?
- Should we talk with anyone else?

Example Questions for Emergency Responders

- What were the initial conditions when you arrived (what did you see, hear, smell, feel)?
- Did you or others move or reposition anything?
- What emergency response activities did you perform?
- Have there been similar occurrences in the past?
- Should we talk with anyone else?

7.3.4.9 *Establishing and Maintaining Rapport*

The interview can be a source of considerable stress, even if the witness is sincere, cooperative, and was in no way responsible for the incident. Each witness brings his own unique collection of emotions (fears, anxieties), motives, attitudes, and expectations into the interview. On some occasions, these emotions can include reactions to the death or serious injury of a friend or co-worker.

The start of the interview may appear on the surface to be very informal, yet it can ultimately determine the outcome of the interview. It provides an opportunity for the interviewer to explain the purpose, format, expectations, confidentiality of the witness providing the information, and to deal with any special concerns of the witness. Yet, the most beneficial aspect is the opportunity to establish a constructive atmosphere in which communication can begin.

Start by introducing everyone present. It does not help to have a "mystery" person taking notes or sitting and listening in the background. Next, explain the investigation process to the witness and describe his role in the effort. Explain the purpose and objectives of the interview and that it is not to establish blame but to gather information that can be used to understand what happened so a repeat event can be prevented. Explain the witness's important contribution to the investigation.

Warm up with non-business issues and routine matters such as the witness's name, position, and years at the company. This allows the witness to answer some easy, simple questions and overcome initial jitters before getting into the body of the interview.

Before moving on to the body of the interview, check whether the witness has any questions. Typical questions from witnesses include the confidentiality of the information provided during the interview, how long the interview will take, and the status of the investigation. Answer all questions about the interviewing and the general investigation process as completely and honestly as possible because misleading the witness will generally cause problems with later interviews and investigations. However, responses to questions about the status of the investigation should be answered by focusing on this interview, not the information obtained from other sources that might otherwise contaminate and influence the witness. Finally, ensure that the witness understands the recording process being used, whether it is simply an investigator's notes or a court reporter or an electronic device.

Throughout the interview, the investigator *should*:

- be friendly, respectful, and professional
- listen attentively and reflectively
- show compassion
- avoid attitudes that destroy rapport
- remain as neutral as possible
- project a calm demeanor
- use language/terms that the witness understands
- observe body language/facial expressions

During an interview the investigator *should not*:

- act surprised when the witness provides new information
- act happy or pleased when the witness confirms other witnesses' testimony or a current theory of the causes of the occurrence
- be overbearing, commanding, proud, overly confident, overeager, timid, or prejudiced
- judge the information that is being presented by the witness, even if it is incorrect
- rush the witness, even if little new information is appearing
- make promises to the witness

Remember that the point of the interview is to obtain as much information from the witness as possible, not to show the witness how smart the interviewer is. Instead, convey respect to the witnesses for their experience, knowledge, and the information that they can provide to help lead the investigation team to the correct conclusions.

7.3.4.10 *Promoting an Uninterrupted Narrative*

Using open-ended questions (questions that require more than one word yes or no answers), ask the witness for an initial statement. Examples of open-ended questions are provided in Table 7.1. It is important during this portion of the interview to remain quiet. Allow the witness to talk. As long as the interviewer is talking, the witness will remain quiet. Do not interrupt with follow-up questions after asking an open-ended question. Try to avoid closed-ended questions (those that only require short answers) during the initial portion of the interview. Too many closed-ended questions at the beginning of the interview can condition the witness to give short answers.

Resolve to remain unbiased and to avoid any actions or questions that may lead the witness. Absolutely refrain from leading and accusatory questions throughout the interview, or projecting the direction that the interview should follow.

If the specific issues the investigator is trying to resolve are not addressed by the answers to the initial open-ended questions, the investigator can pursue these areas of interest with more detailed questions about the following:

- Timing of occurrences
- Location of personnel
- Activities of personnel
- Environmental conditions
- Positions of personnel and victims
- Anything moved/repositioned
- Emergency response activities
- Indicators of conditions
- Actions of other people
- Training and preparation
- Histories of similar incidents
- Information gaps
- Inconsistencies in data
- Management and staff involvement
- Possible causal areas
- Beliefs, opinions, and judgments that led to inadvisable actions

As the interview moves more toward closed-ended questions, the interviewer can periodically restate what the witness has said. This gives the witness a chance to correct any errors or misinterpretations or add further details. This interactive dialog portion of the interview is most like the common image of an interview conducted by TV journalists. Specific, objectively-worded questions are asked in this stage. During this portion of the interview, there is significant potential for the interviewer to influence the witness. This risk is constantly present and demands continuous recognition and resistance by the interviewers.

Interviewers will often experience apparent inconsistencies in incoming information. Conflicts will typically occur during the initial information gathering interviews. Some incoming information will not be fact (that is, objectively verifiable), but may be perceived as fact by the person supplying the information. In most cases, it pays to delay judgment on the apparent inconsistencies. Just as the interviewer should strive not to reach conclusions

on incident causes until the facts are fully developed, judgment should be delayed on these apparent inconsistencies. Often a scenario will emerge which reveals apparently conflicting information to be true, but at different times during the incident sequence.

Even if information is found to be wrong, the reason for the misinterpretation can frequently reveal other important information. At other times, the source of the apparent inconsistencies can be traced back to the interviewer, who inadvertently modified the incoming information from the witness based on what the interviewer knew to-date about the incident.

Keep in mind that different people may have different definitions in mind for the same word. Thus, it can be advantageous to ask questions to clarify the ideas expressed by the witness (Laborde, 1984). When a noun is used, the interviewer may need to clarify by asking, "*What, exactly?*" For example, a motor valve may be electric or air operated; the difference may be important to the investigation. When a verb is used, the interviewer may ask, "*How, exactly?*" For example, *shutting down the reactor* may mean, *gradually reducing the feeds in normal shutdown mode* or it may mean *hitting the emergency stop button*.

Sometimes, rules or values may be mentioned, such as, *the outside operator should always close the drain valve*. It may be helpful for the interviewer to ask, "Why is that important?" or "What would happen if he didn't?"

A witness may generalize, by using words such as: all, always, everybody, never, they. The interviewer can clarify these generalizations by asking, "All?", "Always?", "Everybody?", "Never?", "Who are they?" Similarly, a witness may use a comparator without an antecedent; for example, "Pump A is better." The interviewer can gain clarity by asking, "Better than what?"

The best practice is to let the witness lead the exchange, but it is important for the interviewer to explore apparent paths of new information. More than one witness has said after the interview that they knew a certain fact, but since the interviewer did not ask about it, the witness did not mention it. The witness made a judgment that the information was not important or was not relevant.

7.3.4.11 Using Personal Electronic Data

It is becoming increasingly common for people to record incidents on their mobile telephones. Many sites ban such devices for security and safety reasons. However, information on personal electronic devices may prove to

be invaluable to an incident investigation. Some sites may consider issuing a formal amnesty to obtain evidence from such devices after a major incident, although the team should first ensure that legal counsel has been consulted, since governmental agencies and/or civil litigants often demand that all company electronic data be preserved. Under such a preservation demand, the witness's electronic device may be required to be copied to preserve all data as well as the identification of the source of the data. Towards the end of the interview process, it would be a good opportunity to ask the witness if they have any electronic information that can be provided, with due consideration to the advice provided by legal counsel.

7.3.4.12 Documenting the Interview

The primary interviewer (or secondary interviewer if present) should take notes during the interview as unobtrusively as possible. Other options include a video/audio recorder or the use of a dedicated note-taker or court reporter or stenographer, although these methods may make the witness uncomfortable, as the process may seem more like an interrogation or legal proceeding. The presence of a microphone may somewhat stress the witness and the extra gain in accuracy of recording the interview may be offset by the decrease in participation by the witness.

Documentation of the interview should not be a covert, hidden process. The witness should not believe that hidden, secret notes are being taken during the interview. One way to address this issue is to ask the witnesses if they are agreeable for notes to be taken. They are unlikely to refuse, but they usually appreciate being asked. Documentation of the interview should at least include the witness's name, date and time of the interview, statement, and interviewer/recorder names.

During telephone interviews, take as many notes as possible. The witness will not be able to see what you are doing, so if you need a moment or two to complete note-taking efforts, tell the witness.

7.3.4.13 Wrapping-up the Interview

At the end of the interview, the witness should be asked in as non-threatening a manner as possible, "Is there anything else you want to add regardless of how unimportant you think it might be?" This question is then followed by an extended pause. Ask who else might be able to contribute valuable information and invite additional input if new information is remembered or discovered.

The interviewer should express appreciation for the witness's time, information, and cooperation and gain consent to contact the witness later if necessary for a follow-up interview, even if this is considered unnecessary. If the interviewer asks permission for follow-up interviews with only some of the witnesses, those witnesses may feel they are being singled out.

Finally, the investigator should review the notes with the witness. During this review, numerous clarifications and additional details are usually provided.

It is common for a witness to recall additional information after the interview is over. Astute investigators anticipate this human trait and provide a clearly understood and easily accomplished mechanism for the witness to contact the interviewer later. Always close an interview by inviting the witness to return or contact the investigator if he remembers something else, or would like to otherwise modify or add to the interview results. Provide the investigator's contact information to the witness.

7.4 CONDUCTING FOLLOW-UP ACTIVITIES

Once the interview is complete, the investigator should perform a few additional tasks immediately after the witness leaves the room:

- Review the interview process against the plan
- Organize the information received

- Identify any key points that confirm or conflict with previous information
- Record the findings.

Findings would include such items as observations, specific insights, and a list of items to be followed-up on in later interviews or investigation activity. Where relevant, the investigator should add content to a timeline, based on the witness statement (See Chapter 9.2.1 for more details on timeline development.) Finally, the information from the interview should be communicated to the remainder of the investigation team.

7.5 CONDUCTING FOLLOW-UP INTERVIEWS

Following further evidence collection and causal analysis/ hypothesis development, more direct and structured questions can be developed for follow-up interviews. Conduct these in the same general manner as other interviews, but use a more direct, straight-to-the-point interview style. Initially, the interviewer may use open-ended questions, but follow-up, closed-ended questions are usually asked sooner than they would be asked during the initial interview. Focus on the gaps in information and apparent inconsistencies. However, take care to ensure that witnesses do not believe that the follow-up interview indicates the interviewer doubts their credibility; rather, emphasize that the investigation team is simply trying to gain greater clarity.

7.6 RELIABILITY OF WITNESS STATEMENTS

Some of the details provided by the witnesses may be inaccurate or inconsistent for various reasons as discussed above. It is possible that there may be more than one interviewer leading the various interviews who may record their observations differently. A key challenge is to compile the information received in a consistent manner, combine it with other evidence in a timeline, and determine which witness information is reliable and which is not. These issues need to be considered as the evidence is analyzed, which is discussed further in Chapter 9.

7.7 SUMMARY

Witness information is vital data and can come from a number of individuals and groups. However, it is quite fragile, so great care should be taken to get the most complete and accurate information possible. Human recollection is imperfect and is easily biased, but by applying the techniques described in this chapter, the interview team can extract the best quality information from the witnesses.

8 EVIDENCE IDENTIFICATION, COLLECTION AND MANAGEMENT

Chapter 7 details the recovery of witness evidence and Chapter 8 describes methods and practical guidelines for gathering and archiving physical and electronic evidence. The evidence obtained will be key input to the Evidence Analysis and Hypothesis Testing processes, further described in Chapter 9.

The term evidence, as used in this book, refers to the data and other physical information that the investigation team will rely on for subsequent analysis, testing, reconstruction, corroboration, and ultimately, drawing conclusions. A significant portion of these details are gathered at or around the incident site. Data requirements are also generated during subsequent analysis and testing, but these needs are not as time critical as the initial evidence collection, preservation, and documentation activities.

Evidence and data gathering is very time-consuming and can take more than half of the investigation effort, depending on the nature of the incident.

This chapter addresses types of data that may be collected and considerations for the proper identification, collection, and management of the data.

8.1 OVERVIEW

The process shown in Figure 8.1 presents typical evidence gathering activities a team might use to determine root causes and to support the development of recommendations. However, there is no firm delineation between the end of data gathering activities and the onset of root cause determination. It is common to conduct additional inspections and follow-up interviews to help confirm, refute, or clarify certain inconsistencies.

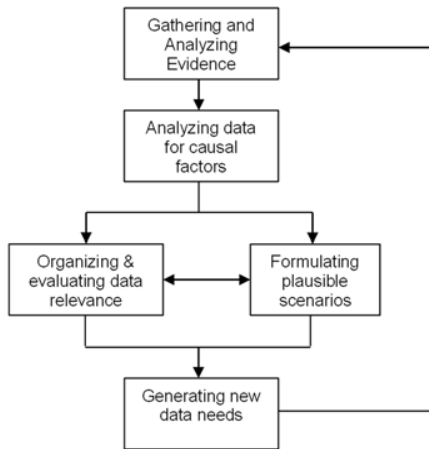


Figure 8.1 Iteration between Data Analysis and Data Gathering

8.1.1 Developing a Specific Plan

The team leader usually develops the initial data gathering plan and conducts a brief orientation visit. An early priority is to create a plan for identifying and securing the evidence before the evidence is lost or altered. Action taken by the site to help with preservation of evidence prior to the arrival of the investigation team can be critical. A high-level checklist on evidence preservation is provided in Appendix F.

Although a full investigation team may not have been selected at this early stage, the initial site visit is the first opportunity to establish the physical boundaries of the investigation. The team leader should ensure that access to the area is restricted as much as possible and that personnel who enter the incident area are aware of evidence preservation considerations.

One of the most critical issues is clearly establishing which groups have responsibility for which activities and areas. These responsibilities may change during the investigation. The incident investigation team leader should ensure that these responsibilities are clear to all groups to avoid duplication of effort or omission of critical activities.

For smaller investigations, the team may consist of only a primary investigator teamed with an assistant investigator. For this type of investigation, all of the field tasks are typically the responsibility of the primary investigator.

8.1.2 Investigation Environment Following a Major Occurrence

The investigation environment can present significant challenges following a major event. The starting point for the incident investigation could be a crater, with much information and evidence already destroyed. The team will want to quickly identify and preserve any remaining evidence to prevent the rapid degradation that can occur with time or exposure to the elements.

The site may be under the control of a regulatory agency that severely restricts access and activity, and the investigation team may need to work cooperatively with the agency having jurisdiction to progress their investigation. There may be pressure from the management of other, undamaged portions of the facility, for permission to resume operations. In addition, the infrastructure of the plant may be severely impaired and normal services (utilities, telephones, access roadways, and administrative support services) may have been significantly affected. Virtually all serious process incidents will involve litigation, which may not be initiated for a considerable time after the investigation has commenced. It is good practice, when handling evidence, to assume that litigation may take place at some time in the future. Frequently, plaintiff attorneys may initiate legal action that restricts activity at the scene of the incident and affects collection of evidence. Insurance companies often have a significant and legitimate financial interest, and therefore may influence the investigation team's activities. These parties may have a legal interest in evidence documentation, collection and testing, and demand to be present during these steps. It is important to establish communications with these other stakeholders to help ensure that the investigation team can quickly identify and preserve vital information and evidence.

The various interests of the different stakeholders can often be more easily managed through the effective use of specific, written protocols for the preservation and handling of evidence. Often, proposing a mutually acceptable evidence collection and management protocol breaks an impasse and moves the investigation forward. Evidence collection and management protocols are written in order to:

- Detail a planned procedure
- Obtain agreement between interested parties

- Obtain approval from authority having jurisdiction over the scene
- Prevent loss of or damage to evidence ("spoliation of evidence").

Under certain circumstances, and using strict control measures, it may be helpful to allow duplication of paper or electronic records and/ or material samples and make these available to the other stakeholders. Agreements can also be reached regarding mutually acceptable testing laboratories and other outside resources when limited quantities or unique pieces of evidence necessitate that all interested parties cooperate in evidence analysis.

The investigation team may be faced with the challenge of determining what equipment was the source of an explosion and what was damaged as a result of an explosion. Fragments and debris can be thrown considerable distances, sometimes outside facility boundaries. Loss of plant utilities, chemical spills, and significant blast damage to adjacent process units and buildings may greatly hamper the investigation or even prohibit access to the site for days or longer.

Identifying and capturing time-sensitive evidence is the top priority at the outset of an investigation to limit the potential for evidence deterioration due to exposure and loss of plant utilities. Electronic process data, chemical samples, fragments outside of facility boundaries, and evidence that may be altered by emergency responders and HAZMAT teams are typically high priority and should be gathered quickly. The loss of electric power to control systems places urgency on the collection of electronic data since battery backups have a limited lifespan, sometimes measured in hours or less. Chemical feed and product samples should be obtained from the area if possible since the material actually in process may have been consumed or ejected during the explosion. Fragments thrown beyond facility boundaries may be picked up by untrained individuals, and may not be returned to the plant. Offsite damage is also beyond company control, and documentation of the extent of damage may be necessary on an expedient basis, before repairs are made.

Evidence that is less time sensitive and within facility boundaries is second priority to collect. Plant personnel can better control such evidence. Nonetheless, evidence may be spread over a large area, and all personnel within the plant must be instructed on the proper manner to communicate the location of evidence for collection by a trained team.

For these reasons, the investigation environment can be challenging, and therefore a systematic approach is necessary for the successful investigation of major process incidents.

8.1.3 *Priorities for Managing an Incident Investigation Team*

The incident investigation team has the responsibility for determining the root causes of the occurrence and therefore needs access to the incident scene and other sources of information as quickly as possible. The plant and site management have the primary responsibility for preserving data and site evidence and for preventing the destruction of any evidence. Nevertheless, the investigation team should provide information to management on the evidence to preserve, method of preservation, resources needed to collect and test evidence, and other evidence related activities.

One noteworthy example is the preservation of time-sensitive data from DCS and PLC systems where uncompressed data may be held in a circular buffer that is being continuously overwritten and battery backups have a limited life. However, there are other priorities, especially in the early stages of the investigation. (Ferry, 1988). It is extremely important to note that the investigation team's responsibilities are significantly different from those of an emergency response team or search and rescue team.

Some key activities at the incident scene and the responsible parties are listed in Table 8.1. The investigation team may not be on site until several of the issues listed below are resolved.

Table 8.1. Scene Activities and Typical Responsibilities

Activity	Typical Responsibility
Rescue and provide medical treatment to any victims	Emergency response team
Decide if further onsite or offsite evacuation is needed	Emergency response team
Complete headcount	As assigned
Address environmental concerns (runoff, verification sampling for contamination from toxic and hazardous materials such as asbestos, PCBs and other possible hazards)	A variety of teams including emergency response, environmental, industrial hygiene, and possibly investigation team
Secure the incident scene to mitigate any further consequences and help to preserve evidence	Emergency response, manufacturing
Preserve evidence (See Appendix F).	Plant/ site management and Investigation team
Notify agencies as required	Site function
Preserve physical data and prevent destruction/alteration	Investigation team with assistance
Photograph data and the scene	Investigation team with assistance
Collect data	Investigation team
Have witnesses complete initial witness statements or interview witnesses while incident details are still fresh	Investigation team
Remediate and clean-up the site	Site function
Repair/restart/rebuild	Companyfunction

Site management has overall responsibility for the safety of all personnel on site, including the investigation team. However, an overriding responsibility for the incident investigation team leader is to help prevent injuries to team members and any other individuals during evidence gathering activities. Team members and auxiliary helpers could be exposed to some unfamiliar hazards, such as unstable working and walking surfaces, sharp edges, partially collapsed structures of unverified integrity, unidentified chemicals, residual hazardous materials, blood-borne pathogens, and trapped potential energy. Sometimes investigators find stray electricity in a supposedly de-energized circuit even after all known sources are isolated. This is especially notable after an incident where short circuits or fire may have fused conductors or contacts. Double-checking the actual circuit is always worth the additional effort; use of electrical lockout, locks, and tags is appropriate. In addition, lockout/tagout of other energy sources

in the work area is also critical. Finally, it is common for the team to work extended hours in a variety of weather conditions. The team leader should watch for signs of fatigue, as this can affect the safety of the team members and the quality of the investigation.

The team leader should also set a rigorous standard for consistent and proper use of personal protective equipment and team members should approach each task with awareness and a high degree of caution to help prevent injuries and minimize unnecessary hazard exposure.

If the incident has led to an interruption of production, the investigation team may have to deal with pressure from management to resume operation. For smaller incidents, production may have resumed before the start of the investigation, or it could have continued throughout the occurrence if process integrity was not compromised. In these cases, the investigation team may have to rely on the support of operations and maintenance personnel to help with initial acquisition and preservation of some of the data from the operating plant. The investigation team should provide guidance to these personnel regarding the key issues of evidence preservation. This may include an explanation on the protocols that have to be used, as discussed in 8.3.2.

For major investigations, production may be interrupted for some period of time following the incident. Pressures to resume production may be apparent from the start of the investigation and may increase as time passes. For example, once one or two *causal factors* are identified, facility staff may pressure the team to release the system for production. They perceive that “the cause” of the occurrence has been identified, and therefore the investigation must be nearly complete. However, the team usually has a great deal of work to perform to identify the remaining causal factors and the root causes of the occurrence. The team leader may need to oppose requests to conduct repairs or resume operations until the required data is collected and compiled. In some cases, the process, or portions of the process, may be released back to the manufacturing management for repair and resumption of operations before the collection of data is complete. The decision to release these portions, begin cleanup, and start rebuilding should be based on a number of factors including:

- Is it safe to reenter the area?
- Have sufficient data been collected?
- Has sufficient knowledge been gained about the causes of the incident to ensure the safety of the operation?

The decision to restart a process is a management decision and should be based on whether or not enough has been learned about the incident to prevent recurrence and sufficient measures have been put in place, as discussed in Chapters 10 and 12.4.5

8.2 SOURCES OF EVIDENCE

8.2.1 *Types of Sources*

Potential sources of useful information can extend far beyond the area of the process in which the incident occurred. Data analysis performed using the techniques discussed in Chapter 9, along with the information in this chapter and the witness information detailed in Chapter 7, should lead the team to identify these data sources.

There are five basic types of data that are useful for the investigation team:

1. **People**—Testimony or written statements from witnesses, participants, or those with information about the operation. Refer to Chapter 7 for more information.
2. **Physical**—Items such as mechanical parts, equipment, stains, residues, chemicals, raw materials, finished products, and results of analysis of parts.
3. **Paper**—Operating logs, policies, procedures, alarm logs, permits, test records, and training records are examples.
4. **Electronic**—All electronic format data are included in this category. Examples are operating data recorded by a control system (both current and historic), controller set points, and documents stored on the company intranet and in email. Email may provide a record of what and how people were thinking when decisions relating to the incident were made. This can be an important and powerful source of information. Data on personal electronic devices (e.g., texts and videos on mobile devices) is now a major contributor of evidence, as discussed in Chapter 7.
5. **Position**—Position data is related to both people data and physical data. It documents locations of people and physical data such as valve positions, tank levels, and explosion fragments and debris.

The priorities for gathering the data are guided by its fragility. The more fragile or changeable the data, the more rapidly the team should focus on its collection. Forms of fragility for each source of data are shown in Figure 8.2. The fragility of the five data types will depend on the specific

circumstances of the incident. It is not possible to offer a prescribed priority. In general, historical paper data such as procedures, maintenance records, and drawings are less fragile than people and physical data. The team should identify time-sensitive data as one of its first tasks, prioritize the data, and implement measures to collect or preserve the data.

If the team includes enough members, the data collection tasks can be assigned to individuals. For example, some team members can perform personnel interviews, while others identify and preserve physical data (and its associated position data), or gather electronic and paper data. For a major event, this type of approach may be required.

Data Source	Form of Fragility		
	Loss	Distortion	Breakage
People / Position	Forgotten Overlooked Unrecorded	Remembered wrong Rationalized Misrepresented Misunderstood	Transferred Influenced Personal conflicts
Physical / Position	Taken Misplaced Cleaned up Destroyed	Moved Altered Disfigured Supplemented	Dispersed Taken apart
Paper	Overlooked Misplaced Taken	Altered Disfigured Misinterpreted	Incomplete Scattered
Electronic	Overwritten RAM lost in power outage Destroyed	Data averaged and individual samples overwritten	Incomplete

Figure 8.2. Forms of Data Fragility

Taking the individual investigator’s skills and experience into consideration when assigning data collection tasks allows the team to progress more rapidly. Some examples of time-sensitive data are outlined below.

- Data stored in software files may be very fragile. Process computer system records are sometimes structured such that the level of detail diminishes over time. Therefore, the team may need to assign a high priority to preserving this data. Computers may have a battery backup that will preserve memory data for a finite time when power is lost. Data on disk or flash memory may be lost or corrupted on restart.

- Paper data in the form of log sheets and paper charts from the control room and other instruments should be controlled immediately to ensure they are not lost, damaged, or destroyed by environmental conditions.
- Decomposing materials can change state rapidly and the physical properties can become altered over time. The team may need to place a high priority on obtaining samples of these materials.
- Metallurgical evidence can change rapidly (e.g., the oxidation of fracture surfaces).
- Residues can be altered or washed away by rain, clean-up activities, etc.

One approach that can speed up the collection of data, as well as to ensure a more complete collection of data, is to develop a generic list of data to be collected that can then be customized for each investigation. The quicker the data is collected, the less likely it is to be compromised. Generic questions for witness data is covered in Chapter 7. Generic lists for physical, paper, electronic and position data are provided in sections 8.2.2 – 8.2.5.

The investigation team should recognize that some of the data collected may not reflect the condition of the equipment immediately after the occurrence. Emergency response activities and post-event stabilization of the system may have altered a significant amount of the data. For example, the as-found position of every valve should be recorded after the incident, but some valves may have been operated during emergency response or mitigation activities; thus, it may not be possible to determine with complete certainty their positions at the time of the incident. Interviews with emergency response personnel may clarify whether equipment was manipulated or relocated.

There may be other information that is useful and does not necessarily relate to the operation of the process equipment. For example, the extent of the damage to structures can be used as a guide to estimate the corresponding blast loads developed during an explosion. This can be evaluated using standard damage assessment references, (Ferry, 1988; Stephens, 1970; Merrifield, 1990) although more recent techniques (CCPS, 1989; Baker, 1983; CCPS, 2012; ASCE, 2010) may produce results that have a greater accuracy. This exercise requires the collection of data related to the structures that are damaged, structures that are not damaged, and details regarding the explosion source.

- A high-quality process safety information (PSI) package, including process hazards assessments (PHAs), is uniquely valuable to the investigation team. Unfortunately, the PSI package may have been partially damaged or even destroyed in the incident. It is good practice to maintain a backup duplicate package in a less vulnerable location. Alternatively, the information may be available on the company intranet. In some cases, the information may be more limited and the team will need to work with the data available.

In most cases, it is best for the team to work with photocopies of paper documents (such as check sheets, permits, recorder charts and alarm printouts) to avoid damage, alteration, or loss of the originals.

In addition to the data sources typically available within the facility or organization, other sources of information for the investigation team may include:

- News media video footage
- Video footage from nearby business security cameras
- Social media content
- Contacts with other manufacturers with similar processes
- University research organizations
- Proprietary databases such as those maintained by insurance carriers
- Freedom of information document access to government records
- Former employees of contract maintenance companies who have personal experience (but not necessarily any vested interest) in the unit of interest
- Transcripts of police and other emergency service communications

8.2.2 *Physical Evidence and Data*

Physical data can provide a source of valuable information for investigators. When examining physical data, typical items and matters of interest include:

- Fractures, distortions, surface defects/marks, and other types of damage to tanks, vessels, valves, piping and other process equipment
- Blast damage
- Items suspected of internal failure or yielding

- Pressure containing equipment
- Gaskets and flanges
- Seized parts
- Misaligned or misassembled parts
- Control or indicating devices in the wrong position
- Use of incorrect components
- Samples from all relevant vessels and piping including:
 - Raw materials
 - Intermediate products
 - Completed products and chemicals
 - Pools of residues of chemicals or materials
 - Waste products (solids, liquids, gases)
 - Scales and deposits
 - Quality control samples
 - Any "new" chemicals present
- Foreign objects
- Portable and temporary equipment (including tools, containers and vehicles)
- Undamaged areas and equipment
- Pressure relief device components
- Metallurgical samples
- Conductivity measurements
- Explosion fragments
- Data recorders
- Sensors
- Process controls
- Electrical switch gear
- Missing physical data such as plant and equipment, stains, oxidation, etc.

Not everything in the incident zone will be significant, although it is often important to identify equipment, structures, and pipework that are not damaged. The key is to quickly identify what may be irrelevant, while causing minimum disturbance to what could prove to be relevant. This judgment is based on team members' experience and expertise. Key physical items should be photographed and tagged before any movement, if possible. A guide rule for the decision on what to keep is—*too much is better than too little*.

Any known or anticipated dismantling, disassembly, or opening of equipment should be planned and coordinated with the appropriate groups using a test plan or written protocol. This is important to ensure the activity is conducted in a safe manner while not inadvertently damaging evidence.

Furthermore, consideration should be given to the preservation of fragile physical evidence such as cracks, deposits, chemicals and residues.

8.2.3 Paper Evidence and Data

Although paper data is not always fragile, investigators should place a high priority on identifying, collecting, and preserving it. Often, the most difficult issues with paper data are locating the required documents and finding the relevant information within them. Analyzing paper data can be a very time-consuming process.

Paper data in the form of operator logs, batch sheets and additions sheets or logs may be particularly important if reactive chemistry is suspected. These may highlight the accidental mixing of incompatible materials, improper sequencing of additions, or improper addition rates or volumes.

The size and scope of the investigation or other factors could mandate a special document control procedure, wherein each document is given a unique identification number. In this way, there is a documented chain of custody (e.g., what documents have been collected, the source of the documents, who has possessed the documents at any given time, etc.). Maintaining a complete, retained document set can help minimize confusion and a special log can be useful in maintaining some degree of control over the flow of paper documents and in finding the answers to questions in the documents when they arise. This is especially important when legal issues or regulatory agencies are involved.

Paper data from older instrumentation systems such as strip or circular chart recorders should be controlled immediately after the occurrence. Strip charts and disk recorders will not all turn at exactly the same rate, so checking the turn rate can be critical in comparing the charts. The measurement range and units for each pen must also be ascertained. For crucial charts, it may be necessary to perform a check of the calibration. If chart recorders are still operating, before removing the charts, mark and document each one with a time, then wait 30 minutes or an hour and mark again. Mark each item with the instrument number or name, the date, time of removal, and the last position of data recording. Make sure that replacement charts are re-installed after collecting the original ones; key data pertaining to subsequent occurrences related to the initial event can be lost if the charts are removed too early or not replenished after removal.

Paperwork may be recovered from locations exposed to an explosion, fire, chemical release, fire-fighting materials, and the weather. Wet or contaminated documents should be dried and/or decontaminated. Some of these documents may be partially destroyed and very fragile. Commercial services are available to facilitate document drying and preservation.

As part of the investigation process, there is often a need to collect a vast amount of documentation. It may be necessary to dedicate one full time person to execute and manage the documentation associated with the investigation, to free up the team members for other investigation activities. This individual would be responsible for a document control and chain of custody procedure for all documents that enter or leave the site of the incident investigation. NFPA 921 provides guidance on chain of custody (NFPA 921, 2017). Maintaining accurate records of the documents distributed to outside agencies during the investigation is essential when legal or regulatory issues are involved.

Examples of specific paper data resources that may be useful during an investigation are shown in Table 8.2Table 8.4.

Table 8.2 Examples of Paper Evidence

Examples of Paper Evidence	
<p>Management Policy and Programs</p> <ul style="list-style-type: none"> • Company safety policy • PSM program and procedures • Contractor records/procedures/policy manuals <p>Site details</p> <ul style="list-style-type: none"> • Site description • Construction project files • Site map/ plot plan / firewater plan <p>Design/ Hazard Analysis</p> <ul style="list-style-type: none"> • Material safety data sheets (MSDS) • Operating procedures, checklists, and manuals • Piping and instrumentation drawings • Material and energy balances • Process specification sheets • Equipment installation drawings • Equipment Engineering drawings • Electrical area classification drawings • Process hazard analyses (PHA) • Design calculations and design basis assumptions • Scenarios for the sizing of relief, venting, and emergency equipment • Dispersion calculations • Descriptions of normal and abnormal chemical reactions, including incompatibilities • Consequence analysis study results • Safe operating limits • Alarms and set points for trips • Instrument and electrical drawings • Interlock drawings • Ladder logic drawings • Control system software logic • Engineering standards and codes • Management of change (MOC) records • Prior incident investigation reports • Completion of actions from PHAs, MOC and previous incidents 	<p>Operating / Maintenance Data</p> <ul style="list-style-type: none"> • Shift log sheets • Run histories / Batch sheets • Process data records—strip and circular charts • Raw material quality control records • Retained sample documentation • Quality control (QC) lab logs • Work permits • Lockout–tagout procedures and records • OEM manuals • Maintenance procedures <p>Inspection Data</p> <ul style="list-style-type: none"> • Maintenance and inspection records • Repair records • Corrosion data • Test/inspection procedures <p>Incident Data</p> <ul style="list-style-type: none"> • Meteorological records • Phone logs • Emergency responder logs • Printed event logs • Gate/building entry/exit logs <p>Personnel</p> <ul style="list-style-type: none"> • Training manuals and records • Professional qualifications • Job instruction development • Supervisor selection criteria • Supervisor training requirements • Aptitude exams • Physical exams • HR records • Supervisor appraisal • Employment application

8.2.4 *Electronic Evidence and Data*

In addition to process control systems, many companies have introduced electronic systems to replace the older paper systems described in 8.2.3. As part of the facility's incident pre-planning, consideration should be given to the remote storage of electronic data, including process data, as discussed in Chapter 3.

As outlined in 8.1.3, process data that is held on DCS and PLC systems can be particularly fragile. Critical uncompressed data may be held in a circular buffer and then compressed and/or encrypted when stored; data from such systems could be lost when they are powered down. This can occur due to the limited life of back-up power systems following loss of power supplies. Even if power is maintained, the circular buffer holds a limited duration of data (e.g., 72 hours), and with each passing hours, the oldest hour of data in the circular data is overwritten with the current hours data. Specialists with particular expertise of the hardware and software involved and data recovery are needed at a very early stage to maximize the amount and quality of the data that can be recovered from these control systems. Once the data has been retrieved, a back-up copy should be made on a different computer or storage device to avoid accidental data loss.

In one example involving process data, an investigator had to download the information within the preset file purge time of eight hours, otherwise it would be lost. However, the programmer was on vacation and there was no documentation available on the program. Much of the data was therefore lost.

Examples of electronic data are provided in Table 8.3.

Table 8.3 Examples of Electronic Data

- Backup of data from control system such as distributive control system (DCS) and programmable logic controller (PLC). Data includes historic trend data, set points, measured values, trends, event logs, etc.
- Configuration files from control system, including range, alarm settings, units, etc.
- Data from interlocks/ Safety Instrumented Systems including event logs, activations, overrides, etc.
- Any electronic records that replace paper systems as detailed in Table 8.1, such as maintenance records, permit to work, MOC, etc.
- Security camera video (on site and from neighboring sites)
- Email records from operations, maintenance, and management
- Data from personal electronic devices (see Chapter 7)
- Telephone and text records
- Gate/building entry/exit records
- Newscasts showing footage of the incident.

8.2.5 Position Evidence and Data

Position data is the last of the five data types and is often linked to people data (See Chapter 7) and physical data. Position data may help answer the following typical questions.

- What failed first?
- Where did the fire start?
- Where was the pressure the highest?
- How far did an object travel?
- Where was the witness at each point during the incident?
- How far apart are the two items?
- Which gaskets failed and which did not?
- Is the distance between the scratches the same as the distance between the protruding bolts?

Examples of position data are provided in Table 8.4 below.

Table 8.4 Examples of Position Data

- *As found* position of every valve related to the occurrence
- *As found* position of controls and switches
- Condition of relief devices (e.g., open/ closed)
- Tank levels
- Pointer needle positions from locally mounted temperature, pressure, and flow devices.
- Location of flame and scorch marks
- Position and sequence of layers of materials and debris
- Direction of glass pieces
- Missile mapping
- Locations of parts removed from the process as part of maintenance
- Locations of personnel involved in the maintenance and operation of the process
- Locations of witnesses/ witness views
- Location of equipment that should be present but is missing
- Smoke traces
- Location or position of chemicals in the process
- Melting patterns
- Impact marks
- Assembly of equipment
- Locations of training aids and procedures/checklists

Position data is one of the most fragile types of data. It can be lost through many activities including:

- Emergency response activities
- Fire extinguishment
- Removal of the injured
- Stabilization of the system, including repositioning of valves/switches/controls, draining of tanks
- Witness movement
- Restoration/stabilization/demolition work
- Degradation from weather
- Investigator actions

Typically, position data are recorded by documenting visual observations via photography/ video, drawings, maps, and measurements. An example photo that documents an as-found valve position is provided in Figure 8.3.



Figure 8.3 As-found Position of Valves—Example Photo

Taking photographs as soon as possible after the occurrence helps to document the “original” condition of the equipment and site right after the incident, before post-event response activities such as site clean-up and demolition activities potentially alter the data.

Document the position of all witnesses (including injured personnel), immediately before, at the time of, and immediately after the occurrence, with special attention given to determining the direction they were facing at the time they first became aware of the occurrence and what first drew their attention to the event. The investigators should attempt to determine and/or confirm what each witness could or could not see from their respective positions throughout the occurrence.

The locations of marks such as scratches, dents, paint smears, and skid marks that could possibly be associated with the incident should be identified and documented. It is important to determine if such marks were made before, at the time of, or after the incident as part of the emergency response or clean-up.

Stains or discoloration can be the result of numerous causes, including heat exposure, overflow, release of material from adjacent equipment, or some internal occurrence. Again, it is important to determine when the stain

or discoloration was created relative to the time of the incident and the subsequent emergency response, recovery, and clean-up activity.

The team should record the accumulation of soot or airborne fallout debris and the overall deposit pattern. The investigators should also note irregularities, breaks/gaps in the pattern, or the absence of soot or fallout, especially when there is an anomaly in the pattern. Any differences in depth, color, pattern, or appearance, should be noted, examined, analyzed, and photographed.

Maps and diagrams should be used to document the locations of items such as people, equipment, materials, and structures. Measurements to reference points can be written on the drawings. The movement of key personnel can be traced on a map or plot plan. Using color-coding and recording the times the individuals were at each location can help to understand the testimony of witnesses.

Certain incidents, such as explosions, may require special mapping of fragments and selected debris. By careful documentation, established at the onset of the investigation, it is possible to create an accurate diagram of the relative position of the various pieces of a vessel after an explosion. By using the data from this missile mapping, knowing the weight of each fragment, and having an indication of the trajectory of fragments, it may be possible to estimate of the energy release of the explosion. The energy release value can sometimes be used to confirm or rule out certain proposed scenarios. The Pietersen (Pietersen, 1985) report on the Mexico City LPG terminal disaster is an excellent example of such a study. Comprehensive treatment of analysis techniques can be found in Baker and CCPS (Baker, 1983; CCPS, 2010).

8.3 EVIDENCE GATHERING

The following sections describe the initial site visit, evidence management, team tools and supplies, and advice on photography. Some activities may proceed simultaneously, including the witness interviews discussed in Chapter 7. As a result, it may be necessary for the investigation team to split up assignments. The team leader should ensure that everyone understands their respective roles and responsibilities. An “Action Reminders” list is included in Appendix E.

8.3.1 Initial Site Visit

Once the preliminary investigation plan has been established, the next step is usually the initial visit by the investigation team. This is not intended to be primarily a data-gathering activity. It is, instead, an orientation walkthrough to establish perspective, relative distances, dimensions, orientations of equipment, scale or magnitude of damage, anticipated logistical challenges, and enable planning of specific initial photography/ video recording or sampling activities. For example, the picture in Figure 8.4 may be helpful in determining which direction the pressure wave traveled.



Figure 8.4 Initial Site Visit—Example Photo

The initial visit to the incident location presents unique opportunities for investigation. It assists in identifying any potential hazards the investigation team may need to address during the later fieldwork and also gives the team the opportunity to note what was not damaged. Clean-up efforts should not be permitted at this point, as the evidence is in its optimum position and condition to provide reliable information for the investigation. Team members participating in this visit should make a slow and deliberate circuit from the outside perimeter, rather than rushing immediately to the suspected point of origin. Most investigators will benefit from intentional pauses during the circuit to allow them to catch up and assimilate available

information. A common mistake is for investigators to quickly spot the obvious and then move on to the next obvious observation. However, questioning the obvious and looking carefully at all of the equipment is often the key to discovering important data. The longer the investigators stay in one place, the more likely they will become aware of other data. Most investigators need to force a slow pace during the observation circuit in order to allow the brain to register what the eyes are seeing. Another advantage of this initial perimeter circuit is that it gives an opportunity to see the big picture before focusing on the smaller, but potentially highly significant details.

For fire and explosion occurrences, the team should make a careful and detailed observation visit to the suspected point of origin. One successful technique used by fire and explosion investigators is to face outwards from the suspected point of origin, and then walk away from the point of origin. During this walk, the investigator notes what was exposed to the energy release, recording details such as insulation damage on the exposed side. The investigator then turns and walks directly towards the point of origin observing what is not damaged on the side and surface of the items that were shielded from the energy release. Data gathering is intended not only to provide conclusive proof of what happened, but also may provide conclusive data to reject a hypothetical scenario. For example, a potential source of hydrocarbons in a vent header could have been a leaking rupture disk. If an examination of the disks finds them all to be intact, that potential scenario can be rejected.

During the orientation tour, the team should use necessary safety precautions, including appropriate personal protective equipment. If it is safe to do so, photography during this stage is normally quite productive; however, care should be exercised to not disturb physical data. Taking notes and making rough sketches and videos can be useful at this point. In the case study (Appendix D), the investigation team was able to visit the site before any of the physical evidence was disturbed. The maintenance foreman, under guidance, was given the duty of taking photographs of the damaged area.

The investigation team should make a conscious effort to determine *what is absent that would be expected to be present* during the operations that were being conducted. This determination requires a relatively thorough understanding of the operation, activities, and physical systems on the part of the investigation team members. In most cases, this determination is not

at all obvious and the assistance of the facility operations and maintenance teams should be sought.

At the time of the initial team visit, the incident scene may still be under the control of the emergency response organization. Any restrictions established by the emergency response organization need to be followed. It is common for the team to require an escort for this initial visit. Portions of the investigation area may remain under the administrative control of the emergency management organization for extended periods following the incident. If necessary, the investigation team can ask emergency responders to answer questions about the site, to take photographs, or to collect data.

Immediately following the initial field tour, the team will begin developing the detailed investigation plan, specifying action items, and assigning responsibilities. Some experts find that it is helpful to repeat the field tour the next morning, before any clean-up is permitted. It is often surprising how much additional data is observed that was missed on the initial tour.

This is a point in the investigation where the need for specialists may be identified and plans are initiated to secure their services. One lesson learned from experienced investigation team leaders is to not assume that the team possesses a particular skill or expertise. Delayed discovery of a missing or incomplete team competency can lead to frustrating delays and loss of valuable information. Correspondingly, individual members should decline an assignment beyond their expertise.

It is critical to develop a plan for sharing documents and information among groups very early in the investigation. This plan should have a specific protocol for document control as outlined in section 8.2.3, thus establishing a clear record of where and to whom specific documents were distributed. This plan is especially important if regulatory agencies are involved or if litigation is anticipated.

8.3.2 Identifying and Documenting Evidence

The level of rigor required for the identification and documentation of physical data will usually depend on the nature and scale of the incident. As soon as possible, the lead investigator should develop an agreement with any other interested parties (regulatory agencies, insurers, fire departments, and representatives of potential plaintiffs), on the necessary rigor required for identifying and documenting evidence. A series of mutually acceptable protocols may need to be developed for the handling of the evidence. The

methodologies outlined below would be necessary for a significant incident, or for an incident where multiple parties are involved and litigation is likely to take place at some stage in the future.

Once the site has been inspected and its post-incident condition has been recorded and photographed, the next stage for the investigation team is to conduct a more detailed examination of the physical evidence. Documenting a list of parts, samples, and other physical data that are collected during the investigation, with each part tagged, numbered and/ or permanently marked (where this does not damage evidence) helps prevent mishandling or disposal of the items. Color-coding via tags or paint can be helpful to those engaged in moving or removing debris. One method is to have the demolition crew move only material that has been clearly marked. The guiding rule is: *if it is inside the investigation zone and it is not marked, then it is to be left alone*. Long, intermittent runs of piping should be marked at regular intervals, especially where the piping passes across the boundary of the investigation zone. Tag attachment should be robust and secure, such as plastic tie-wrap type devices. It is a good practice to photograph the item prior to and after attaching the tag to collected items and to log each of the tags.

Some evidence will be highly mobile (e.g., small parts of valves and instruments, personal protective equipment and tools belonging to injured workers). Other items will be perishable (e.g., residual liquid and residue inventories for example) and will require careful handling under the guidance of a written protocol. Electronic data may be difficult to download but is easier to duplicate. A good practice is to bring a large capacity storage device such as a solid-state hard drive to use as a “master” storage device for use by all team members, and which is backed-up on a daily basis. Access to electronic data should be restricted if there is potential for litigation. It is important to set up a numbering system that can be applied to a variety of types of physical and documentary data, such as that shown in Table 8.5.

Table 8.5 Example Data Collection Form for Recording Physical Evidence

Physical		Paper		Electronic		Position	
Item No.	Equipment parts, raw materials, packaging, stains and residues etc.	Item No.	Documents, logs, policies, procedures, test records, etc.	Item No.	DCS data, trip data, set points, email, intranet documents, personal electronic device data	Item No.	Physical locations to inspect, e.g. valve positions, tank levels, debris, etc.
Ph1		Pa1		E1		Po1	
Ph2		Pa2		E2		Po2	
Ph3		Pa3		E3		Po3	
Ph4		Pa4		E4		Po4	
Ph5		Pa5		E5		Po5	
Ph6		Pa6		E6		Po6	
Ph7		Pa7		E7		Po7	
Ph8		Pa8		E8		Po8	
Ph9		Pa9		E9		Po9	
Ph10		Pa10		E10		Po10	
Ph11		Pa11		E11		Po11	
Ph12		Pa12		E12		Po12	
Ph13		Pa13		E13		Po13	
Ph14		Pa14		E14		Po14	

Once the evidence has been identified, stabilized, labelled and documented, a chain of custody procedure should be used for situations where the evidence needs to be moved. This may be necessary for many reasons including:

- Evidence preservation (security/ protecting from the weather)
- Transportation to a test facility
- Cutting or collecting samples

Chain of custody is an important issue for investigators to address for physical data. This is not only a concern from a legal and regulatory perspective, but it is also a good practice that ensures each item collected is retained, preserved, evaluated, and tested as intended. Large accidents can have hundreds, if not thousands, of evidence items and keeping track of all items is a critical task. Some data may be of interest to multiple groups. This varied interest requires a clearly understood and well-communicated method for data identification which can be controlled by the use of protocols.

It can be helpful to establish a secure “evidence room”, which should have restricted access and is under the control of one individual from the investigation team. The initial documentation of evidence should include the details shown below:

- Item identification (number and text)
- Condition
- Date and time placed in evidence room
- Person delivering the item (including signature)

- Person receiving the item (including signature)
- Original location (where found)
- Photograph or video reference number

Moving an item from the evidence room, should be conducted under a chain of custody procedure that will typically include the following information:

- Item identification (number and text)
- Originators name (and signature), date, time
- Receiver's name (and signature), date, time
- Upon return to evidence room, delivery and receipt signatures, dates, and times

8.3.3 Tools and Supplies

The following equipment has been found to be useful for incident investigation. Appendix E includes a checklist for equipment that may be required at an investigation site. Not all is needed or appropriate for every investigation, but it should be available on short notice. An inventory of all of the equipment should be maintained and periodically reviewed to ensure it is available when needed. Note that some of this equipment may be prohibited from the incident site due to hazardous area classification or other site policies.

Personal Equipment

The items below can be packed into a single soft pack container that can be carried with shoulder straps or attached around the waist, thus leaving both hands free.

- notepad, clipboard, pens, pencils
- small plastic bags (sandwich size)
- duct tape
- string
- toothbrush (for cleaning soot/debris off selected evidence)
- Swiss-Army knife, scissors, Phillips and regular screwdrivers
- flashlight (explosion proof)
- pocket extension mirror
- magnifying glass
- 25-foot retractable tape measure
- 6-inch or 1-foot ruler
- permanent marker

Protective Gear

- hardhat, goggles, gloves (rubber and latex), safety shoes or boots meeting site requirements
- extra pair of socks and gloves
- respiratory protection (1/2 mask air purifying devices with a supply of organic vapor/acid gas (OVAG) and general purpose cartridges or other as required)
- waterproof suit, acid/ chemical resistant suit, disposable suit, etc.
- fall protection equipment

Team Supplies

- quality digital camera, capable of taking sharply focused photos (both close-up and wide angle), flash, film or data cards, extra sets of batteries
- barrier tape
- tags with plastic ties
- 1-gallon (3.785-liter) plastic bags, self-closing
- small first aid kit
- plastic jar (1-quart or 1-liter size) with tightly closing cap
- level
- video camera with extra battery pack and extra data cards
- pocket dictating recorder with extra batteries and extra memory card
- pair of walkie-talkie radios with extra batteries
- thermometer
- compass
- 100-foot (30.48-meter) steel measuring tape
- spray paint, paint stick markers, grease pencil (waterproof, indelible marking pens, dark and white)
- small tool kit, non-sparking type tools (channel lock pliers, needle nose pliers, screwdrivers adjustable wrenches, clamps, tie-wire, valve wrenches)
- large supply of duct tape
- plastic drop cloth (100 ft²/9.2 m²) for data preservation/protection
- masking tape
- sticky notes—various sizes and colors
- data collection forms (Table 8-5)
- chain of custody forms
- notebook computer/ tablet for documentation tasks
- electronic media for file backup (solid state hard drives/ CDs / DVDs/ Flash memory cards)

8.3.4 Photography and Video

Photography can be used to capture a great deal of information about the condition of equipment and the relative positions of items following the incident and can be used throughout the investigation process. The term *photography* is used in this section in the broadest sense and includes film cameras and a host of digital recording devices. Since the earliest days of image reproduction, investigators and documenters have applied this powerful tool in continuously more creative ways. Drones are proving to be extremely useful tools to collect video evidence from incident sites, although safety regulations must be followed and may disallow their use.

Although photography of the scene as soon as possible after the incident should be a high priority for the team, emergency response activities, including treatment of injured personnel, containment of chemical spills, securing unstable equipment, and de-energizing systems always come first. Some hazard reduction activities could take days or weeks; nonetheless, photography may be possible in selected locations as designated by the incident commander.

There is an increasing tendency for witnesses to use their mobile telephones to record incidents as they occur. While this is not encouraged (and is often contrary to safety and security regulations) evidence on such devices can prove to be invaluable as part of the investigation process. This is discussed further in Chapter 7. It may be appropriate to declare an amnesty from disciplinary action (for use of the device against policy) in order to obtain as much relevant data as possible from personal electronic devices, although advice from legal counsel should first be sought (See 7.3.4.11). Video footage can appear on social media platforms several weeks after an event, although this data should be treated with skepticism since some details can be doctored or even faked.

Incident investigation involves varying levels of photographic expertise. For most minor incidents, the team or a company employee can adequately meet the photographic needs. Incidents that are more serious may require an experienced individual, such as a forensic specialist, who systematically documents the scene, equipment involved, damage, evidence collection, and position data. For specialized photographic needs, the services of a professional commercial photographer or other specialists are necessary and are justified.

Examples of such needs include:

- Microscopic analytical views
- Magnetic Particle Inspection
- X-rays
- Infrared
- Complex sequences
- Extremely close-up views of machinery or equipment
- Nighttime shots
- Drone video and still photography

It is obviously desirable to photograph objects of interest before they are disturbed in any way. This includes moving, turning over, or even lifting to tag or affix an identification number. A thorough and up-to-date log of all photographs is invaluable. Whenever possible, identify the data as part of the photograph itself. Data preservation concepts can and should be included in the initial and periodic refresher training given to personnel involved in incident investigation. Photographic equipment containing electrical components should be intrinsically safe if used in any location with potentially flammable concentrations of vapors. Plant safety procedures will frequently dictate the atmospheric monitoring requirements and types of equipment that can be used. Cameras for use in electrically classified areas are available, although these still need to be used within the site safety regulations.

Digital cameras are standard tools for investigations. They are relatively simple to use, inexpensive, reliable, and can perform most tasks needed by the incident investigation team. Digital SLR (single lens reflex) cameras with good close-up capabilities may be needed for specialized documentation, such as fracture surfaces. Compact digital cameras are available which are rugged and weatherproof, with built-in flash and automatic focus and settings. These smaller cameras are more easily carried and suitable for general documentation and many macro photography needs.

For incident investigation documentation, a camera with a resolution of at least 5 mega pixels is recommended and resolution of 10 to 20 mega pixels is suggested to allow for enlargements without significant loss of clarity. Ideally, the camera will also have the capability for extreme close-ups and a zoom capability for pictures of distant objects. Although digital photography has many advantages for most investigations, digital photographs may be challenged as admissible in court proceedings.

However, if the original camera data card is removed, labelled, sealed, and properly catalogued, it is more likely to be admissible. It is therefore necessary to carry several newly formatted data cards in the investigation pack.

Additional lenses are sometimes useful. The wide-angle lens can show relationships between equipment, and, for close up work (less than 3 feet or 1 meter), a macro lens has great advantages. Detailed discussions of photographic technology such as depth of field, shutter speeds, filters, F-stops, and other types can be found in other publications.

The investigator should have some prior experience with the particular camera used in the investigation. An avoidable mistake is to use the camera for the first time during the actual investigation. Shooting 20 to 30 different types of photos in advance using various features (macro, zoom, etc.) and under various conditions (outdoors, indoors, poor light, etc.) is a good investment of time. Additional advice and guidelines on photography are provided in Appendix A.

The normal practice is to designate a single person on the incident investigation team to coordinate photography. This person works closely with the team member responsible for documentation and record keeping and coordinates with other groups outside the team. Note that duplicate photographs between team members is not problematic; not having a photograph of a key item is. It is better to err on the side of caution and repeat photographs rather than potentially miss an item. An accurate, complete, and up-to-date log of photographs is a necessity. For most process safety-related incidents, each photograph should be identified with the following information:

- Time and date taken
- Key item of interest (content)
- Orientation of the photo (e.g., "looking east from reactor R-123")
- Identity of the person taking the photograph
- Sketches, drawings, and plot plans to document the perspective of each photograph rapidly if needed to augment or as an alternative to the orientation entry

For digital photography, these additional procedures should be followed:

- Always use a newly formatted data card
- Use maximum resolution

- Do not delete any photographs from the data card
- Remove the data card after use and copy the data to back-up
- Label, bag, and safely store the original data card

A camera's automatic date and time feature is useful, especially when conditions are changing. The investigation team should understand, however, that such camera imprinted date/time markings are generally *not* accepted in most courts unless auxiliary documentation is provided (for example, logbook). When using the date and time feature, be aware of possible interference with the composition and background. Sometimes the date stamp obscures or confuses the image of the object of interest. In addition, be sure to check that the automatic settings are correct prior to beginning work each day.

Digital video photography represents another powerful tool for recording data, although digital video recordings are usually in a lower resolution than digital photography. Follow the same procedure for the data cards, with the original card clearly marked and preserved, and copies of videos made for working purposes. One major advantage of a video recording is the ability to have a narrated commentary, thus reducing the clerical load on the investigator. Another unique benefit is the capability to capture motion as a particular investigative action unfolds, such as the opening or disassembly of a piece of equipment. A common error in video recording is inadequate lead-in time before panning the camera. Allow a full 15 seconds at the beginning of each shot. This lead-in time is needed if the recording is later edited for reports or training.

A special application of photography is to record the viewpoint perspective of a particular witness. This can sometimes enhance the witness testimony, clarify apparent inconsistencies, and verify key items in question. When a close-up picture is needed to show detail, it is important to take a second picture farther away to put the detailed picture in context.

Before-the-event photographs may be difficult to find, although it is good practice for companies to retain photographs of their facility. One possible source is construction progress documentation shots. Another is satellite imagery such as Google Earth™ or similar "street view" resources, which are generally available across historical dates. Company websites, annual reports and advertising departments can sometimes produce a useful picture, although usually not of the exact view desired. Current and retired employees sometimes possess photographs of the area in which they used to work. Sometimes if the need or request is publicized in a productive and

positive manner, illicitly taken “before” photographs may turn up anonymously.

8.4 TIMELINES AND SEQUENCE DIAGRAMS

During the evidence collection process, it is helpful to construct a timeline or sequence diagram. Starting the timeline/sequence diagram early and expanding it as the investigation progresses ensures that relevant events and conditions are captured. Gaps in the timeline/sequence diagram can be identified, which lead to investigation actions to fill the gaps. Chapter 3 provided a history of timelines and sequence diagrams with reference sources. The following sections describe construction of a timeline or sequence diagram.

8.4.1 Constructing a Timeline

Organizing Data with a Timeline

Timelines organize events and data in chronological order. Besides the sequence of events, it is helpful to include conditions in a timeline; however, it is important to distinguish between events and conditions. Conditions tend to be passive items, such as *the pump **was** running, the pipe **was** corroded, or the operators **were not** trained on the draining procedure*. Condition statements are identified by the words *was* or *were*. *Events* by contrast are active, such as *the pump started up or the pipe failed*. Both events and conditions can be facts if verified. However, they can also both remain as suppositions if not verified or corroborated.

The timeline can also include non-events or omissions, such as: *failure to follow a step within standard operating procedure or relief valve failed to open at the set point*.

Developing a Timeline

Developing a timeline is an iterative activity, extending across the entire life of the investigation. The timeline increases in content and accuracy as new information becomes available and inconsistencies are clarified and resolved. Timelines can be developed using various forms and levels of complexity, usually dictated by the particular circumstances of the investigation being conducted. The timeline helps the team to see the events in a chronological order. This can help them understand when—and perhaps why—important events took place. Any pertinent information or evidence is

inserted in the timeline. When gaps are observed, the team can try to find the information to fill in those gaps. Timelines deal with a combination of data to be charted. Some of the data that will go on a timeline is very precise, both in timing and in values. For instance, the printout of operating conditions and alarms from a basic process control system or a safety-instrumented system may show:

- When a particular parameter was exceeded, to the tenth of a second
- The rate of change for that particular parameter
- The final value before the incident occurred

Process control systems and associated logs provide data with time stamps. However, the way the process control systems records data can lead to misinterpretation of the data. For example, an alarm may be recorded at a specific time for the level in a vessel exceeding the high-high level, but the process data does not show the level reaching that level until one second after the alarm. Alarms may be recorded at the actual time the alarm event occurred, whereas process data are recorded only at the sampling interval of the system. In instances where timing precision is critical to determining a sequence of events, the scanning frequency of the system recording the data should be investigated to determine the actual time precision of the data.

Figure 8.5 is an example of a simple timeline using Distributed Control System (DCS) data from the incident example discussed in detail in Appendix D.

11:10:21 AM	Heat detector alarms for Kettle area annunciate (DCS, assumed fireball #1)
11:09:30 AM	LEL detectors in Catalyst Prep area alarm (DCS)
11:05:03 AM	Plant wide electrical outage (DCS, time of pump shutdowns)
11:03:45 AM	Kettle #3 high pressure alarm acknowledged (DCS)
11:03:15 AM	Kettle #3 high-pressure alarm alarms (DCS)
11:00:47 AM	Kettle #3 level reaches 90% (DCS) but alarm does not log (later found inhibited)
10:30:33 AM	Control room operator initiates filling of Kettle #3 (DCS)

Figure 8.5 Timeline Example Based on Precise Data

On the other extreme, a field operator's observations and actions may be less precise. "Sometime around noon," or "right after the 10:00 AM morning break," may express these approximations.

Figure 8.6 is an example of a simple timeline using imprecise data from the field operator. This timeline uses a portion of the approximate data from the incident example discussed in detail in Appendix D.

11:15 AM	<ul style="list-style-type: none"> ◆ Plant fire brigade reaches emergency location (plant dispatch log)
11:12 AM	<ul style="list-style-type: none"> ◆ Plant fire brigade called (plant dispatch log)
11:10 AM	<ul style="list-style-type: none"> ◆ Control operator tries to reach outside operator by radio, but there is no response ◆ Heat detector alarms for kettle area annunciate ◆ "Whooshing" noise heard
After outage	<ul style="list-style-type: none"> ◆ Control room operator asked outside operator to visually inspect Kettle #3 due to high LEL alarm ◆ Thunderstorm passed and rain diminishing ◆ Kettle #3 exit piping cracks (concluded from data)
11:05 AM	<ul style="list-style-type: none"> ◆ Plant wide power outage ◆ Kettle #3 high pressure alarm acknowledged ◆ Kettle #3 high pressure alarm sounds
11:00 AM	<ul style="list-style-type: none"> ◆ Severe thunderstorm starts
10:30 AM	<ul style="list-style-type: none"> ◆ Control room operator initiates filling of Kettle #3 ◆ Contractor enters Reactor Area to replace gas detectors

Figure 8.6 Timeline Example Based on Approximate Data

Normally the investigator is presented with a combination of both precise and imprecise data. Mixing these significantly different data often proves to be a challenge—a challenge, however, that can be overcome simply by understanding the source and precision of the data and the use of appropriate graphing techniques. One such technique involves using a line with timing marks as the common boundary between the two different types of data. On one side of the line, the known precise data is logged against the

timing marks. On the other side of the line, imprecise or approximate data is listed within the period in which it occurred. This is usually displayed as an event occurring sometime between two timing marks.

Figure 8.7 is an example of a timeline that uses a mixture of precise and imprecise data from the incident example discussed in detail in Appendix D.

One additional benefit of this technique is that the imprecise approximate times can often be narrowed when compared to the precise data. For instance, the operator may realize that when he manually closed valve A, valve B had already been automatically closed. Therefore, the period within which he closed valve A is narrowed.

Timelines do not have to end at the time of the occurrence or incident. Sometimes post occurrence data can be valuable. Often, it is important to understand how the emergency response actions affected the ultimate outcome of the occurrence. This type of data can be used to improve emergency response actions in the future. Also, changes made during emergency response to positions (valves, switches, debris positions, etc.) can be important to interpretation of the data.

When timelines are combined with simulations, they become powerful tools, both in understanding the sequence of the events leading up to the incident and in the development of accurate recreations. This allows for a more thorough and comprehensive analysis.

	11:15 AM	◆ Plant fire brigade reaches emergency location (plant dispatch log)
	11:11 AM	◆ Plant fire brigade called (plant dispatch log)
	After heat detectors alarm	◆ Control operator tries to reach outside operator by radio, but there is no response
		◆ Plant fire brigade called (plant dispatch log)
Heat detector alarms for Kettle area annunciate (DCS, assumed fireball #1)	11:10:21 AM	
	11:10 AM	◆ "Whooshing" noise heard
	After LEL detectors alarm	◆ Control room operator asked outside operator to visually inspect Kettle # 3 due to high LEL alarm
		◆ Thunderstorm passed and rain diminishing
LEL detectors in Catalyst Prep area alarm (DCS)	11:09:30 AM	◆ Kettle # 3 exit piping cracks (concluded from data)
Plant wide electrical outage (DCS, time of pump shutdowns)	11:05:03 AM	
Kettle #3 high pressure alarm acknowledged (DCS)	11:03:45 AM	
Kettle #3 high-pressure alarm alarms (DCS)	11:03:15 AM	
Kettle #3 level reaches 90% (DCS) but alarm does not log (later found inhibited)	11:00:47 AM	
	11:00 AM	◆ Severe thunderstorm starts
Control room operator initiates filling of Kettle #3 (DCS)	10:30:33 AM	
	10:30 AM	◆ Contractor enters Reactor Area to replace gas detectors

Figure 8.7 Timeline Example Based on a Combination of Precise and Approximate Data

Figure 8.8 presents some tips on timeline development.

TIMELINE TIPS	
•	Use a poster size piece of paper to start your timeline. Use sticky notes for each condition or event item. You can easily rearrange the blocks.
•	Identify precise and imprecise data (different colors are one way).
•	You may also find it useful to list the source on each note (basic process control system, interview, etc.)

Figure 8.8 Timeline Tips

Determining Conditions at the Time of Failure

Conditions are included on the timeline. Determining conditions at the time of the failure is an activity bridging the gap between evidence gathering and root cause determination. Failures rarely occur without some prior indications or precursor information. However, unless someone specifically is charged with looking for it, the information is frequently overlooked in an investigation. Therefore, someone should be assigned the project of timeline development and should update it periodically as new information comes available. A goal of the incident investigation team is to search back in time, find this information, and correlate it with the failure occurrence to confirm or refute a postulated failure hypothesis. This circumstantial evidence may be short-term (that is, immediately preceding the failure), or may be long-term and include anecdotal information from earlier failures or from previous operating experience. It should also include post-incident occurrences that may have affected emergency response, mitigation actions, or secondary damage.

The information that is gathered will be used to accurately determine conditions at the time of the incident and immediately preceding it. Analyzing evidence and determining pre-incident conditions begin as parallel efforts but converge as the investigation progresses.

The incident investigation team should look specifically for evidence that provides the point of initial failure, its progression path, and the pre-existing conditions that led to the initiation. Having an understanding of a fundamental failure mode and the sequence of events, the investigator then seeks evidence that indicates the actual failure mechanism. For example, the incident investigation team could analyze to confirm material properties and

examine the actual failure sites to identify the nature of the failure, such as fatigue, stress corrosion cracking, intergranular stress corrosion, or embrittlement.

The timeline tool pulls all of this information together into a manageable record of events and sequence providing a perspective conducive to proper causal analysis.

8.4.2 Constructing a Sequence Diagram

Organizing Data with Sequence Diagrams

Sequence diagrams are a more elaborate graphical depiction of a timeline that allow the investigator to present related events and conditions in parallel branches. As with a timeline, begin construction of the sequence diagram at the earliest opportunity, as soon as the initial facts become known about the incident. By starting early, the investigation can spot missing information or inconsistencies in the “facts” and focus upon resolving those gaps.

A diagram depicting the sequence of events leading to an incident has a number of advantages over a simple timeline that can be summarized in three main areas: investigation, identifying actions, and reporting as shown below (Ferry, 1988).

Investigation

- Summarizing the events in the form of a diagram provides an aid to developing evidence, identifying causal factors, and identifying gaps in knowledge.
- The multiple causes leading to an incident are clearly illustrated.
- Diagrams enable all involved in the investigation to visualize the sequence of events in time, and the relationships of conditions and events.
 - A good diagram serves to communicate the incident more clearly than pages of text and ensures a more accurate interpretation.

Identifying Actions

- The diagram provides a cause-orientated explanation of the incident.
- Areas of responsibility are clearly defined.

Reporting

- Use of summary diagrams in reports provide a concise, easy-to-follow-representation of the incident for readers.
- Diagrams help to prevent inaccurate conclusions by revealing any gaps in the logical sequence of events.
- Where gaps are shown, the requirement for further analysis/investigation is identified.
- Diagrams provide a means of checking the conclusions as the facts are uncovered.
- Facilitates evaluation of recommendations against the events and causal factors identified in the diagrams.

As an example of sequence diagram, take the case of tank overflow that occurred due to failure of a level safeguard. In this example, the high-level alarm did not function. Tank filling took several hours, and operators did not notice the high level in time to prevent an overflow. The spill was contained in the dike and there were no injuries. However, the tank in the adjoining dike was being cleaned and a crew was working in the dike. Had the wind been blowing toward the maintenance crew, they could have been exposed to toxic vapors. The sequence diagram for this example is shown in Figure 8.9. The investigation team determined that the causal factors were:

- Operators had become accustomed to filling the tank until the high-level alarm sounded rather than actively monitoring the tank level.
- The high-level switch was quite old, well beyond its expected service life, and had never been serviced.
- Maintenance personnel in the adjoining dike were not informed of the tank filling, nor had any provisions been made to closely monitor the tank as it approached the full level.

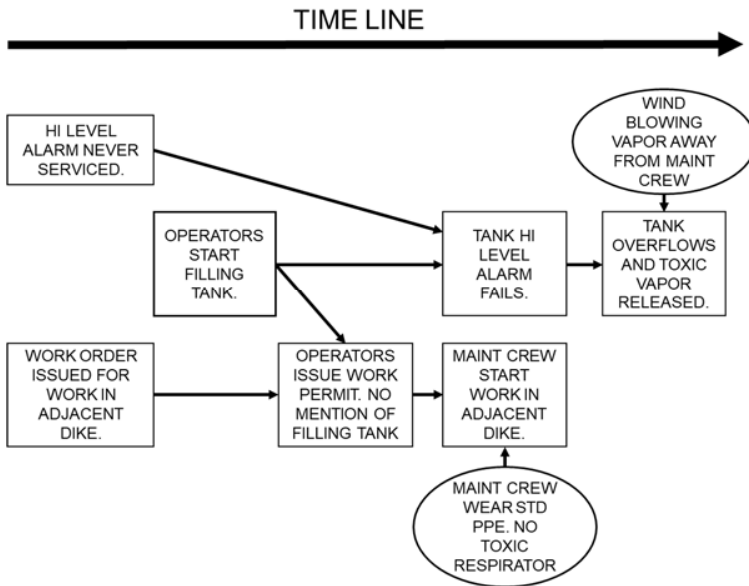


Figure 8.9 Sequence Diagram for Tank Overflow Example

8.5 SUMMARY

Careful, complete and effective evidence gathering is key to a successful investigation. Evidence can be physical (damaged equipment, parts, materials, residues etc.), paper records, electronic data or position data. Consider the fragility of the evidence when determining priorities for the investigation team. Preservation of fragile evidence, such as electronic process data, is a key factor. The team members may have to work several paths simultaneously and the need for additional skill sets should be identified quickly. Agreement between interested parties about how the evidence is handled can be supported using protocols. It is important to establish a system for documenting and securing evidence and a chain of custody is required for items that are moved between locations or different parties. Photography is used extensively to record evidence and can also be an inherent part of the chain of custody process. A set of tools and other equipment should be available for measuring, inspecting, recording and preserving evidence. Timelines and sequence diagrams are effective tools to document events and conditions and identify gaps that require further evidence gathering.

9 EVIDENCE ANALYSIS AND CAUSAL FACTOR DETERMINATION

Once evidence has been gathered, the data can be analyzed. Evidence analysis along with observations, the timeline, witness accounts, and other data are used to determine factually what happened. The factual data is the basis for determining the causal factors, the omission of which would have prevented the incident or reduced the severity of the incident. Causal factors provide the foundation for determining root causes, which is discussed in Chapter 10.

This chapter provides practical guidelines for analyzing evidence and proving/disproving hypotheses (testing hypotheses). Analysis activities may suggest new hypotheses and identify the need for additional data, such as additional evidence collection, witness interviews, DCS trends, etc. As a result, data collection, evidence analysis and hypothesis testing is an iterative and overlapping process.

9.1 SCIENTIFIC METHOD

The Scientific Method is a method of problem-solving in which a problem is first identified, and observations, experiments, or other relevant data are then used to construct or test hypotheses that purport to solve it. More specifically for incident investigations, NFPA 921 defines the Scientific Method as “the systematic pursuit of knowledge involving the recognition and definition of a problem; the collection of data through observation and experimentation; analysis of the data; the formulation, evaluation and testing of hypotheses; and, where possible, the selection of a final hypothesis” (NFPA 921, 2017).

As can be seen from the definition, the Scientific Method provides a systematic analytical process of inquiry into examination of a problem. When applied consistently to an incident investigation, the Scientific Method provides organization as well as objective evaluation of hypotheses to determine what happened.

Figure 9.1 is a diagram of the steps involved in the scientific method as it is applied to a process safety incident investigation. The process begins with defining the problem to be solved; for example, the problem could be

determining the cause of loss of containment that led to a flammable material release and fire.

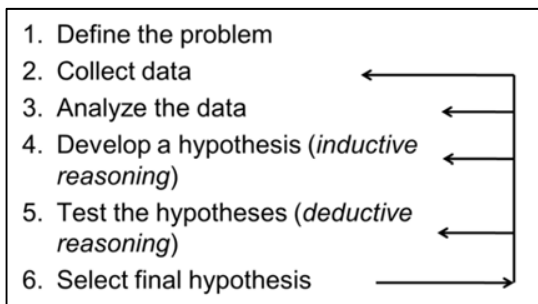


Figure 9.1 Scientific Method Process

Data collection is the second step of the Scientific Method process. This includes examination of the scene, measuring and documenting damage, interviewing witnesses, and data collection activities, as described in Chapters 7 and 8.

The collected data are analyzed in the third step. Analysis refers to all manners of evaluating data, including examination and testing of physical data, engineering calculations, systems testing, simulations, and reconstructions as described in this chapter.

Observations, measurements, data analysis and other information are used to formulate hypotheses in the fourth step. Hypothesis formulation is inductive reasoning. It is important to recognize that inductive reasoning involves postulating a reasonable conclusion from the available data, but the conclusion may not necessarily be true. For example, it may be hypothesized that a pipe burst because the internal pressure exceeded the pipe's pressure capacity. However, it remains to be proven that the pipe failed due to excessive pressure rather than corrosion, a material defect, some other cause, or a combination of factors.

It may appear to be unproductive to postulate hypotheses that may not be true. However, during the course of an investigation, data may not be available to prove or disprove a hypothesis at the time that a hypothesis is postulated. By postulating the hypothesis, investigation activities can be developed to evaluate the hypothesis, such as metallurgical examination of

the failed pipe in the example above, review of DCS data for pressure excursions, and testing of pressure relief devices. It is the process of postulating hypotheses and developing investigation actions that organizes an investigation in a scientific manner.

The fifth and crucial step in the Scientific Method is testing the hypothesis. Hypothesis testing is deductive reasoning in which the conclusion must follow from the premises. Skipping this step can lead to incorrect determination of cause. Incorrect determination of cause can lead to incorrect root causes. In the pipe burst example, it may be true that a facility lacked adequate process pressure control limits, or had pressure relief valve problems, but if the true hypothesis was temperature excursion or vibration fatigue that induced failure, then the resulting recommendations most likely would not prevent a repeat incident. Investigation mistakes can be avoided by testing hypotheses rather than using judgment, past history with the equipment, approximations, and other such methods to draw conclusions about a hypothesis. It is essential to test each hypothesis by a scientifically sound method. All too often, investigator judgments are found to be indefensible when put to the test.

It is noteworthy to emphasize that root cause analysis methods cannot discern if “what happened” has been determined properly or not. In fact, a root cause analysis performed on incorrect immediate causes can lead to recommendations that will not correct the true root causes of an event. It is the hypothesis testing step in the Scientific Method that assures the correct incident hypothesis and associated causal factors have been validated.

Should proposed hypotheses fail the deductive reasoning test, investigators should consider the need for additional hypotheses, data collection, and testing techniques. As shown in Figure 9.1, the Scientific Method is an iterative process, with the process being repeated as many times as needed.

Once all hypotheses have been tested, the most probable hypothesis is selected in the sixth and final step. There can be numerous hypotheses in an investigation, depending on the complexity of the investigation. Most hypotheses will eventually be disproven, but it is often helpful for investigators to be able to explain to stakeholders (and the originator of a given hypothesis) why hypotheses were proven or disproven. Tracking all hypotheses and the supporting data and analyses provides a solid foundation for the investigation team to explain its conclusions and increases confidence in the conclusions.

9.2 CONFIRMATION BIAS

It is human nature to quickly (and automatically) form a hypothesis and then begin to seek confirming evidence. This tendency is called “confirmation bias.” Investigators do not inherently place emphasis on seeking evidence that might disprove what he/she believes. Investigators can become fixated on (and vigorously defend) their favorite hypothesis even when faced with conflicting evidence that might disprove it. Investigators therefore should make a strong and conscientious effort to investigate with an open, unbiased approach, especially during the early phases of an investigation when data may be lacking and testing has not been performed.

The investigation team should also make a conscientious effort to disprove every hypothesis. In the field of critical and logical thinking, there is a concept of falsifiability where a specific effort is made to disprove a hypothesis. This approach can be used to overcome “confirmation bias.” A hypothesis that withstands the attempts to disprove it is demonstrated to be true.

9.3 EVIDENCE ANALYSIS

Evidence analysis is a distinctly separate activity from evidence gathering. The relevance of collected data to incident origin and causes can be determined by analysis. The evidence analysis phase is an iterative activity that overlaps with evidence gathering and can often lead to additional evidence collection. Evidence analysis is conducted over a typically longer timeframe and, on a major investigation, can last for several months as additional tests and data generation are done. Evidence analysis activities often identify the need for additional, specific information, and the evidence gathering cycle begins again.

During evidence analysis, evidence can be compared to determine if one piece of evidence corroborates another piece of evidence or not. Corroboration of evidence adds confidence to the findings. Conversely, if no corroboration can be found for an item of evidence, it may not be given the same weight by the investigation as a well-corroborated item.

Evidence analysis is performed using a systematic and thorough approach. Specific techniques for evidence analysis are beyond the scope of this guidebook. This section is intended to provide an overview and general understanding of some of the common concepts and issues associated with

evidence analysis. Discipline-specific expertise is normally supplied to the incident investigation team via the use of specialists from either the parent organization or from outside experts engaged for the exact analytical task at hand.

9.3.1 Data Organization - Timelines

The first step in evidence analysis is to organize the collected data. A timeline is an excellent tool for laying out what data has been collected and representing that data chronologically in sequence with the incident development. A detailed description and case study example of timeline development can be found in Chapter 8. The following section shows how witness accounts and evidence analysis factor into a timeline.

Timelines should record all known events relevant to the incident investigation. The timeline is factual in that it includes events substantiated by data. The timeline does not include hypothesized events. If the incident involves a piece of equipment or process vessel, then the timeline might start with records of the history of the vessel such as installation, maintenance, repairs, and inspections. The timeline should be based upon the reported time stamp as given by the data source. For example, if a witness states a specific time for the reported observance, then the timeline should record what the witness stated. A good way to verify a witness's time reference is to ask the person to check cell phone text or phone call time stamps made near the time of the observance. All DCS events should be entered as occurring at the time recorded by the DCS system. A secondary analytical step can permit the shifting of events to match known discrepancies such as computer clock time offset, adjustment of operator recollection of alarms and shutdowns to match valve movements as recorded by the DCS, etc. Shifting reported occurrences is not the same as documenting the verbatim reports and therefore that exercise is considered an analysis. Both types of documents should be clearly identified and kept separate.

9.3.2 Use of Protocols

Protocols are written procedures for evidence inspection, examination, removal, alteration, and testing. Protocols can help ensure that an investigation activity concerning an evidence item is performed in a carefully planned manner, ensuring preservation of the evidence to the maximum extent possible while achieving the scientific purpose of the activity. The planning that goes into developing a protocol can avoid unintended alteration of evidence. For example, once a cover on a piece of equipment

is opened to see what is inside, the cover cannot be replaced in exactly the same manner it was originally. The oxidation layers and adhesives used to seal the cover cannot be replaced exactly as they were. Once a pump is hand rotated, it cannot be disassembled to see the position in which it came to rest following the failure. Consequently, investigators must be careful to think about the data that is needed and what data could be altered or destroyed when certain actions are taken. Protocols are intended to help investigators think ahead. Protocols also serve to gain agreement from multiple parties on how, by whom, and when the test should be performed.

Typically, protocols are designed to answer one or more of the following questions:

- How does the part work?
- Did the part function as intended?
- How did the part fail?
- Why did the failure occur?

Protocols should be developed before the analysis of physical data is started. Protocols help:

- Ensure complete collection of required data
- Ensure complete analysis of the data
- Prevent inadvertent destruction of data by the investigators
- Gain agreement from all parties involved in the investigation concerning the analysis processes and methods
- Ensure the test is worth doing before it is done
- Identify decision points in the analysis

The protocol should include:

- The objective of the investigation activity
- The methods for performing the activity
- Safety considerations for executing the protocol
- A description of the methods/procedure
- Names of the persons who will perform the tasks in the protocol
- Scheduled times and locations of the protocol
- How the protocol results will be recorded and reported
- Information on multiple tests of the same item
- Disposition of the test specimens after the protocol
- The order in which the different steps of the protocol will be executed

- Which organizations, both internal and external, will approve the protocol

Protocols are not intended to be long, complex documents. They should be concise documents that lay out the inspection, examination, documentation, and/or test processes in sufficient detail to allow all involved parties to understand what will be done to the evidence. Protocols often include an allowance for deviations from the protocol based on developments during the course of conducting the protocol with mutual agreement of the parties attending the protocol. Appendix B provides an example of a protocol to check the as-found position of a manually operated valve.

9.3.3 Mechanical Failure Analysis

Many documents have been written on specific issues such as the fracture patterns of alloys and the corresponding clues for determining the actual failure mechanisms. To illustrate the process that may be followed in examining an equipment component failure, analysis of a mechanical part is used as an example. The basic steps in failure analysis include the five steps shown in Figure 9.2.

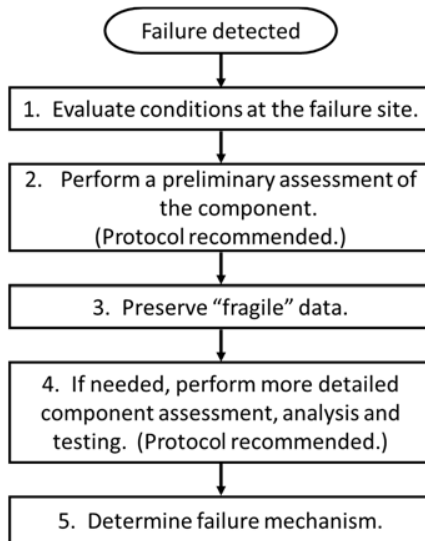


Figure 9.2 Basic Steps in Failure Analysis

9.3.3.1 *Evaluate Conditions at the Site - Step 1*

Evaluating conditions at the failure site can be a critical important step in the analysis. Understanding the conditions at the site and how the parts or items were used can eliminate some potential failure mechanisms from consideration and support other failure mechanisms. Typical questions to ask include, but are not limited to:

- How long had the part been in service?
- What were the environmental conditions?
- Did the failure occur during startup, shutdown, abnormal, or normal operation?
- Was it a rotating piece of equipment?
- Did it rub against something?
- Was there any fluid or gas flow past the device?
- What are the chemicals to which the part is exposed?
- What are the materials of construction?
- What activities were taking place in the area?
- Does any portion of the process utilize reactive chemistry?
- Is there a potential for reactive interactions (caused by inadvertent mixing of incompatible materials) at the site? If so, what are the materials?
- Is remaining, relevant equipment properly installed (alignment, rotation, etc.)?
- Is any equipment used for more than one service? Does it require cleaning before reuse?

Investigators can supplement/edit this list based on the particular circumstances associated with the incident they are investigating. The answers to these questions should allow the investigators to focus their subsequent data collection efforts.

9.3.3.2 *Perform a Preliminary Component Assessment - Step 2*

During Step 2, a preliminary analysis of the parts is performed. Typically, the focus is a visual examination of the items. The investigators should avoid disturbing evidence until necessary, conducting their visual examination without alterations.

When it is time to do so, remove the parts in a planned, controlled, careful, and methodical manner. Photograph each step of the disassembly.

Evaluate the importance of coatings, residues, deposits, and impurities before disturbing the item. Samples of the chemicals, soil, deposits, and coatings may be taken at this point.

9.3.3.3 *Preserve Fragile Data Sources - Step 3*

Provide a safe, secure, and controlled storage location for the physical data as described in Chapter 8. Consider special storage features that might be needed such as temperature control, humidity control, wrapping, and others. Prepare the parts for further evaluation and avoid actions that may destroy, alter, or degrade data.

9.3.3.4 *Perform a More Detailed Assessment of the Component (as Necessary) - Step 4*

Perform a more detailed analysis of the items. This stage may include field-testing, field disassembly, and shop disassembly. Additional pictures of the component should be taken, especially during testing and disassembly activities. All of these activities should be performed in a careful and controlled manner using a test-specific protocol.

Detailed assessment techniques for failed mechanical components may include, but are not limited to:

- Examination of the fragmentation, deformation, and tear patterns
 - Dimensional measurements
 - Fractography
 - Microscopic visual examination
 - Scanning Electron Microscope (SEM)
 - Transmission Electron Microscope (TEM)
- Identification of cracks
 - Dye penetrant
 - Magnetic particle
 - Ultrasonic testing
 - Acoustic Emission inspection
- Interpretation of burn, char, calcination patterns, and temperature zones at the failed component
- Characterization of mechanical damage (e.g., estimation of overpressure blast zones, Finite Element analysis of loading required to produce observed effects, etc.).
- Characterization of electrical conductor faults
- Chemical composition analysis, tensile strength, hardness testing

- Other analyses specific to the components, materials, operating conditions, and potential modes of failure

9.3.3.5 *Make a Failure Mechanism Determination - Step 5*

This step is always performed. The combined information gathered from the above analyses, testing, and simulations are used to determine the failure mechanism. The mode of failure of a component can provide valuable insight into understanding what occurred during the incident.

9.3.4 **Advanced Data Systems**

Technology advances in electronics such as process control systems, safety instrumented systems, programmable logic controllers, the use of independent personal computers at field locations, and other computer capabilities present new challenges to incident investigation. Some of the advances are so rapid that the team may not have the internal expertise to determine failure hypotheses, sequences, and modes. The suppliers and manufacturers of these high-tech devices or other specialists are sometimes the only sources of credible information on failure modes and related analysis techniques for these devices.

Reliance on outside expertise may be the most feasible option for some of these issues at some locations. The incident investigation team may act as facilitators and advisors. The outside expert would supply information on which failures are credible, suggested applicable physical examinations and field performance tests, orchestrate such testing, etc. If available, an independent outside expert not associated with the supplier or manufacturer of the equipment under examination can reduce perception of bias.

9.4 **HYPOTHESIS FORMULATION**

Hypothesis formulation is the process of using inductive reasoning based on observations, measurements, empirical data, and other information to develop a hypothesis to describe what happened and how it happened. Multiple hypotheses are postulated as described in Section 9.1. The section below describes techniques to summarize the incident development, identify pertinent facts, document information, and organize the information and hypotheses. The suggested techniques are often used in conjunction with other tools such as sequence diagrams, fault/event trees, cause and effect diagrams, etc.

9.4.1 *Fact/Hypothesis Matrix*

The fact/hypothesis matrix is a tool available to the incident investigation team. This tool is used to compare the known facts against the various hypotheses. One side of the matrix lists each hypothesis, and the other side (usually across the top) lists the known facts, conditions, and stipulations. Each intersecting box is then examined for compatibility, known truthfulness (yes, no, or unknown), and its logical fit into the particular hypothesis. The matrix makes it easier to determine the most likely hypothesis and to refute other hypotheses based on the available facts. Use of a matrix can help the team avoid jumping to conclusions and selecting a most likely hypothesis too early. The fact/hypothesis matrix can be used in the inductive stage to help organize hypotheses and postulate new hypotheses, and in the deductive stage to test hypotheses against facts.

Hypotheses for many process safety incidents can be rather complex. The fact/hypothesis matrix technique has proven to be useful in sorting, analyzing, and comparing information. Depending on the nature of the incident, the degree of complexity of this matrix can vary, from a simple [YES/NO/?] to a variety of categories and sub-categories. A more complex set of matrix conditions might take the following form:

- + The fact is consistent with the hypothesis
- The fact is contradictory to the hypothesis
- NA This fact apparently has no relation to this hypothesis, it is neither consistent with nor contradicts the hypothesis
- ? There is not enough information currently available to decide on this fact

A sample appears in Table 9.1 for a hypothetical incident. Developing the matrix is not a one-time exercise; the matrix is usually revised numerous times during the course of the investigation. Gradually, some hypotheses will emerge as more likely and others will become less probable or be disproved. It is very helpful to others to keep unlikely and disproven hypotheses on the matrix and document why the hypothesis was so classified. Seeing that a comprehensive set of hypotheses was evaluated and why hypotheses were proved or disproved increases transparency and can help people more readily accept the team's conclusions.

Case Study - Application of Fact/Hypothesis Matrix

Example case: Explosion and fire in a chemical reduction unit

Background: A tank exploded at 1:30 A.M., 3 hours after a batch product transfer was made. Maintenance had recently replaced a gasket on the transfer pump. There was a power outage shortly before the incident.

Status: The investigation is currently incomplete, being only in the second day of activity. The team has accumulated some evidence and has begun to compare known facts against possible hypotheses. The matrix in Table 9.1 is the result of initial deliberations and is being used to develop action items and priorities, such as which direction the information gathering and cause analysis should proceed.

Table 9.1 Example Fact/Hypothesis Matrix – Chemical Reduction Explosion

Hypothesis	Fact or Condition					
	Power Tripped Out at 4:09 PM	Operator Added Chemical "A" to Batch at 10:30 PM	Storage Tank Transfer on Evening Shift 7:30 PM	Maintenance Changed Gasket P120B	Top of Tank Found on East Side of Warehouse	Lab Analysis Showed Zero Water in Residue
Contaminated Batch of Incoming Raw Materials	?	+	?	+	+	-
New SOP Not Followed	?	?	+	+	+	?
Wrong Gasket Designed or Installed	N/A	N/A	+	+	-	N/A
Oxygen Entered Nitrogen Header from Back Flow-Preventer Device Failure	?	+	?	NA	+	-
Oxygen Entered the System during Maintenance	N/A	?	?	+	+	-

Legend: (+) – the fact supports the hypothesis; (-) – the fact refutes or is inconsistent with the hypothesis; (NA) – this fact apparently is not related to this hypothesis, neither supports or refutes; (?) – not enough information is currently available to decide on this fact.

9.5 HYPOTHESIS TESTING

The following discussions are intended as an introduction to some special techniques used by experts for technical analysis of evidence and hypothesis validation. Novice investigators and individuals who are not experts in these fields should be cautious when applying these tools. For most minor investigations, review and application of the information in this section is adequate for the investigation team to analyze the data. However, if legal concerns arise during an investigation, experts in the forensic analysis of data should be used to ensure a proper analysis has been performed and correct interpretation of the data has occurred.

9.5.1 *Engineering Analysis*

In addition to physical analytical methods, engineering analysis tools and methods are also useful during incident investigations. Engineering analysis refers to calculations that can be performed to investigate and test various hypotheses. Examples of engineering analyses include:

- Forces
- Stresses
- Fluid motion and pressure
- Heat transfer/temperature
- Thermodynamics/energy transfer
- Mass transfer and balance
- Mass of process fluids and process equipment
- Concentration of fluid in process equipment
- Flow rates of fluids through process equipment and through release points
- Change in levels of tanks over time
- Rates of chemical reactions
- Dispersion of a gas

Investigators use engineering analysis methods to test the various hypotheses that are put forth during the investigation. Often rough calculations may be all that is needed to determine if a hypothesis is possible. For example, even if the entire contents of a tank are released, the volume may not be sufficient to cause an overflow in another part of the process. A simple calculation may be sufficient to eliminate certain hypotheses that have been proposed.

9.5.2 Computational Modeling

Numerical models may be used to evaluate hypotheses in a variety of problems. Numerical modeling refers to computer modeling that involves time-stepping to simulate the behavior of a system. Types of numerical models that may be used in an incident investigation include:

- Finite element analysis (FEA) – calculation of stresses, motion, deformation and other properties of mechanical or structural components subjected to forces during an incident.
- Computational fluid dynamics (CFD) – analysis of fluid flow, including the thermodynamic conditions of the fluids
- Fire and explosion CFD – these models incorporate combustion and explosion simulations.
- Process simulation – process conditions are calculated using models of process equipment such as distillation towers, heat exchangers, etc. The simulation can be steady state or dynamic (time varying).

Numerical models have become quite sophisticated. A qualified analyst is needed to properly use numerical models. There are many non-physical parameters in numerical models such as time step and mesh (grid) size that can change the results of a simulation. The numerical model selected for the simulations should be suitable for the type of event and the range of input parameters associated with the event. Numerical models should be used with caution if the numerical model has not been validated for the input conditions.

Numerical models are not first-principles models. Many numerical models contain approximations, tuning coefficients, and numerical methods so that the models run in a stable fashion and produce reasonable results. While numerical models can provide valuable insights into the behavior of a system during an incident, the results must be reviewed carefully to ensure that they are reasonable. Comparison to empirical data and first principles calculations can be useful to check the numerical model.

9.5.3 Reconstruction

In some major investigations, reconstruction of a piece of equipment or system may be required to understand failure patterns, the physical relationships between the various items that are recovered, the functionality of equipment, and equipment behavior under certain conditions. A dedicated area or warehouse space may be required to effectively

reconstruct and analyze the physical data. Reconstruction can be as simple as placing the pieces of failed components in the proper position relative to each other, such as the mating halves of a broken bolt, or as complex as reassembling and operating a system, such as a burner system.

A reconstruction should be carefully planned as evidence may be altered as a result of the reassembly and operation. Non-destructive examination, component testing, modeling and other analyses are often performed before reconstruction is considered if evidence alteration is likely during reconstruction.

9.5.4 Test the Items under Simulated Conditions

In this step, experiments may be performed such as operational tests, mixing experiments, combustion experiments and other types of experiments. Simulations can be performed with similar parts or samples in an attempt to recreate the situation at the time of the failure. Pilot runs of the process or system may also be performed.

Information gained from simulations can reveal key insights that explain gaps or contradictions in information. For incidents of unexpected chemical reactions, a lab scale simulation of the conditions involved in an exothermic reaction or explosion may be attempted, if it can be done safely. Adiabatic calorimeters have proven to be highly useful tools for studying exothermic or gas-generating runaway reactions.

Two important concepts should be kept in mind when considering the use of simulations. First, the top priority is the prevention of a second injury or incident, which could result from the simulation. This classic error happens with surprising frequency. Second, these simulations only mimic and do not exactly duplicate the occurrence. The information obtained can be useful, but it is narrow in scope and by nature is obtained under ideal and known conditions. Investigators should be mindful of these limitations and should use discretion when evaluating the data from these sources.

9.5.5 Testing of Human Input/Performance

Investigations involving complex human performance problems can benefit from simulations. Process simulators are often used for operator training. In some cases, these process simulators can be excellent tools for learning .more about human error causation. The incident investigation team can expose operators to simulated process upsets and gain valuable insights into

the operator's response to rapidly and accurately diagnose the problem and execute the proper action.

9.6 SELECT THE FINAL HYPOTHESIS

The culmination of the evidence analysis, hypothesis development, and hypothesis testing is selecting the final hypothesis. The final hypothesis often becomes self-evident if a rigorous, systematic and scientific process is followed. Hypotheses that do not stand the test of hypothesis testing are disproved. The hypothesis that cannot be disproved is the final hypothesis.

In technically complex investigations, there may be aspects of a hypothesis that are found to be true while other aspects are disproved. In such cases, the hypothesis is disproved. However, a new hypothesis can be developed that incorporates aspects that are known to be true. For example, for a pressure vessel that fails, a hypothesis could be failure at working pressure due to corrosion. DCS data may prove that the vessel failed at working pressure, but metallurgical analysis disproves that corrosion was the cause. Instead, metallurgical analysis found a flaw in a weld repair that caused crack initiation at working pressure. The corrosion hypothesis was disproved and a new hypothesis for failure at working pressure due to the flawed weld repair was developed.

As mentioned above, hypothesis formulation and testing are an iterative process. The process is repeated until the investigation team has exhausted all hypotheses that are consistent with observable, measureable, empirical and other information.

9.6.1 Causal Factor Identification

Once the evidence has been collected, a timeline or sequence diagram developed, and the actual hypothesis confirmed, the investigation can proceed to the next stage – identifying causal factors. Causal factors are the negative events and actions that made a major contribution to the incident. Root cause methods that based on pre-defined trees use causal factors to identify root causes (logic trees do not require causal factors).

Causal factors involve human errors and equipment failures that led to the incident, but they can also be undesirable conditions and failed barriers (layers of protection, such as process controls or operating procedures).

In practice, the initial stages of the investigation are steps in an iterative process with a significant degree of overlap. For example, the events and conditions on a preliminary timeline or sequence diagram may be revised many times as new facts about the failure mode and sequence of events emerge, and the investigator seeks evidence that confirms the actual incident hypothesis. Sometimes it may be necessary to progress the investigation along more than one hypothesis until the team completes all analyses and can confidently select the final hypothesis. Because of this iterative process, the investigator's initial perspective of potential causal factors may change, and it is important to remain objective and not jump to conclusions too early. For this reason, all the evidence should be collected and analyzed to determine a single incident hypothesis before commencing causal factor identification.

Causal factor identification is relatively easy to learn and apply to simple incidents. For more complex incidents with complicated timelines, one or more causal factors can easily be overlooked, which inevitably will result in failure to identify their root causes. There are a number of tools, such as Barrier Analysis, Change Analysis, and Fault Tree Analysis, that can assist with bridging gaps in data and the identification of causal factors. Each of these tools has merits that can assist the investigator in understanding *what happened* and *how it happened*.

9.6.1.1 Quality Assurance

There are a number of quality assurance checks that should be considered *before* identifying the final list of causal factors. It is important to test for *sufficiency* of the information when compiling a timeline or sequence diagram. In this respect, sufficiency means that the causal factors fully address the pertinent negative events and undesirable conditions. For example, in the case of a fire have all three elements (fuel, oxygen, ignition) of the fire triangle been considered? This test for sufficiency may be performed by asking one or more of the following questions, when comparing two adjoining facts in the sequence of events:

- Will (*insert the complete statement of Fact B here*) always lead to (*insert the complete statement of Fact A here*)?
- Every time Fact B occurs, does Fact A have to follow?
- Just because Fact B occurs, will Fact A always follow?
- Are there any layers of protection that should have prevented Fact B from progressing to Fact A?

- Does anything else have to occur or does any other condition have to be satisfied for Fact B to lead to Fact A?
- Are there any other potential causes of Fact A other than Fact B?

The use of this sufficiency test is described in Figure 9.3. In the case of the fire example, the investigation team should consider all potential causes as there may be multiple sources of fuel (chemical vapors, combustible solids/dust, natural gas, etc.), oxygen (air, oxidizing agent, pure oxygen, etc.) and ignition (hot work, static, faulty electrical equipment, pyrophoric material, etc.). The facts in the timeline should fully and adequately address the questions above, i.e., validate what events were necessary and sufficient to have caused the next event(s) in the timeline.

Once the timeline or sequence diagram has been compiled, a test for *completeness* should be performed by reviewing the entire chronology for any omissions or gaps. The investigation should then focus on gathering evidence on any identified gaps and adding new data to the sequence diagram. Barrier analysis and change analysis may be used in addition to brainstorming to assist this test. Any new data added to the diagram should be subjected to the sufficiency test above.

The entire timeline or sequence diagram should also be reviewed to identify any conflicting facts. The aim should be to determine a single hypothesis of events that caused the incident, although on occasion it may not be possible to distinguish between potential hypotheses. The fact/hypothesis matrix approach should be used to resolve any conflicting facts and determine the most likely hypothesis. It may not be necessary to tabulate the data in a matrix, but the same logic should be applied in comparing all of the information.

9.6.1.2 Causal Factor Summary

The identification of causal factors points investigators to the key areas to be examined further to better understand why that factor existed. It acts as a filter to limit the number of areas that are subjected to further analysis to determine root causes. This critical activity should be performed diligently and systematically to identify every causal factor applicable to the specific incident. If a causal factor is missed, one or more root causes will likely be omitted as well, which could lead to similar incidents in the future. Some investigators review each of the causal factors to determine any unsafe acts

or unsafe conditions of the incident, as an intermediate step before proceeding to determining the root causes.

9.6.1.3 Identifying Causal Factors

The simplest technique for identifying causal factors involves reviewing each event or condition on the timeline. The investigator repeatedly asks the following question:

Would the result have been significantly different if the event or condition had not existed at the time of the incident?

If the answer is YES, that is, the incident would have been prevented or mitigated by the elimination of a negative event or undesirable condition, then the fact is a causal factor. Generally, process safety incidents involve multiple causal factors. This technique is equivalent to step #15 in Figure 9.3. Once identified, the causal factors become the candidates to undergo root cause analysis.

The investigator may streamline this technique by focusing upon each unplanned, unintended, and/or adverse fact (negative event or undesirable condition) on the timeline. It is also important to recognize those items that are still speculative and based on an assumption, as these should be tested later to verify if they are accurate facts.

It is critically important that the wording or the phrasing of each causal factor accurately and clearly describes the factor. Teams will struggle with cause analysis if the causal factor is not crystal clear to all. In the case of an incident arising from work on a pump that has not been adequately isolated from energy sources, an investigation team may say one causal factor is “no lockout/tagout (LO/TO)”. However, this short statement can be interpreted in a number of ways, depending upon individual team members’ views of the evidence and personal biases.

For example, “no lockout/tagout” can mean:

- No procedures for LO/TO exist
- Procedures exist but the employees involved had no knowledge of them
- An attempt was made to perform LO/TO, but it was performed incorrectly
- LO/TO was performed on the wrong equipment or missed on one item
- No effort was made to perform LO/TO.

When different team members approach an issue from different directions, it is not unusual to see prolonged and circuitous causation discussions. It is better to resolve what the team believes the evidential issue is before starting the root cause analysis.

In the same example, if the team has the evidence to support that there were adequate procedures, training and equipment in place, and the failure involved a technician circumventing the rules, the causal factor should be worded along the lines of “Technician failed to install the required locks and tags on the pump.” This provides little room for differing interpretations.

If the team is not settled on what the evidence tells them, it is indicative that more investigating needs to be done—cause analysis is premature at this point.

The following tools can assist with the identification of causal factors for complex incidents with complicated timelines.

9.6.1.4 Barrier Analysis

The design of most process plants relies on redundant safety features or layers of protection, such that multiple layers must fail before a serious incident occurs. Barrier analysis (Trost, 1985) (also called Hazard–Barrier–Target Analysis, HBTA) can assist the identification of causal factors by identifying which safety feature(s) failed to function as desired and allowed the sequence of events to occur. These safety features or barriers are anything that is used to protect a system or person from a hazard including both physical and administrative layers of protection. The concepts of the hazard–barrier–target theory of incident causation are encompassed in this tool.

The term *barrier* encompasses a wide range of safeguards and preventative measures. Some examples of barriers are:

Physical

- Closed Valve
- Blast/firewall
- Electrical insulation
- PPE

Natural

- Distance
- Time
- Laws of Nature

Administrative

- Standard Operating Procedure (SOP)
- Pre-Startup Checklists
- Lockout/Tagout Procedure
- Design Standard

Human Action

- Supervision
- Manually Controlling Process
- Monitoring Process Parameters
- Taking Process Samples

Active

- Process Control
- Interlocks
- Safety Instrumented Systems
- Mitigation Systems

Barrier Analysis may be performed by asking a series of questions while studying the timeline or sequence diagram. Typical questions are:

- What physical, natural, human action, and administrative controls are in place as barriers to prevent the incident?
- Where in the sequence of events would these barriers prevent the incident?
- Which barriers failed to work?
- Which barriers worked successfully?
- What other physical, natural, human action and administrative controls might have prevented the incident if they had been in place?

The tool helps the investigator to understand and focus on the failed barriers, which are normally identified as causal factors. To be effective, the failed barriers should be strengthened, replaced, or supplemented, especially where weak administrative controls are highlighted. Even successful barriers that prevented more serious consequences may require reinforcement. Therefore, barrier analysis can give the investigator valuable insights into how the incident happened and some of the multiple causes that need corrective action to prevent recurrence.

9.6.2 Causal Factor Charting

Events & Causal Factor Charting (E&CF) (Buys, 1978; Johnson, 1980) was adopted by the developers of MORT (Buys, 1977) to identify and document the sequence of events leading to an incident. A number of proprietary process safety incident investigation methodologies include E&CF as one of their building blocks.

The causal factor charting method of developing chronological data in graphical format is an excellent tool for organizing process safety incident evidence. The graphical representation of the incident sequence assists the investigator in organizing all the data and understanding the incident. The investigator is then better able to effectively communicate that

understanding to others. This is especially important with complex process incidents, although the diagrams can become rather complex.

The technique for developing causal factor charts shares a number of fundamental principles with MES and STEP. Basic principles for constructing sequence diagrams (Benner, 2000; Hendrick, 1987) are given below.

Chart Format

- All events are enclosed in rectangles, and conditions are enclosed in ovals.
- All events are connected by solid arrows.
- All conditions are connected to other conditions and/or events by dashed arrows.
- Each event or condition should be based upon valid evidence or, if presumptive, shown by dotted rectangles or ovals.
- The primary sequence of events is depicted in a straight horizontal line (bold arrows are suggested).
- Secondary event sequences are presented at different levels.
- Relative time sequence is from left to right.

Criteria for Events Description

- Events should describe an action, not a condition.
- Events should be described with one noun or verb.
- Occurrences should be precisely described.
- Events should describe one discrete action.
- Events should be quantified when possible.
- Events should range from beginning to end of the accident sequence.
- Each event should be derived from the one preceding it.

These principles are not mandatory. The most important aspect is that the investigator understands the incident, and these principles are meant to facilitate that objective. Some investigators draw causal factor charts differently; for example, some investigators do not distinguish between events and conditions. It is permissible to deviate from the above principles

provided the method helps the investigator and others understand the incident.

9.6.3 Developing a Causal Factor Chart

The first step in developing a causal factor chart is to define the end of the incident sequence. Construction of the chart should start early from the end point and work backward to reconstruct what happened before the incident by identifying the most immediate contributing events.

Starting at the end point, it is then necessary to convert the collected evidence into statements of either fact or supposition. By taking a small step backward in time, the investigator asks, *“What happened just before this event?”* It is important to clearly distinguish any assumptions as supposition. Then the investigator writes a statement for what happened and enters the fact (or supposition) as an event block or condition oval on the causal factor chart at the appropriate location on the timeline. Statements that caused an event to occur should be treated like conditions and added in an oval.

The investigator tests this new event (or condition) for sufficiency by asking, for example, questions such as:

“Does this block always lead to the next block (in this case, the endpoint)?”

“Are there any layers of protection that should have prevented this sequence?”

The process is repeated slowly working backward in time.

The entire causal factor chart is then reviewed to identify any omissions or gaps in the chronology. Additional effort is required to gather further evidence to close these gaps. If new data are inserted into the timeline, the sequence should be retested for sufficiency. Some gaps may remain even after this additional effort. The causal factor chart review should also identify and eliminate any facts that are not necessary to describe the incident. Detailed rules for causal factor charting are shown in Figure 9.3.

Charting the events and conditions on a causal factor chart assists the investigator in thinking logically through the incident. However, the investigator must exercise care to avoid locking into a preconceived hypothesis. It is important to keep an open mind and objectively analyze all possible hypotheses for the events and conditions leading up to the incident. Initial assumptions can change dramatically during the course of an

investigation. Note that it is sometimes helpful to reconstruct what immediate actions occurred after the incident.

Rules for Causal Factor Charting

1. Start at the end of the sequence (at the incident or the near-miss statement) and work backward in time.
2. List all outcomes, if there are multiple impacts/outcomes of the sequence of events.
3. Generate any questions necessary to quantify the outcomes.
4. Use whole sentences and quantify each statement as much as possible (merely stating that the "pump is destroyed" is not sufficient; include a quantification of the damage to the pump).
5. Take a very small step backward in time by asking "What happened just before this event?" The answer may be a phenomenological occurrence or condition, or it may have been an action by a human or machine. If there are multiple choices for the size of the step backward, take the smallest step proposed.
6. Write a complete sentence for what happened and add the event to the chart.
7. Test for sufficiency of information by asking one or more of the following questions:
 - a. Will (insert the complete statement of Fact B here) always lead to (insert the complete statement of Fact A here)?
 - b. Every time Fact B occurs, does Fact A have to follow?
 - c. Just because Fact B occurs, will Fact A always follow?
 - d. Are there any layers of protection that should have prevented Fact B from progressing to Fact A?
 - e. Does anything else have to occur or does any other condition have to be satisfied for Fact B to lead to Fact A?
 - f. Are there any other potential causes of A other than B?

FACT B → FACT A
8. If the answer to either question 7a, 7b, 7c, or 7d is NO, or if the answer to question 7e is YES, then brainstorm what else would have to occur or what other conditions would have to be satisfied for Fact B to lead to Fact A. Generate the questions or list the data needed to answer the hypothetical questions/concerns.
9. Gather data to answer the questions or address the data needs identified in step 8.
10. If any of these facts are relevant, convert them into building block format and insert them into the Causal Factor Chart at the appropriate location on the time line. If any facts are inserted between Fact B and A, then retest each pair of facts for sufficiency as stated in steps 7 and 8, and repeat steps 9 and 10 as necessary.
11. Continue to gather data to answers the questions/needs developed above. Remove the questions from the chart as they are answered.
12. From Fact B, repeat steps 5 through 11 until all data are exhausted (changing the reference to Fact C, Fact D, etc. as necessary, of course).
13. Keep all remaining questions on the chart to demonstrate what is known and not known.
14. Review the entire Causal Factor Chart and eliminate any facts that are not necessary to describe the incident.
15. Find the facts in the main sequence on the Causal Factor Chart that describe a component failure or a human error. Ensure the fact is not describing a management system failure (i.e., ensure the fact is not a root cause, near root cause, or root cause category). The identified negative events/conditions are candidate causal factors. Any candidate causal factor that is not dependent on another candidate causal factor is a valid causal factor.

Figure 9.3 Rules for Causal Factor Charting

An example of a causal factor chart for a relatively simple incident is shown in Figure 9.4. In this example, there are two redundant pumps, one of which is required to supply feed to a reactor downstream. The operator is requested to change-over operation from Pump A, which is running, to Pump B, which was previously shut down. Instead of opening Pump B suction valve, the operator opens the wrong valve, causing the reactor to trip on low flow detection.

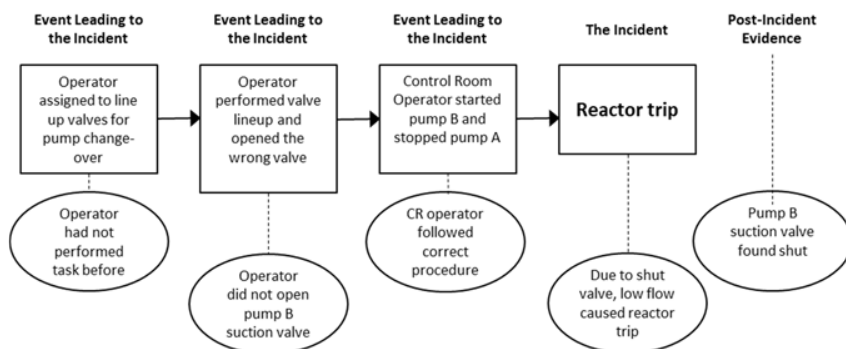


Figure 9.4 Example of a Causal Factor Chart

9.7 SUMMARY

Evidence analysis is an important stage in an investigation during which factual data are used to develop and test hypotheses, which leads to determining causal factors. Evidence analysis can include physical examination, measurements, component testing, simulations, and other means of extracting key information. The scientific method is used to test hypotheses against factual data, engineering analyses, laboratory analyses and simulations to determine whether the facts of this event are consistent with the required conditions. Evidence collection, hypothesis generation and hypothesis testing are often iterative. The hypothesis that cannot be disproven is the final hypothesis. Once there is an accurate understanding of what happened, it is possible to determine the causal factors and identify the root cause. Root cause determination is discussed next in Chapter 10.

10 DETERMINING ROOT CAUSES— STRUCTURED APPROACHES

Previous chapters discuss the essential steps (and associated tools) required for the investigation team to progress their investigation to the stage that the root cause analysis may be successfully implemented. In particular, the team should have completed their evidence gathering and analysis, determined a single hypothesis (scenario) that the evidence supports, and developed a timeline of events/conditions leading up to the incident.

In addition, depending upon the root cause analysis methodology chosen, the investigation team may also need to identify the “top event” and/or causal factors before commencing the root cause analysis. Chapter 3 introduces some of the root cause analysis methodologies. Methodologies, such as the 5 Whys and Logic Tree, require the team to select the top event before proceeding, and this is discussed in Section 10.5.1. Other methodologies, such as Predefined Tree and Checklist, require the team to select the causal factors before proceeding, and this is discussed in Chapter 9 Section 9.6.1.

Commencing the root cause analysis prior to completion of these steps will almost certainly result in an ineffective investigation.

10.1 CONCEPT OF ROOT CAUSE ANALYSIS

Organizations may use different nomenclature to describe their categorization of causes of incidents. Process safety incidents are invariably the result of multiple causes, which can usually be categorized into two types:

1. Causal factors
2. Root causes

The terminology and definitions used in this book are as follows:

Causal Factor—*A major unplanned, unintended contributor to an incident (a negative event or undesirable condition), that if eliminated would have either prevented the occurrence of the incident, or reduced its severity or frequency.*

Root Cause—*A fundamental, underlying, system-related reason why an incident occurred that identifies a correctable failure(s) in management systems. There is typically more than one root cause for every process safety incident.*

Correcting only a causal factor is a simplistic approach that may prevent the identical incident from occurring again at the same location, but will not prevent similar incidents. Identifying and correcting the root causes should eliminate or substantially reduce the likelihood of recurrence of the incident and other similar incidents at the location. More importantly, the new knowledge and corrective methods resulting from the investigation may be shared for use throughout a company and possibly apply to an industry as a whole.

... It is from identifying the underlying causes that the most benefit is gained. By addressing only the causal factor, the identical accident is prevented from occurring again; by addressing the underlying root cause(s), numerous other similar incidents are prevented from occurring. . .

A thorough incident investigation identifies and addresses all of the causes of an incident, including the root causes. It also provides the mechanism for understanding the interaction and impact of management system failures. This analysis provides the means for fully addressing the incident, similar incidents, and even dissimilar incidents caused by the same root causes, throughout the facility, company, and industry. Addressing management system failures is the ultimate goal, yielding the maximum benefit from an incident investigation.

The following example illustrates the concept of root cause analysis. Consider a scenario where a worker steps into a puddle of oil on the plant floor, slips, and falls. A traditional investigation might identify “oil spilled on the floor” as the cause, with the remedy limited to cleaning up this particular spill and possibly admonishing the worker for not being more careful. By using the tools described in this chapter, it will be clear that the oil on the floor is actually a symptom of underlying causes, rather than a root cause of itself. A structured root cause investigation explores the underlying causes and examines the systems and conditions involved in the incident.

This approach would consider evidence gathered related to the following issues:

- How did the oil come to be on the floor in the first place?
- What is the source of the oil?
- What tasks were underway when the oil was spilled?
- Why did the oil remain on the floor?
- Why was it not cleaned up?
- How long had it been there?
- Was the spill reported?
- What is the usual condition of walking surfaces in that unit?
- What influenced the employee to step into the oil?
- What type of shoes was the employee wearing?
- Why didn't the employee go around the puddle of oil?
- Was the area barricaded to prevent entry?
- Are there training or consistency of enforcement issues involved?

As these questions are answered, the continuing prompt for a better understanding of why the incident occurred should be, "Why? Why did this particular event occur?" These answers take the investigators deeper into the origin of the incident. Once this evidence has been analyzed and the causal factors identified, the root cause analysis can commence to identify weaknesses in the management systems involved. For instance, if the oil was determined to have leaked from a defective container, one might ask:

- Why was a defective container used?
- What are the procedures for inspecting, repairing, or replacing the containers?
- Are the procedures clearly understood and enforced?
- Is the system to manage the containers properly designed or are there gaps?

If a failure occurs and no changes are made to the management system, then the failure will likely occur again. Often corrective action is taken — yet the failure still recurs. Frequently this is because the corrective actions address symptoms rather than root causes.

The objective of incident investigation is to prevent a recurrence. This is accomplished by establishing an incident investigation process that:

- *Identifies and evaluates causes;*
- *Identifies and evaluates recommended preventive measures that reduce the risk (probability and/or consequence); and*
- *Ensures effective implementation and follow-up of all recommendations.*

Determining the root causes of a failure is a necessary precursor to formulating recommendations and implementing actions.

Best practices in incident investigation have evolved substantially over the years. This chapter uses case studies to illustrate effective root cause analysis, describes some non-proprietary tools and techniques, and presents three approaches to incident root cause analysis.

10.2 CASE HISTORIES

The following two case studies highlight how incidents can have multiple causes, including root causes related to management system deficiencies.

FLIXBOROUGH

In 1974, 28 people died in an explosion resulting from a large release of cyclohexane in Flixborough, U.K. The source of the hydrocarbon release was a failed expansion joint in a section of 20-inch (508-mm) diameter pipe. Investigation revealed the pipe had been “designed” with little technical input as a temporary bypass for a reactor that had been removed for repair after it cracked (CCPS, 2010).

The immediate cause was a failed expansion joint. Fixing or replacing the expansion joint was the apparent corrective remedy. However, a more thorough root cause analysis looked deeper into the reasons why the joint failed. Here are some of the identified underlying root causes:

- The management system for reviewing, approving, and managing changes to process equipment was inadequate. Temporary modifications were not reviewed by the appropriate technical discipline.
- The reactor that had been removed and bypassed with the expansion joint had failed due to stress corrosion cracking from nitrates. The source of the nitrates was water sprayed from an external hose used for supplemental cooling due to insufficient heat transfer removal capability. The inadequate cooling capacity was resolved with a less than adequate technical solution that caused unexpected and unwanted consequences. Management of Change was not properly applied to this modification.

CHALLENGER SPACE SHUTTLE

The *Challenger* space shuttle disaster (January 1986) was the culmination of a series of occurrences, each with its own root cause (Rogers, 1986).

The immediate cause was failure of the ring joint seal on the solid rocket booster. Yet, a root-cause analysis revealed a much more complex scenario. According to information published after the investigation, post-flight evidence from as far back as early 1984 showed that the joint seals were failing to meet design specifications.

A decision was made to use reusable solid rocket boosters to save cost in order to get the Shuttle project approved by Congress. Engineers at the time complained that the design integrity was suspect, but were overruled to keep budgets in line. Almost 2 years before the incident, engineers knew that holes were being blown in the putty that shielded the *primary* O-rings from hot gases. In addition, evidence from 1983 showed the *secondary* O-rings were experiencing problems due to joint rotation during launch conditions. The reduced flexibility of the O-rings at temperatures below 50 °F was also known. In July 1985, the

concerns had grown to the point that further launches were postponed until an attempt was made to remedy the situation. But these remedies were ineffective and did not deal with the causal factors or root causes of the problem joint. Despite all that was known about the O-ring problem, a decision was made to launch the Challenger on a cold January morning with devastating consequences. The *Challenger* space shuttle disaster is an excellent example of the principle that apparently simple mechanical problems are related to more complex underlying causes rooted in management systems. The recommendations submitted by the presidential commission focused on *root* causes. These involved changes in management systems that would not only fix the ring joint problem, but also the systems, procedures, and overall approaches to identifying, evaluating, resolving, monitoring, and auditing safety-related concerns.

10.3 METHODOLOGIES FOR ROOT CAUSE ANALYSIS

10.3.1 5 Whys Technique

The 5 Whys is a simple methodology for identifying root causes that involves repeatedly asking the question “why?”. The methodology is easy to understand and perform, and the technique adds some structure to group brainstorming. Large quantities of information and data are not necessary (although useful for complex process safety incidents), and therefore the technique is suitable for minor incidents, especially those involving human factors and interactions. The 5 Whys is also widely used as an integral part of Kaizen, Lean Manufacturing, and the Six Sigma methodology [e.g., the Analyze phase of Six Sigma DMAIC (Define, Measure, Analyze, Improve, Control)].

Although called 5 Whys, five is only a rule of thumb, and sometimes the investigation team will ask “why?” more or fewer than five times. The technique requires that the investigation team asks “why?” a negative event occurred or undesirable condition existed (i.e., causal factors), and then asks “why?” enough times to reach a management system deficiency. The process is repeated until all the causal factors have been considered. In essence, this is analogous to a logic tree approach without actually drawing the logic tree.

SOME GUIDING QUESTIONS FOR MULTIPLE CAUSE DETERMINATION:

- *WHY? (Keep asking WHY? WHY?)*
- *What were the underlying causes? (Why did they exist?)*
- *Was there a system-related deficiency (or weakness) that caused (or allowed) this condition to exist, or caused or allowed the occurrence to proceed? (Why did such a system failure exist?)*

An example of the 5 Whys root cause analysis technique is illustrated in Figure 10.1. In this example, two deficient management systems (asset integrity management and operator routine rounds) are identified after asking “why?” five times, and a sixth or seventh time may reveal an underlying reason for those deficient management systems.

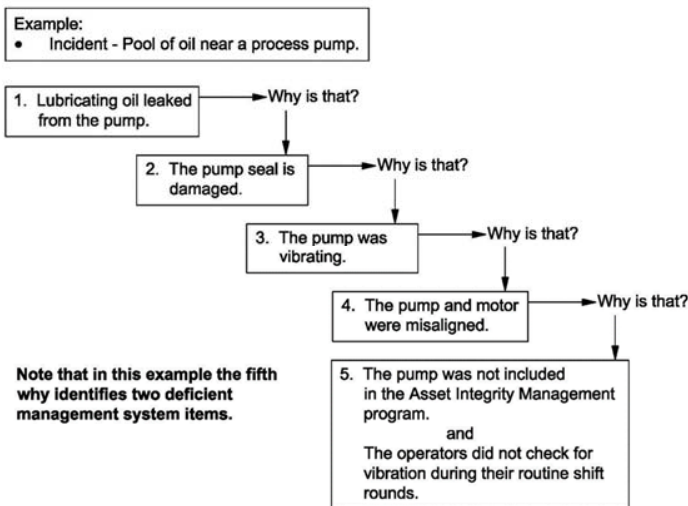


Figure 10.1 Example of 5 Whys Root Cause Analysis

Judgment is needed to use the technique effectively. If it is easy to answer “why?” at a certain level, then the analysis typically has not gone deeply enough and should continue to ask “why?”. Similarly, if a

management system deficiency has not been reached, the team has stopped too soon at a symptom, immediate failure, or an event that contributed to the incident. Sometimes, the investigation team may not be able to proceed due to a lack of knowledge or information, in which case further evidence gathering and analysis may be required.

Most incidents do not have a single root cause. In order to identify multiple root causes, the technique should be repeated asking a different sequence of questions each time. For example, the investigation team should examine other possible reasons for the original causal factor *before* starting with a different negative event or undesirable condition that influenced the course of activity leading up to the incident.

The 5 Whys technique may be used individually or to assist development of a fishbone diagram (also known as Ishikawa or Cause & Effect diagram). A fishbone diagram is used to examine potential causes of an incident or equipment failure, and the 5 Whys may be used to uncover the root causes. The incident is shown as the fish's head with the causes extending to the left as fishbones. Causes are usually grouped into major categories (e.g., people, process equipment, etc.), and branch off the backbone as ribs with sub-branches for root causes. Figure 10.2 illustrates a typical fishbone diagram.

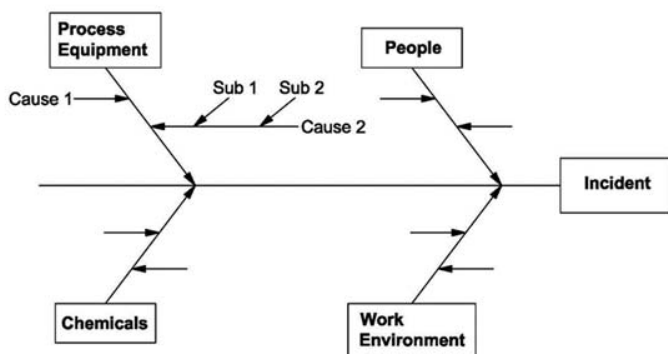


Figure 10.2 Example of Ishikawa Fishbone Diagram

While companies in different industries have successfully used 5 Whys, the technique has some inherent limitations. Table 10.1 illustrates some of its strengths and weaknesses. The fishbone diagram has many of the same

limitations. For example, the fishbone diagram is not particularly useful for complex incidents where many causes are interrelated.

The knowledge and experience of the investigation team is important in any root cause analysis, but especially so when applying the 5 Whys. In simple, low risk incidents, flaws tend to be diminished as the analysis is simpler, and there is less tendency to skew results. Conversely, complex high risk incidents increase the possibility that the analysis may fail to identify some causes, and care is necessary to avoid bias. Investigators might inappropriately start the analysis with their ultimate cause in mind and then look for signs that they are right rather than completely understanding what happened. However, with training, practice and understanding its weaknesses, it is possible to overcome most of the 5 Whys’s drawbacks and correctly identify the root causes of an incident.

Table 10.1 Strengths and Weaknesses of the 5 Whys Technique

Strength	Weakness
Simple, easy to teach and use	Requires skill as: <ul style="list-style-type: none"> • selection of poor/meaningless causal factor may invalidate the analysis • one poor/meaningless why? may invalidate the analysis
No rules regarding line of questioning	Lack of rules regarding line of questioning can introduce investigator’s bias
Starter tool - can instill discipline of searching for true root cause	Investigation team may focus on a single causal factor or stop too soon at a symptom
Can identify multiple root causes	Investigation team may stop at single root cause – requires persistence to seek multiple root causes
Not data driven	Requires knowledgeable investigation team, otherwise the cause(s) is unknown
	Results may be (un)intentionally biased by the investigation team: <ul style="list-style-type: none"> • tendency to use deduction rather than facts (observation & analysis) • lack of rigor to test for sufficiency
Less time-intensive	Not repeatable - different investigation teams may come up with different root causes
Can be used alone or in combination with other methods	Other techniques are better for complex incidents
Best suited to simple or minor incidents	May not find all root causes for complex investigations

10.3.2 Structured Root Cause Determination

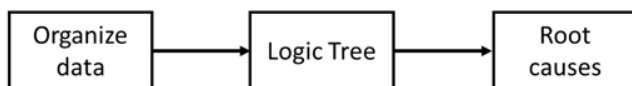
The “5 Whys” methodology is a brainstorming approach to root cause identification. There are other, more structured methodologies that are useful in root cause determination. Two structured root cause approaches, logic tree and a pre-defined tree, are presented in this chapter.

1. *Logic Tree* analysis involves a deductive search for all credible ways in which an occurrence could arise, using timeline construction and a simplified fault tree approach. It can be viewed as an integrated method for systematically searching for all underlying root causes. The structured framework helps the investigator to keep on track, reach sufficient depth, and not stop prematurely at the symptoms or apparent causes.
2. *Predefined Tree* analysis involves timeline or sequence diagram construction, identification of causal factors, followed by the use of predefined trees or checklists. A predefined tree provides a systematic approach for analyzing and selecting the relevant elements of the incident scenario. It is a deductive approach, looking backward in time to examine preceding occurrences necessary to produce the specified incident.

Structured root cause investigations attempt to identify and implement system changes that will eliminate recurrence, not only of the exact incident, but of similar occurrences as well. Structured root cause methods recognize that incidents have multiple underlying causes. These methods improve the quality of investigations by directing the focus past the immediate surface causes to the underlying root causes and mandating a search for multiple causes. One of the strengths of systematic methods is the ability to separate a complex incident into discrete smaller occurrences (segments) and then to examine each piece individually.

Figure 10.3, the two flowcharts describing root cause determinations using the above methods, presents general frameworks for root cause determination after evidence gathering and analysis.

Logic Tree



Predefined Tree

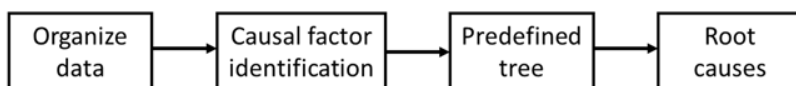


Figure 10.3 Structured Root Cause Methods Described in This Chapter

While some methods use checklists as the logic analysis step, an understanding of the logic tree approach is still helpful because checklists are often developed from logic trees. Checklists are especially helpful for incidents involving human factors.

The approaches shown here also present tools to test logic, determine if the root causes identified go deep enough, help discern what to do if a team gets stuck, and aid in decision-making. These tools work with any logic analysis methodology.

It is not the intention of the CCPS to endorse one particular method, but to present guidance on the various options and applications available. Structured methodologies that seek out multiple underlying systems-related causes of an incident and provide the mechanisms for determining and correcting system faults are generally found to be the most effective.

10.4 ROOT CAUSE DETERMINATION USING LOGIC TREES

The following section presents a systematic discussion of the concepts and actions depicted in Figure 10.4. The starting point for the flowchart is the accumulation of facts, information, observations, insights, questions, and preliminary speculations gained from the evidence collection activities described previously.

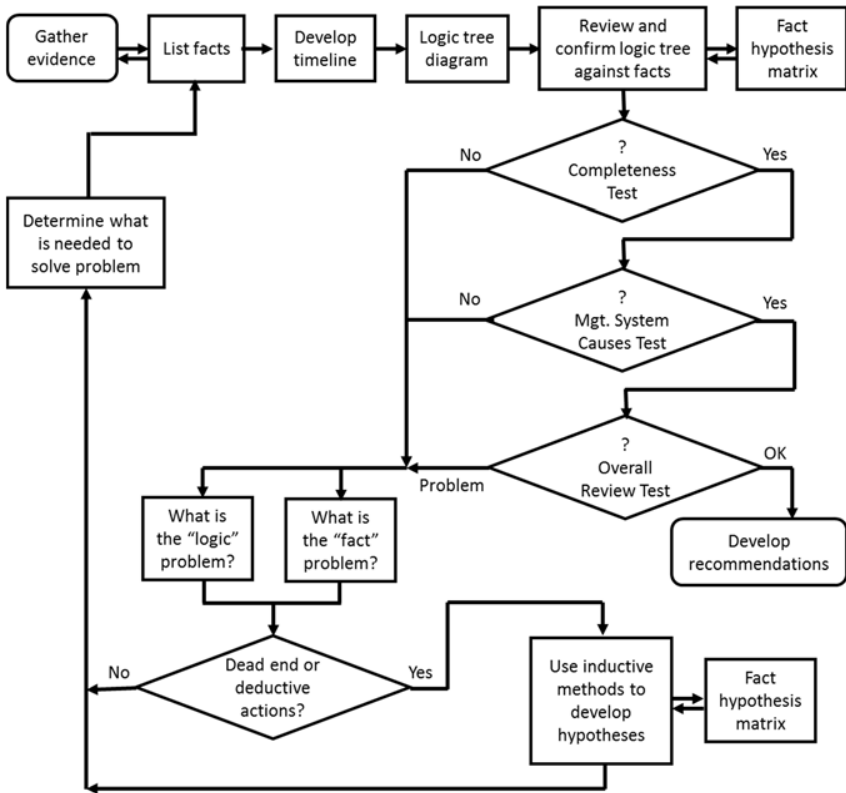


Figure 10.4. Flowchart for Root Cause Determination Using Logic Trees

10.4.1 Gather Evidence and List Facts

The first task is to develop a list of all known facts. This list includes not only facts relating to the incident sequence, but also all pertinent background data, specifications, and recent past or external events that could or did have an influence on the overall system.

A fact should be a true, proven piece of data. Avoid drawing conclusions or making judgments at this stage. An example fact is—*Hearing protection boundaries in the area are not marked*. A conclusion may be that the boundaries are not clear, but do not make that jump yet. Sticking to the facts will help prevent people involved in the incident from becoming defensive and will prevent the team from jumping to conclusions. Sticking to the facts will also assist readers in understanding the complete incident report.

The team needs to take care to avoid being trapped by hidden or erroneous assumptions. All facts should be tested. The facts are essential inputs to ensure that the correct scenario is selected later. Any apparently conflicting facts should be resolved through additional data gathering. Listing the source of each fact will facilitate conflict identification and resolution.

10.4.2 Timeline Development

Next the team develops a chronology of events based on the available known times and sequences and prepares a timeline or sequence diagram. Unconfirmed assumptions regarding chronology should be clearly identified as unconfirmed, and action should be initiated to verify assumptions. Many investigators use relatively simple timelines (instead of sequence diagrams) with the logic tree methods because the logic tree itself shows the interactions of events and conditions.

10.4.3 Logic Tree Development

After the initial facts have been listed and the initial timeline has been developed, the logic tree diagram can be constructed. The tree diagram is a dynamic document; it continues to expand and may even be rearranged as additional information becomes available or when new information changes the understanding of the original facts.

Once the facts have been gathered and the timeline developed, there may be sufficient information available to confirm or refute a hypothesis in the early stages of logic tree development. For many simple and straightforward failures, general knowledge of the component failure mode

behavior, used in conjunction with the specific information gathered for a particular incident, may be sufficient to diagnose the causes. However, most process safety incidents are complex in nature and have multiple underlying system causes. Therefore, a systematic deductive approach is usually appropriate.

An exercise that can be performed at this stage of the investigation is to conduct a multiple root-cause determination meeting. Besides the investigation team, the participants may include members of the operating unit where the incident occurred. (There will probably be some members from the operating unit already on the team.) The meeting should be small enough to be efficient and inclusive enough to have all the information necessary to develop the logic tree. When possible, try to limit the number of participants to about eight or fewer to foster interaction. Selected participants should understand the facts of the investigation, and the participants should also bring knowledge of important elements of the process such as operations, chemistry, equipment, and controls. Some specialists may be brought in when needed. In some situations, it may be necessary to include representatives from unit management, employee unions, and legal counsel. The meeting should be as open and as fact-based as possible. When deciding to include people from outside the investigation team in the meeting, consider these questions:

- Are they knowledgeable about the process?
- Do they have knowledge that will contribute to the investigation?
- Will their involvement hamper the independence of the team?

In the opening segment, the facilitator should discuss the importance of choosing the appropriate top event for the logic tree as well as any pre-established and existing boundaries of the investigation. If multiple events are involved, it is best to start with the last event in the time sequence. It may be appropriate, depending on the nature of the occurrence, to formally review the rules and symbols used in logic tree or fault tree development (or whichever other formal method will be used).

At the end of this meeting, a formal critique should be considered to consolidate lessons learned for future meetings. The critique should consider what went well and what changes could be made to improve future meetings. It would also be appropriate at the conclusion of the session to thank the participants for their contributions, to restate the purpose of the meeting, and to recap how and whether it was achieved.

At this point, the logic tree structure is examined to ensure that the tree is logically consistent and compatible with the known facts. In some instances, there may be inconsistencies, and application of the fact/hypothesis matrix will be appropriate. Inconsistencies found at this point require further tree development or rearrangement.

Once the logic tree structure appears to be consistent, the first of three quality assurance tests is applied by examining the overall logic tree structure for completeness. The logic in each branch of the tree should be tested to determine if it is necessary and sufficient. (Details and tips for testing the logic are discussed in Section 10.5.2.) If the tree appears to be complete, the next quality assurance test is initiated. If the tree is incomplete, then the fact or logic problem is identified and the entire process is repeated. This is called an iterative loop.

If the logic tree appears to be complete, then the second quality control test is applied by asking the question, "Are the causes that have been identified actually related to management systems?" If the answer is yes, then the investigation proceeds to the third quality control test—the final overall review. If management system causes have not been found, then the iterative loop process is used.

It is important to note that not all management system causes may be located at the extreme bottom points on the logic tree. Some of the management systems-related causes can be - and often are - located in the upper or middle portions of the logic tree diagram. Some causes can also be identified by the logic tree structure itself. For example, an overview of the entire tree structure may indicate significant gaps or overlaps in responsibilities, or it may disclose conflicting activities or procedures. These insights may be overlooked if the investigators limit their cause search to only the bottom level of the structure and fail to review the entire tree and the interrelationships between branches.

If the test for systems-related causes is satisfactory, then the third and final quality assurance test is applied. This is an overall review of the logic tree as a whole for both facts and logic. A conscientious review of each branch should be made to look for possible conflicts or inconsistencies. It is a pause to focus on the logic tree from an overall perspective, not just each branch. The final logic diagram should be thoroughly checked against the final timeline to ensure that these two are in complete agreement. The team should also verify that none of the facts is in conflict with the tree. If the incident investigation team is satisfied with the causes identified, then the

investigation proceeds to the recommendation stage. If a problem or some incompleteness is noted, then the iterative loop is reactivated.

After the tree is developed, and before moving on to the recommendations and deliberations, the team should ask, “Are there any *other* causes that anyone had in mind at the beginning of this meeting that are *not* included in the tree?” If additional causes are identified, the team adds them to the tree if there is logic to support them. Some team members may have specific concerns that the logic tree has not adequately resolved. This is the point at which remaining issues are brought forward and addressed. It is important that any new causes also pass the necessary and sufficient testing.

In the deductive process of identifying root causes, known facts are assembled and used to develop and test one or more possible scenarios. The process normally requires multiple iterations of the cycle shown in Figure 10.4 until at least one plausible scenario is identified that fits all the known facts.

If a scenario is disproved by the known accepted facts, the reasoning is documented and the scenario need not be investigated further. If the scenario needs additional data in order to be proven or disproved, then the iterative loop path is followed and additional information is gathered. Sometimes this new information is very specific, precise, and limited in scope. Examples of tasks initiated by this iterative loop include:

- Follow-up witness interviews,
- Revisiting or reexamining a certain area of the incident scene, and
- Commissioning expert consultant opinions.

If the deductive process continues to indicate progress, then additional facts are sought or the logic tree is restructured. For example, one witness stated a particular valve was open, yet the post-incident inspection found it to be closed. The team must be careful to ensure that the valve is closed because of the actions taken prior to the incident, and not as a result of post-event response activities. The position of this particular valve may be a critical item in determining which of two scenarios is the more probable case. The incident investigation team would then initiate a short-term action item to resolve this question.

If the deductive process has stalled and no further progress seems possible or likely, then the iterative loop calls for application of inductive

investigation methods such as a checklist or HAZOP. The inductive methods may also benefit from use of the fact/hypothesis matrix tool.

10.5 BUILDING A LOGIC TREE

As previously discussed, the logic tree is a systematic mechanism for organizing and analyzing the elements of the incident scenario. It is a deductive approach, looking backward in time to examine preceding events necessary to produce a specified result. This section illustrates building a logic tree using a simplified fault tree approach and includes the key steps of the methodology and tips for successful use. Examples are also provided to illustrate the application of the logic tree approach.

Standard symbols from systems theory are often used to construct the logic tree diagram. The diagram often takes the form of a qualitative fault tree, showing the incident as the top event and the various branches using conventional AND- and OR-gates. Some investigators have simplified development of the logic tree by not distinguishing between AND-conditions and OR-conditions on the first pass through the tree. Instead, they use a “universal gate” and determine its status as the investigation progresses. Other techniques use only AND-gates. Other similar methods (such as causal tree) will be somewhat different in terms of symbols and the look of the tree, but the basic concepts are the same. Various proprietary software programs are available to facilitate development of logic trees.

The trees in this section will be drawn from top to bottom. Some similar techniques are drawn from left to right or right to left. In a systematic way, the logic tree provides a structure for thoroughly considering possible multiple causes. Each of the succeeding lower levels is developed by repeatedly asking “Why?” until a level is reached that allows examination of a management system or a small segment of it. The particular management system would then be scrutinized for deficiencies that caused or contributed to the incident. Identifying deficiencies provides a foundation for recommended improvements and preventive action.

Many deductive investigation techniques use logic tree diagrams. A partial list of these methods includes fault tree analysis (FTA), causal tree method (CTM), and Why Tree. These methods are described in Chapter 3.

10.5.1 Choosing the Top Event

Choosing the top event for the logic tree may sound like a simple task, but it is often more difficult than expected. In the Flixborough incident, the top event could be the fatalities, the potential fatalities in the administration office building, the explosion, or the initial chemical release. If the chemical release is chosen as the top event, the discussion of why the people were in the area or why the office building was so close to the unit might never have occurred. As you review the example trees in the following sections, look at what might be left out, or included, if the top events were chosen differently.

It is also important and appropriate to consider the question “What could have happened?” When dealing with a near miss, there can be differences of opinion among the team members as to the credible negative consequences of the incident.

*Team Members should remember:
Severity is often a matter of chance.*

The incident investigation team should evaluate potential effects of an incident on all the stakeholders interested in a facility’s continued safe operation. Public perception and good will are very important. The top event chosen for a near miss might be a credible potential outcome such as an injury, chemical release, toxic exposure, fire or explosion.

10.5.2 Logic Tree Basics

To put it simply, a logic tree is developed by repeatedly asking “Why?” and organizing the results of the answers.

A generic logic tree for a fire incident is shown below in Figure 10.5. The top event is defined as the unwanted fire, with fuel, oxygen, and ignition depicted in the three branch conditions leading to the top event. Each of the three branches would then be examined, developed, and expanded into further detail as the investigation progresses.

The diagram can be developed from the top downward and can model a system, subsystem, or any individual component. For each level, a set of *necessary* and *sufficient* lower-order conditions or events is identified.

The basis for logic tree construction lies in the application of logic gates (Other symbols are used to explain the overall system structure and analysis boundaries.) The most important logic gates are the OR-gate and the AND-gate. (Other gates are used occasionally).

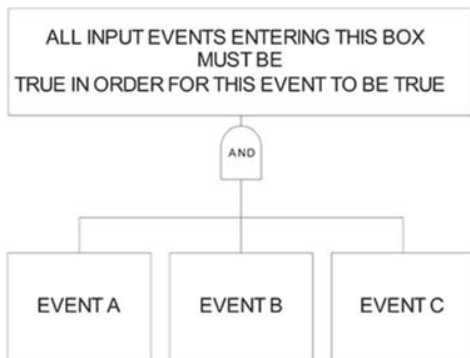


Figure 10.5 Generic Logic Tree Displaying the AND-Gate

The AND-gate is such that the *output occurs only if all the input events occur*. Event A **and** Event B **and** Event C must all occur for the output event to happen. A generic logic tree with and AND-gate is shown in Figure 10.6.

Figure 10.6 illustrates an AND-gate: fuel, oxygen, and an ignition source must be present for a fire to occur. If any of these components were missing, the fire would not occur. These conditions are necessary and sufficient for the fire to occur.

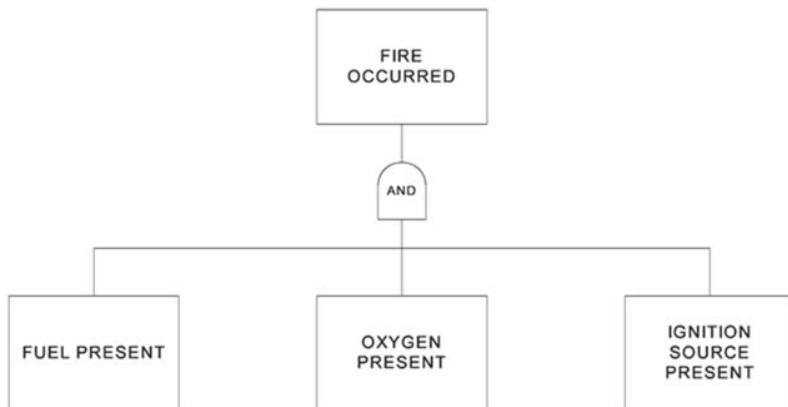


Figure 10.6 Generic Logic Tree for a Fire

Figure 10.7 illustrates an OR-gate. The OR-gate is such that the *output event occurs if any one or more of the input events occur*. Event A **or** Event B **or** Event C . . . must occur for the event to happen.

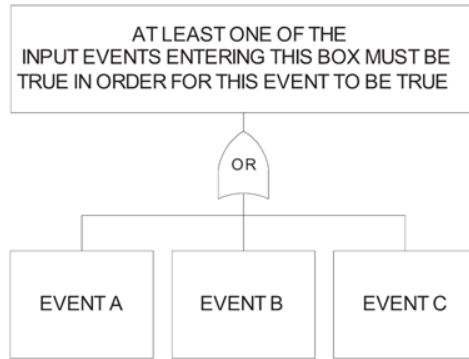


Figure 10.7 Generic Logic Tree Displaying the OR-Gate

A good example of an OR-gate is an ignition source as shown in Figure 10.8.

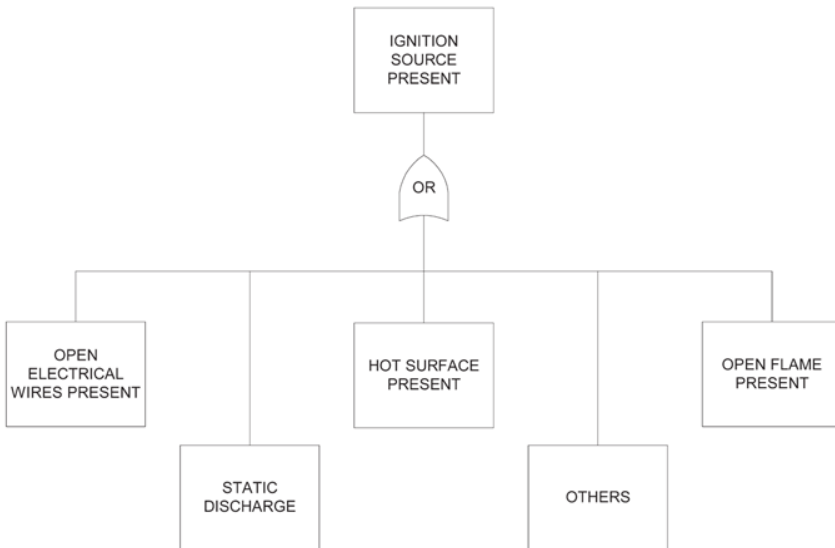


Figure 10.8 Logic Tree using the OR-Gate to establish an Ignition Source

The symbols for AND- and OR-gates are often omitted. Instead, the words are written above the connecting lines.

The tree logic should be checked every time a new event is added to the tree. If an event below the OR-gate is not sufficient on its own to cause the event above it, it needs to be joined with an AND-gate with the other necessary event. If an event below an AND-gate can cause the event above it on its own, then the event should be moved out from under the AND-gate and connected to the event by an OR-gate.

The investigation team uses an iterative process and begins to prove (accept, confirm, verify) or disprove (refute, reject) each of the OR-branches. Keeping the "OTHERS" box on the chart until very late in the tree development will help prevent the team from drawing premature conclusions.

Determining whether you have an AND- or an OR-gate becomes important when testing the tree logic, because the types of gates are tested in different ways. The type of gate is also important when developing recommendations. The recommendations will help reduce the frequency of an event when implementing the recommendations will add an AND-gate to the tree. A recommendation that eliminates only one branch of an OR-gate will be less effective (for instance, eliminating one ignition source out of many).

Some investigation techniques do not use OR-gates. If the team cannot figure out which input led to a top event, they stop tree development at that point. Speculation is not allowed.

Investigators can use the following frequently used logic tree symbols (Figure 10.9); however, adequate logic trees can be developed without using them.

Small steps should be taken in developing the tree. One technique available to help the team take small steps is to determine whether input blocks are active or passive. Active blocks are factors that change (e.g., an ignition occurs or a valve is opened). In each AND-gate, there should only be one active event. The rest of the blocks in the AND-gate describe passive or existing conditions (e.g., system contains pressure or people are in the control room). At the time the active event occurs, the gate event happens.

Figure 10.10 presents tips on developing logic trees.

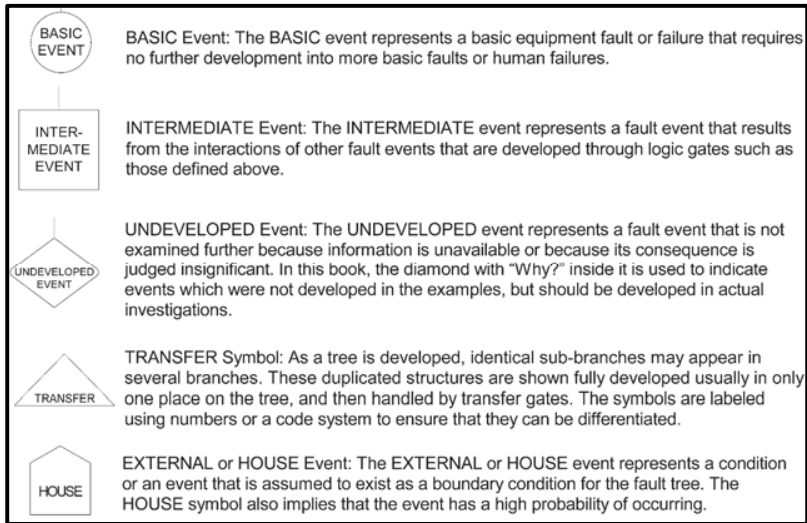


Figure 10.9 Other Symbols Used in Logic Trees

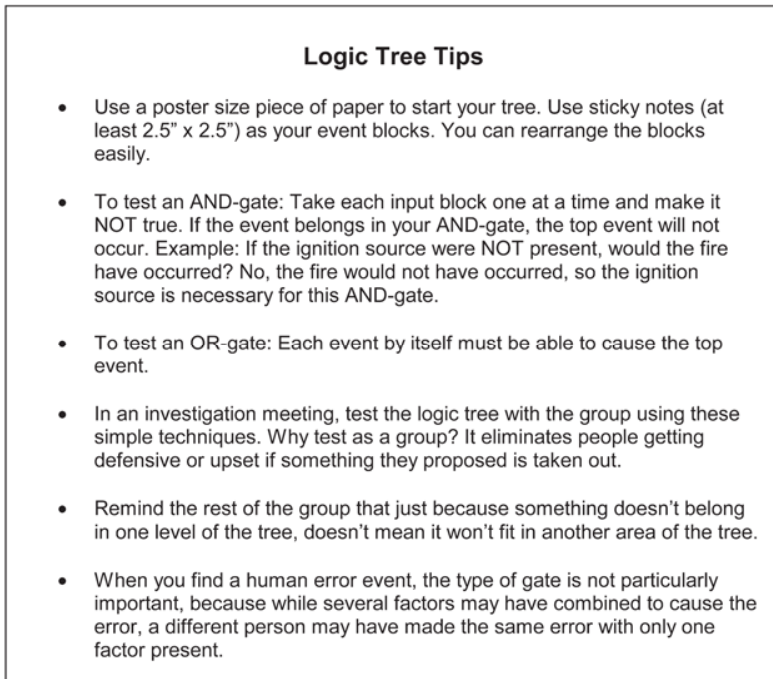


Figure 10.10 Logic Tree Tips

Consider the incident scenario discussed previously:

A worker was walking on a concrete walkway in the process unit. There was some lube oil on the pad. He stepped into the oil, slipped, and fell. It was a sunny day; the worker was not carrying anything, was not distracted, and was not doing any urgent task.

The top portion of the logic tree may look something like the tree in Figure 10.11.

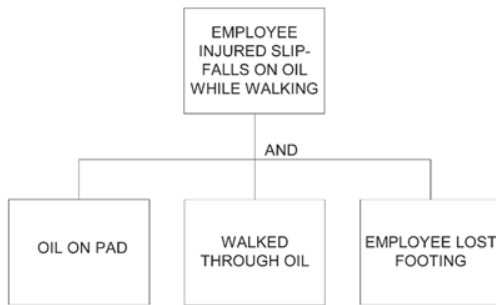


Figure 10.11 Example Top of the Logic Tree, Employee Slip

Each of the succeeding lower level events is further developed by repeatedly asking the question, “Why did this event occur?” Pursuing just one branch, for example the *Oil Spilled on Pad* branch would lead to at least two possible sources: *Leak from Pipe* and/or *Hand Carried Containers*, as shown in Figure 10.12 and Figure 10.13.

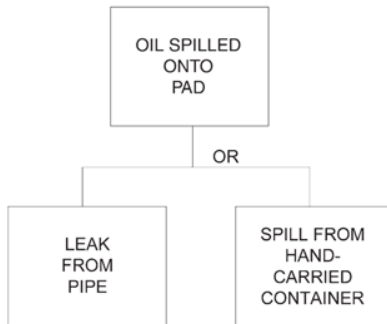


Figure 10.12 Example Logic Tree Branch Level, Oil Spill

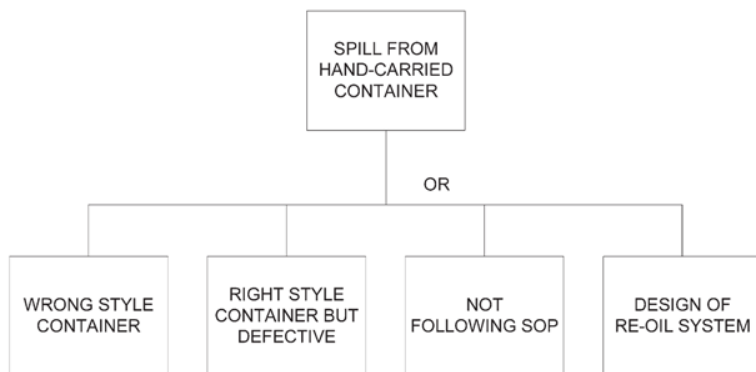


Figure 10.13 Example Logic Tree, Hand-carried Containers

Going a little farther down the tree and further developing just one of these sources, a spill from a hand-carried container, would yield additional possible causes. Each of these four subcategories can now be examined individually. Selecting one (*Right style container—but defective*) and returning to the concept of management systems leads to the following considerations.

- What is the management system involved in inspecting, repairing, or replacing the containers?
- Is the management system properly designed and arranged to achieve the desired output?
- Is the management system clearly understood and consistently enforced?

In this example, the team examined the pad surface and the employee's shoes and found both acceptable for the working conditions. Therefore, they decided "Employee lost footing" was a boundary event, i.e. a 'trigger' event assumed to exist as a boundary that defines the incident for which the logic tree is constructed. The team decided to pursue the "Recognized Hazard but Walked Through it Anyway" path. However, each of these items could also be evaluated further. In this example, the root causes are related to weaknesses in the management systems for hazard awareness and asset integrity of containers.

A larger version of the tree is shown as Figure 10.14, although it is not completely developed. (The figure is turned for better viewing.)

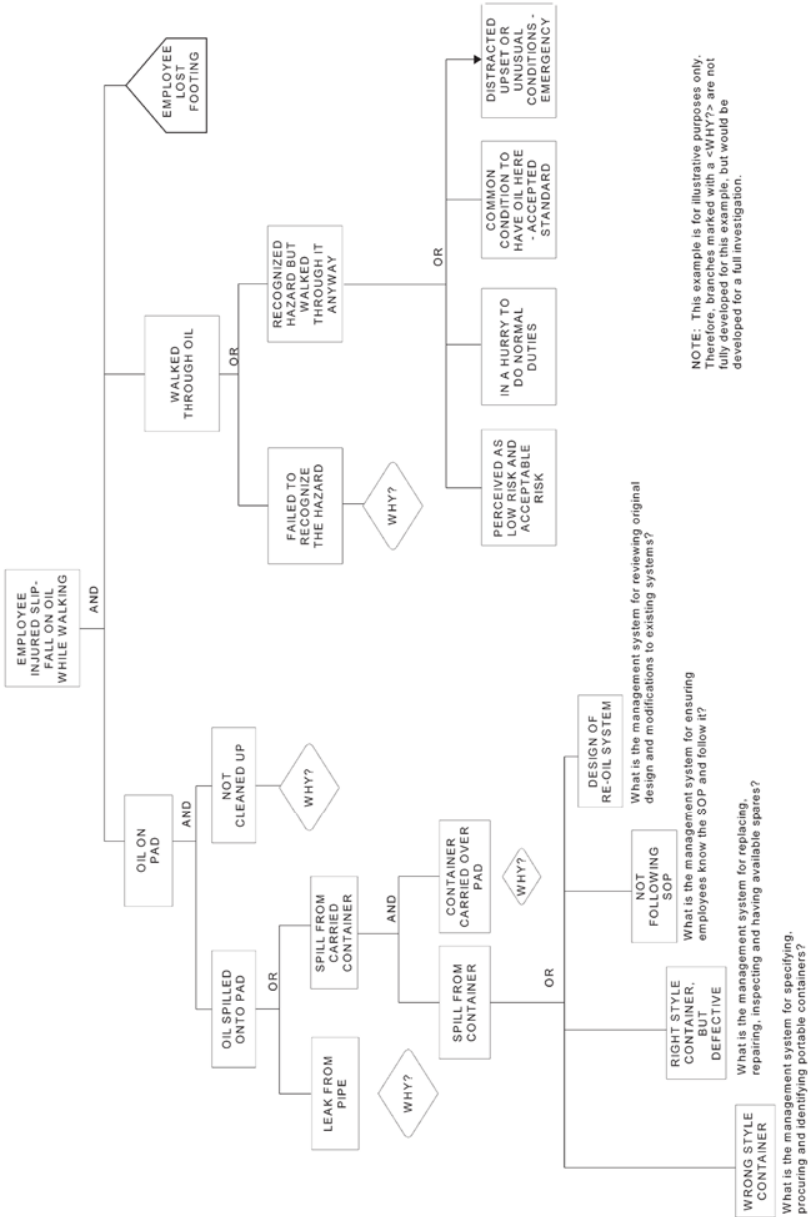


Figure 10.14 Logic Tree, Slip/Trip/Fall Incident

10.5.3 Example—Chemical Spray Injury

Consider the following typical incident.

An employee is sprayed with an organic acid while loosening the handles on a filter lid in preparation for changing the filter. The employee is burned, although the acid takes several minutes of contact before a burn occurs. It took the employee a few minutes to get to the safety shower, because a pallet blocked the path to the closest shower. The employee went to another shower, which was farther away.

The employee statements include: “The filter was already blocked in. I opened the drain and only a small amount of material came out, so I figured the last shift had already drained it. I can’t believe that someone put that pallet there and blocked the shower access.”

A check of the records indicated the pallet had been delivered several days earlier.

The top part of the tree looks like the one shown in Figure 10.15.

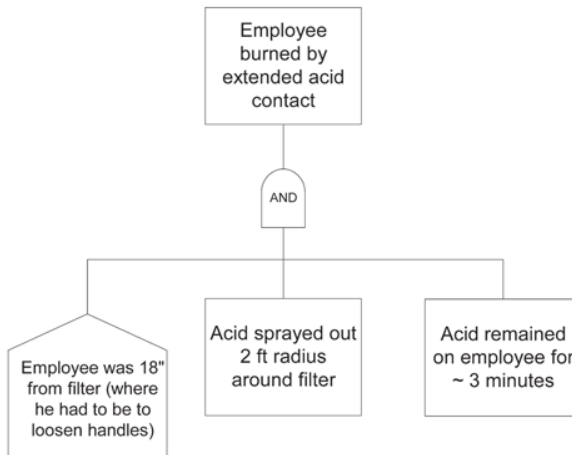


Figure 10.15 Logic Tree Top, Employee Burn

The team decides not to pursue the left branch any further, because the employee had to be in that location to open the filter. It was a necessary condition for the desired activity to occur.

Now, the team pursues the middle branch, shown in Figure 10.16.

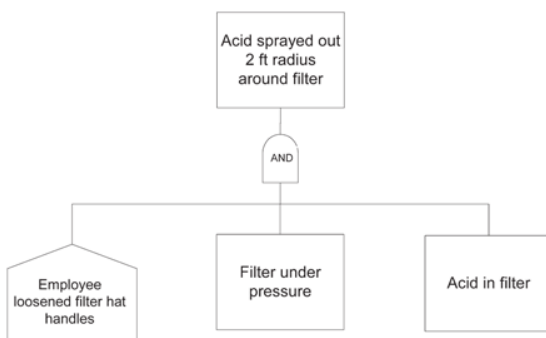


Figure 10.16 Logic Tree Branch, Acid Spray

The team continues asking, “Why?” and develops the branches. A more complete tree is shown in Figure 10.17, but is not fully developed. (Again, the figure is turned for better viewing.) The team still needs to delve into the reasons the pallet was put in the path in the first place, and why it was allowed to remain there for several days.

They should seek answers to questions such as:

- Was there a procedure for where the pallet should have been placed? If so, was the procedure followed?
- Do operations personnel approve locations for placing materials?
- Do operations personnel receive any training in hazard recognition?
- Should pre-job safety reviews be conducted?

Notice the event labeled “Drain/vent valve plugged” appears on two branches of the tree. This illustrates the concept of *common cause* failure, when the same cause appears in more than one place on the tree. In this case, the liquid drain and the vent valve were one and the same, located on

the bottom of the filter. In addition, there was no way for the employee to tell if the pressure was still on the filter, since the pressure gauge could become plugged as well. In this case, the investigation team recommended that a pressure indicator and a separate vent valve be added to the filter.

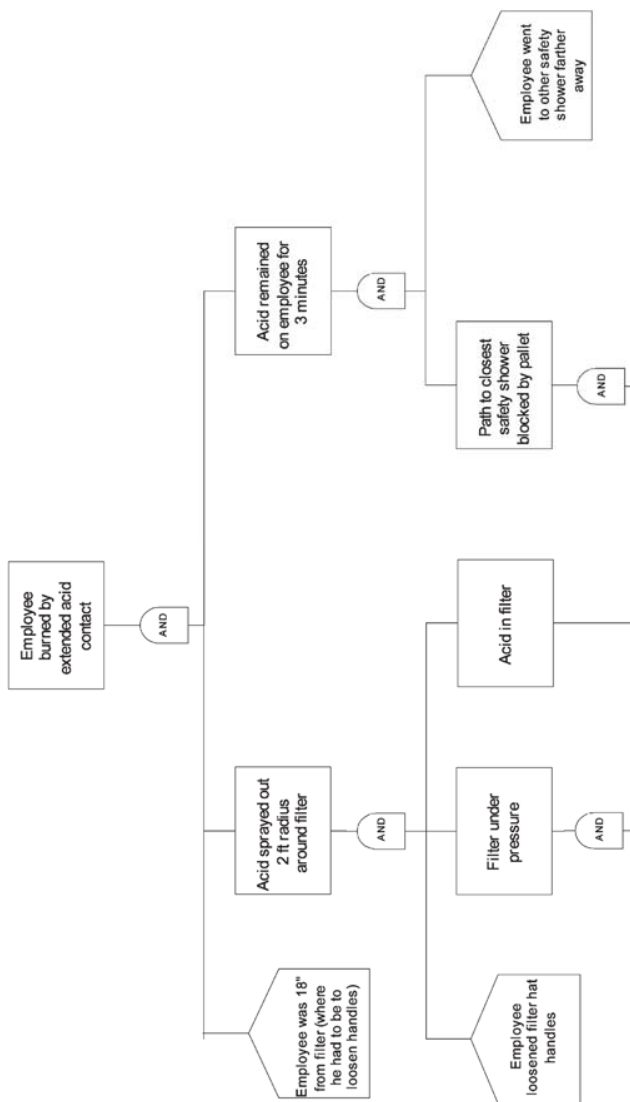


Figure 10.17 Expanded Logic Tree Sample, Employee Burn

[Note – Tree Top: the Tree Bottom is on the following page.]

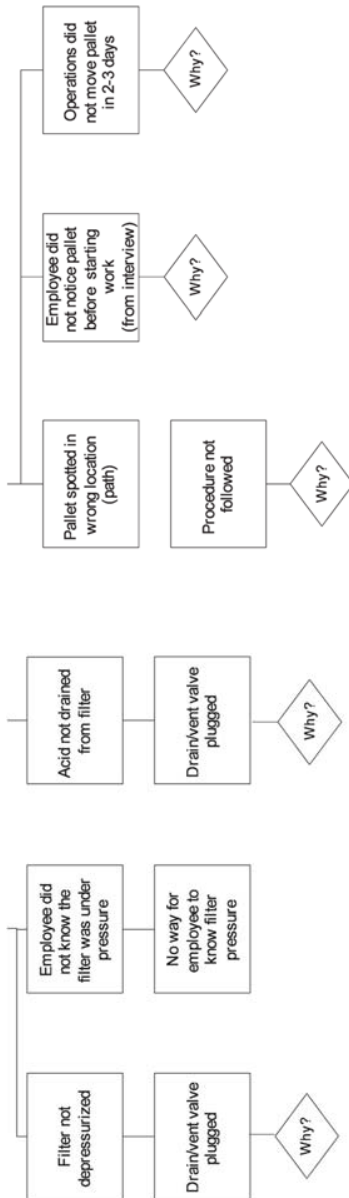


Figure 10.17 Expanded Logic Tree Sample, Employee Burn

[Note – Tree Bottom: the Tree Top is on the previous page.]

The team should also be asking questions about the filter design and PPE worn by the employee, such as:

- Was the design of this filter reviewed?
- Has the filter design changed since installation? If so, were any such changes reviewed?
- Did safe work practices for breaking containment require special PPE (e.g., face shield, chemical splash gear, etc.)?
- Was the employee wearing the correct PPE? If not, why not?

10.5.4 What to Do if the Process Stalls

The deductive process can stall for two major reasons:

1. There is no hypothesis for an event.
2. There are too many hypotheses for an event.

If there is no hypothesis for the event, use an inductive method to find potential scenarios. Common inductive logic methods include HIRA techniques such as checklists, What If?, and Hazard and Operability studies (HAZOPs). Inductive methods speculate a given fault or failure, then look forward in time to determine the probable outcome, that is, “What would happen if ...?” For example, by asking “What if there was no indication of pressure and the filter was opened?” the team could apply an HIRA approach to postulating potential causes and considering the adequacy of existing safeguards.

If there are too many hypotheses for an event, use a fact-hypothesis matrix to help figure out which one it might be. The team may have to evaluate several branches of the logic tree if more than one hypothesis seems credible.

10.5.5 Guidelines for Stopping Tree Development

After the most likely scenario has been identified and the logic tree developed, the incident investigation team now reaches the stage of searching out the system-related multiple causes. An accompanying challenge is deciding when to stop further development of each branch of the tree.

Perhaps the most common mistake made by root cause investigation teams is to mistake a symptom for a root cause. At each level, continue to ask, “Why?” If you can easily answer, you have not gone deep enough.

Management system deficiencies tend to be a reliable indicator. These deficiencies can include breakdowns, oversights, weakness, failures not anticipated, audits not performed, or changes not incorporated into all related systems. If a management system change is required to correct a deficiency, then the item is a strong candidate for being a root cause. Judgment is needed to determine a realistic stopping point for downward tree development. It is usually theoretically possible to develop another lower level for any event, but it may not be of any benefit.

A common intermediate level finding may be that someone failed to follow an established procedure. Stopping at this point would be a mistake since *“failure to follow established procedure”* is rarely a root cause. A root cause approach would look further into the reason(s) for the operator failing to follow the procedure. Examples of possible reasons are given below.

- The procedure was unclear, hard to follow, out-of-date, sequence or facts wrong, or the situation was not covered.
- Employee perceived that a hazard was not significant.
- Enforcement or monitoring of procedures was inconsistent.
- The employee was in a hurry due to task overload (temporary or chronic).
- Some tool or supply was missing, so the employee improvised.
- The employee was rewarded for violating the procedure in the past.

The management issues involved in these failures could include policies, standards, administrative controls, supervisory practices, or training.

Consider the case of a component failure in a physical system, such as a bolt or a gasket. When an unexpected failure occurs, it can be for a number of possible reasons, such as:

1. Something changed while the component was operating, and an increased load was imposed on the component.
2. The strength of the component had degraded, but this degradation had gone undetected and/or uncorrected.
3. The material of construction of the component was unsuitable for the duty.
4. The component was improperly installed.

Investigators should keep developing the tree until they find issues, such as:

- What was the management system involved in this failure?
- Why did the management system for plant surveillance, test, or inspection programs fail to detect the incipient failure?
- Why did the preventive maintenance program at the plant not prevent the failure?
- If the failure resulted directly from a human error, what was the underlying reason for this error?

For components or devices supplied by outside manufacturers, the downward progression is usually stopped at the component level, unless the device is normally opened, repaired, calibrated, adjusted, or inspected by in-house personnel. Electronic black boxes (similar to those under the hood of our automobiles) are good examples. Owners may have occasion to manipulate the connection points (wires, attachment, and securing brackets) but typically do not open them or attempt to diagnose an internal malfunction.

Alternatively, certain systems are assembled and maintained by operators of chemical plants. For example, various components of a control valve system may be purchased separately and then assembled and configured by plant personnel. The incident investigation team would investigate possible accident causes associated with the methods of integration, assembly, maintenance, inspection, and calibration of the control valve system. Nevertheless, if a malfunction of a factory-sealed sub-component were involved, the incident investigation team would seek out the appropriate expertise. The team would usually *not* attempt to analyze any factory-supplied components that normally remain sealed without additional help. If the malfunction contributed to the incident, it should be investigated until it is understood, especially if similar components are in use elsewhere.

Another guideline is to stop the development of the tree when the events become external to the point that they can no longer be controlled by the organization. There are significant differences in the ability to control *internal* events as opposed to *external* events. Company "A" may experience a massive explosion and toxic vapor release that injures employees at the adjacent plant of Company "B." Investigators and managers at Company "B"

may not be able to change systems within Company “A” to prevent a repeat explosion and release. Therefore, Company “B” may have to limit the focus to those internal actions that *they can* undertake to mitigate the effects of the release. Mitigating activities such as alerts, alarms, evacuations, shelter-in-place procedures, training, personal protective equipment, or other emergency preparedness and emergency response actions all represent internal actions that Company “B” *can* reasonably address. Each investigation team would stop its tree development at the point where they no longer had control of the events.

The investigation team should document the truncation of branches and alternate cause scenarios that were disproved by the team. The investigation team may have to explain or defend its decision to reject certain potential cause scenarios. This explanation or defense may occur many months or even years after the conclusion of the investigation team activities, so adequate documentation is critical. The rationale for stopping should be recorded, such as:

- Other paths more productive
- Potential investigation by others
- Limit of scope of control

10.6 EXAMPLE APPLICATIONS

The following examples illustrate variations in the use of logic tree analysis:

- Fault tree supported by a fact/hypothesis matrix
- Use of historical data to identify potential causes

10.6.1 Fire and Explosion Incident—Fault Tree

The example process safety incident described in Appendix D can be used to illustrate the application of how a fact/hypothesis matrix can be used during logic tree development. Extensive details of the incident appear in the appendix; to summarize:

A major fire and explosion occurred in a polyethylene manufacturing facility, resulting in one fatality, five personnel injuries, and extensive damage. The fire originated in the catalyst area when a vessel was over-filled and the exit piping ruptured, releasing isopentane, a flammable material, and aluminum alkyl, a pyrophoric material. The first fireball, at approximately 11:10 AM, caused an operator fatality

and a contractor injury. Emergency response was impaired because the firewater pumps were inoperable, which contributed to the severity of the consequences. The fire spread to the vertical catalyst storage tank. A subsequent explosion of an adjacent catalyst storage tank resulted in the injury of four firefighters. The local fire department and plant fire brigade extinguished the fire at 12:10 PM.

For this example, the first event will be considered. The top portion of the tree for the operator fatality is developed in Figure 10.18.

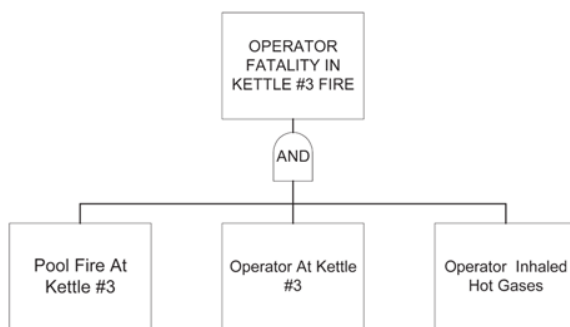


Figure 10.18 Operator Fatality Branch

The pool fire branch is further developed in Figure 10.19.

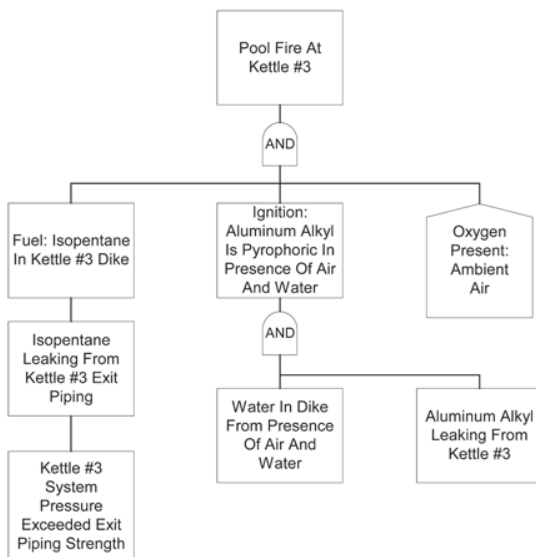


Figure 10.19 Fire Branch

At this point, the investigation team reaches a stage where they have more than one hypothesis for the reason the isopentane line ruptured. The pressure could have exceeded the design pressure for the pipe or the pipe could have failed at a point below the design pressure.

The team could use a simple fact-hypothesis matrix to decide which branch to pursue. An example matrix is shown as Figure 10.20.

Known facts→	Isopentane Pipe samples show external corrosion especially in heat affected zones	Pressure indicator on system went up to 120 psig.	Pipe samples found with split running along pipe	Maintenance records indicate correct material and schedule used for repairs	Area has clearly understood gasket chart
Possible Scenarios↓					
Design pressure of 150 psig vessel exceeded	NA	-	NA	NA	NA
Pipe/vessel failed below design pressure due to corrosion	+	+	+	NA	NA
Pipe/vessel failed below design pressure due to flange gasket failure	NA	+	NA	NA	-
Pipe/vessel failed below design pressure due to wrong material installed	NA	+	- samples were correct material	-	NA

Legend: (+) - the fact supports the scenario; (NA) - this fact apparently has no relation to this hypothesis, it neither supports nor refutes the scenario; (-) - the fact refutes the scenario; (?) - not enough information is currently available to decide on this fact

Figure 10.20 Fact/Hypothesis Matrix for the Kettle Exit Piping Failure

In this example, assume the team obtained pipe samples of some of the remaining pipe and finds evidence of external corrosion. The team concluded that the feed line failed due to higher than normal pressure combined with corrosion of the piping system (an AND-gate). These relationships are shown in Figure 10.21.

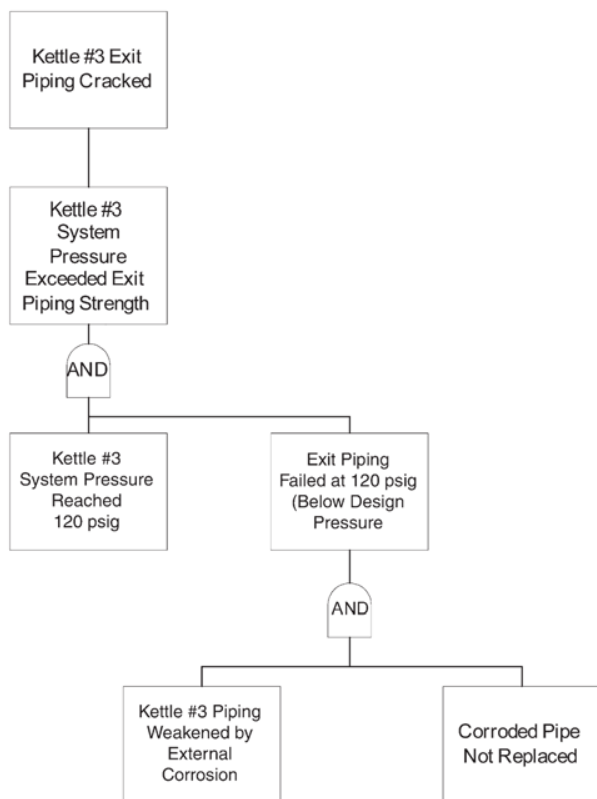


Figure 10.21 Exit Piping Crack Branch

What if the team was not able to obtain any physical evidence? They could use the absence of any corrosion inspection records plus knowledge of the expected corrosion (internal and external) of the system as an indicator of whether corrosion was a credible possibility.

With no evidence at all, the team might develop each hypothesis as a separate branch of the tree and try to address potential causes of corrosion, improper choice of materials, flange failure, or other items.

After collecting and analyzing the available evidence, the incident investigation team constructed the logic tree diagrams shown in Appendix D. These diagrams present, in a logical and systematic format, the sequence of events and conditions that ultimately resulted in the major incident. The simplified qualitative fault-tree indicates various events and conditions that

could have contributed to the incident causation and progression. Some of these sequences acted with direct impact on the trigger event, the pipe failing and initial fire, while others acted to increase the severity.

The incident investigation team's complete report is attached in the Appendix D, and details of the root causes are discussed. The root causes of the incident were related to several process safety management areas:

- Asset integrity and reliability
- Contractor management
- Emergency management
- Hazard identification and risk analysis
- Management of change

Take the time to review the complete example in the Appendix. Look at the trees and think about what the root causes might have been if the chosen top event had been the release of isopentane. Would the team have made a recommendation about escorting and training contractors?

10.6.2 Data-Driven Cause Analysis

Another approach to root cause determination is to use historical data to infer or identify potential causes. In this case, the investigators use past experience to look for patterns that support or refute failure hypotheses. The technique is only as good as the records, and if data have not been put in the files or are in error, then misleading inferences may result. In addition, if this type of event has not occurred before, the approach cannot be applied. Failure data for the system under investigation are presented in a timeline that can be correlated with overall plant history. Two types of evidence are sought:

- Evidence for correlation with plant state, plant condition, or external environmental effects.
- Evidence that indicates a failure pattern that may correlate with maintenance activities.

The following case study illustrates data-driven cause analysis using historical data to identify potential causes.

CASE STUDY:

In a plant with a shaft-driven boiler feed water pump, problems had historically occurred due to failure of the bearing in the hydraulic coupling. There was no specific failure mode identified; however, throughout the 12-year life of the equipment, the failure occurred about once every 1 or 2 years and resulted in an outage of about 3 weeks.

Plant data did not indicate a cause, other than bearing failure, with a notation that the bearing was repaired/replaced. A detailed root cause investigation had never been performed. When an investigation was eventually conducted, the equipment was operable, and detailed evidence from the last failure was lost during the repairs.

A timeline for the failures was developed and patterns sought. The first pattern noted was that failures seemed to occur predominantly following an outage in the winter. This immediately led to the thought that temperature was an important influence. The equipment is in a heated building so all components *should* have been at room temperature. If winter-time temperature was contributing to the problem, it was most likely a result of overcooling by one of the cooling systems or normal lubricating oil systems operating at too low a temperature. The written reports of the previous failures stated that “bearing wipe” was the cause. This fact indicated that lubrication failure was a likely candidate.

When the operational characteristics of the oil systems were examined in detail, it was found that the oil supply came from the main turbine lube oil system. The operators said that, after a start in cold weather, they had trouble maintaining greater than the minimum lube oil temperature of 120°F (49°C) until the turbine was at full power. The feed pump hydraulic coupling specifications indicated that a minimum temperature of 140–160 °F (60–71°C) was required for proper operation. A reasonable failure hypothesis was that, during a start, oil temperature was too low (and therefore the viscosity was too high) to provide adequate flow and lubrication of the pilot bearings. This allowed excessive frictional contact and resulted in a “wiped” bearing. The corrective action was to heat the oil feed to the coupling; this solution reduced the number of failures dramatically.

This example is intended to show that all of the elements of the cause determination process were used, but not quite so formally as the name of the methodology might imply. This is important, because different techniques achieve the intent of the process via specific but different

approaches. The investigator needs to understand the functional objectives that provide the foundation of the multiple cause determination. Without this understanding, a “shotgun approach” is often used, without rigor or a search for completeness. The first identified potential cause often becomes adopted by the investigation team as the cause, and the investigation terminates. This is one reason that failures recur although remedial action was taken after an earlier failure. There is also a tendency to stop the investigation process at the intermediate causes level. In the case study, the general cause of bearing wiping was lubrication failure. Suggested cures were proposed for bearing redesign, new materials, vibration monitoring, etc. Even modified bearings would be prone to continued failure following winter outages until low temperature was identified as a cause and corrected. For example, the underlying cause of the low temperature could be related to inadequate design practices, an error in installation, inadequate training, etc. The investigation team should also consider why previous investigations did not identify root causes.

10.6.3 Logic Tree Summary

Logic trees can be an effective means of identifying root causes. However, the technique requires skill, especially for complex, high risk incidents. One of the strengths of the logic tree method is that it creates a graphical aid for system analysis and management. Managers like the pictorial representation of system behavior and possible interactions, and for a complex system, it provides focus on the critical issues. Conversely, some background items might not fit easily in the tree, especially if they impact many branches. For example, human factors and cultural issues may be difficult to account for accurately. Table 10.2 illustrates some of the strengths and weaknesses of logic trees.

Table 10.2 Strengths and Weaknesses of Logic Trees

Strength	Weakness
Structured technique showing relationship between facts, causes & effects, and may expose non-obvious paths to failure	Requires skill as one poor/meaningless gate may invalidate the analysis
Shares some strengths of 5 Whys, e.g.: <ul style="list-style-type: none"> • If keep asking "Why?", can lead to underlying system defects • Can identify multiple root causes 	Shares some weaknesses of 5 Whys, e.g.: <ul style="list-style-type: none"> • Investigation team may stop too soon at a symptom or causal factor • Investigation team may stop at single root cause – requires persistence to seek multiple causes
Encourages "Out of the Box" thinking	Requires knowledgeable investigation team, otherwise the cause(s) is unknown
Shows simultaneous events & captures common mode failures	Can get bogged down in discussions about logic structure - requires a good facilitator
Suitable for simple and complex incidents	Logic can become complex and difficult to capture/follow in presentation format
	Can miss deep cultural issues
	No guidance for identifying human error issues

Further information and guidance on logic/fault trees is available from the following publications: *Guidelines for Chemical Process Quantitative Risk Analysis* (CCPS 2000); *Guidelines for Hazard Evaluation Procedures, 3rd Edition*, (CCPS 2008); *Root Cause Analysis* (Okes 2009); *Lees' Loss Prevention in the Process Industries* (Mannan 2012).

10.7 ROOT CAUSE DETERMINATION USING PREDEFINED TREES

The previous section detailed the use of the logic tree method. The second structured methodology discussed in this chapter involves timeline construction and identification of causal factors, followed by the use of predefined trees or checklists. This latter approach is discussed in detail below.

The following section presents a systematic discussion of the concepts and actions depicted in Figure 10.22.

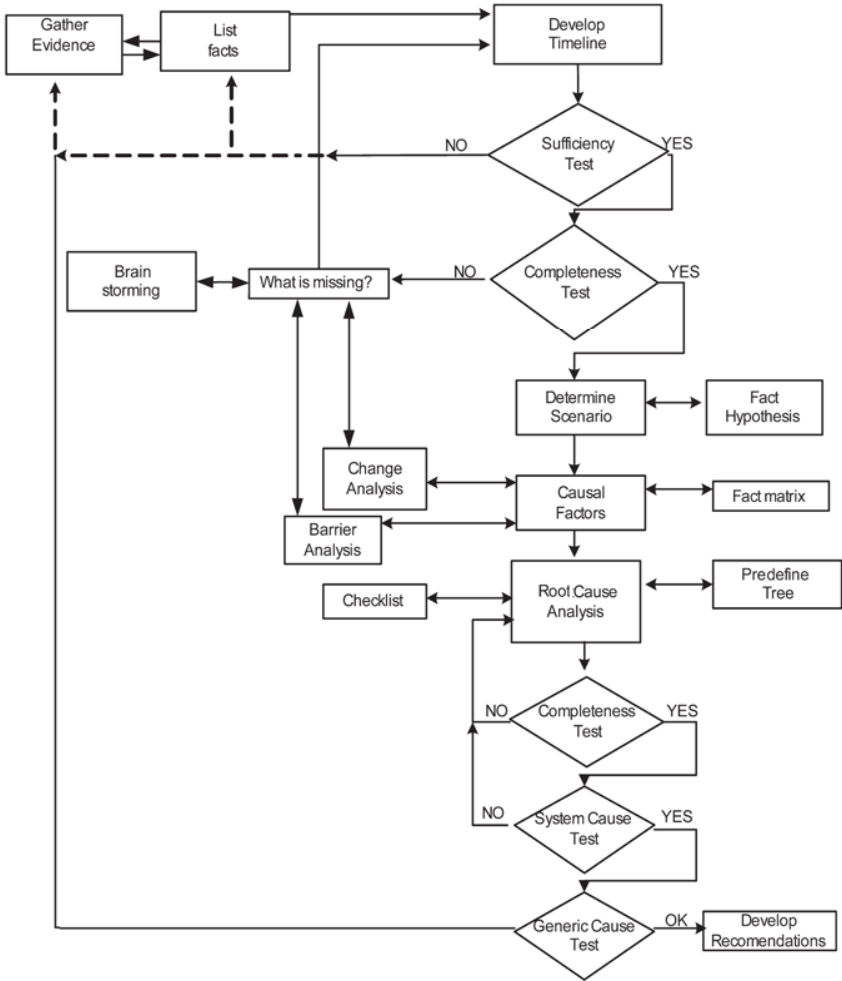


Figure 10.22 Flowchart for Root Cause Determination—Predefined Tree/Checklist

The initial tasks are similar to those of the logic trees previously described:

- The accumulation of facts, information, observations, insights, questions, and preliminary speculations gained from the evidence collection activities.
- The development of a chronology of events leading to the incident based on the available known times and sequences using a *timeline*.

These tasks have been discussed previously. The following represents a brief summary, but more detail about organizing data with a timeline is provided in Chapter 9

10.7.1 Scenario Determination

If there are two or more possible scenarios, it will be necessary to determine the actual incident scenario. In this situation, a fact/hypothesis matrix may be employed to help resolve conflicting facts. This is most efficiently performed prior to identifying the causal factors.

10.7.2 Causal Factors

Once the timeline or sequence diagram based upon the actual scenario has been developed, the next phase of the investigation involves identifying the causal factors. Causal factors involve human errors and equipment failures that led to the incident, but can also be undesirable conditions and failed barriers. The causal factors are the negative events and actions that made a major contribution to the incident. They can be identified by asking whether the incident would have occurred if each event on the timeline had not existed.

The process of evidence gathering, timeline development, scenario determination, and causal factor identification is somewhat iterative, and therefore some of the tools and quality tests previously described may assist in causal factor identification. More specifically, barrier analysis and change analysis, together with a completeness test, can ensure that all valid causal factors are identified.

10.7.3 Predefined Tree

The causal factors need to be examined further to determine why those factors existed. The investigation team may use a predefined tree to examine each causal factor individually. The first causal factor is analyzed, starting at the top of the tree and then working down all of the branches as far as the facts permit. When an appropriate subcategory on one of the branches is identified, it is recorded as a root cause. The remaining branches are checked, as one causal factor may have multiple root causes. The procedure is then repeated for each causal factor in turn.

Several quality assurance tests should be applied when using predefined trees. This is an important step because predefined trees are designed to capture most root causes, but they may not be comprehensive. A completeness check should be conducted on each branch of the tree to see if there are other root causes associated with the category of that branch that are not listed on the tree.

Some predefined trees do fully reach down to the root cause level. A system test should be applied to each identified root cause to ensure that it relates to a management system failure. By applying the 5-Whys tool to each cause identified at the end of the relevant branches of the tree, the investigator can determine if another underlying cause can be identified.

After the predefined tree has been used, a final generic cause test should be applied. The plant operating history, especially previous incidents, is considered to indicate if other generic management system problems exist. For example, repetitive failures may indicate generic causes that would not be apparent by only investigating the current incident. It is also an opportunity for a final overall review of the investigation to focus on the big picture, not just individual facts or causal factors. The team should ask, *“Are there any other causes that anyone has in mind that have not been included?”* If the incident investigation team is satisfied with the root causes identified, then the investigation proceeds to the recommendation stage. If a problem or some incompleteness is noted, then an iterative loop is followed.

10.8 USING PREDEFINED TREES

Once the actual incident scenario is understood and its multiple causal factors identified, this information may be used to determine the incident’s root causes. One means of performing root cause analysis involves the use of ready-made, predefined trees. A predefined tree provides a systematic approach for analyzing and selecting the relevant elements of the incident scenario. It is a deductive approach, looking backward in time to examine preceding events necessary to produce the specified incident.

Predefined trees contain a relatively complete list of potential root causes organized by subject matter, such as equipment failure, safe work practices and human error, into various categories and subcategories in a hierarchy of branches and sub-branches. Although the trees do not display any logic symbology, each of the nodes between branches and sub-branches represents an OR-gate. An example of a section from a proprietary predefined tree is shown in Figure 10.23.

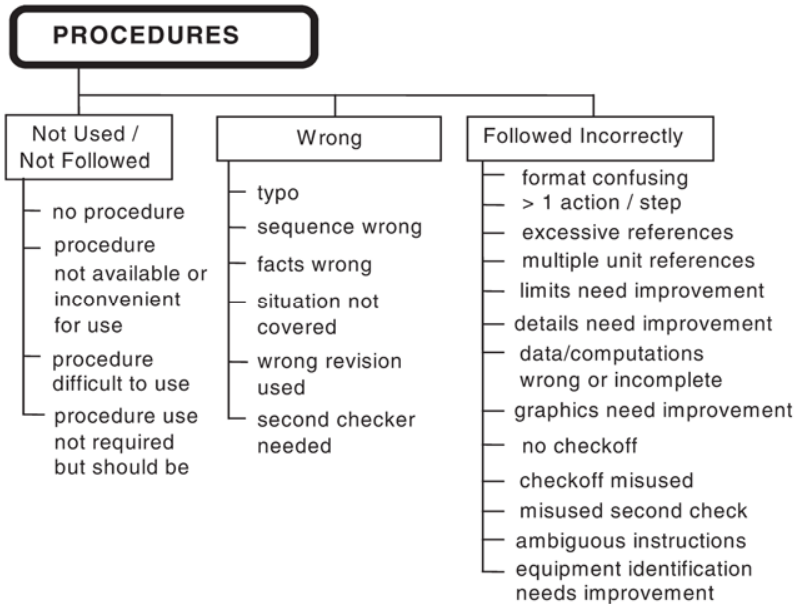


Figure 10.23 Example of Root Causes Arranged Hierarchically within a Section of a Predefined Tree (Paradies, 2016)

Unlike the procedure followed in developing logic trees, the investigation team does not construct the tree. Rather they apply each causal factor to each branch of the predefined tree in turn, and those branches that are not relevant to the incident are eliminated. This prescriptive approach offers consistency and repeatability by presenting different investigators with the same standard set of possible root causes for each incident.

The consistency offered by predefined trees with standard categories and subcategories of root causes also facilitates statistical trend analysis. This allows an organization to more easily collect and analyze data from the investigation of incidents and near misses over a period of time to determine any trends not apparent from single incidents. Some organizations deliberately structure the root cause categories and subcategories along the lines of their management system in order to focus on common system issues.

While the use of predefined trees does not directly challenge the investigation team to think laterally of other possible causes, many predefined trees present a wide range of causes, some of which the team may not have otherwise considered. It is therefore possible that the incident could involve a novel root cause that was not previously experienced by those who developed the predefined tree. The addition of a final test based on another tool, such as brainstorming, can overcome this potential weakness

10.8.1 *Predefined Tree Methodology*

Although there are differences between various predefined trees, the basic method to perform a root cause analysis using the trees is similar, whichever tree is used. The following basic steps apply:

1. First, it is necessary to identify the multiple causal factors of the incident. The procedures in Chapter 8 (Section 8.4-Timelines and Sequence Diagrams) may be used to identify the causal factors from a timeline or sequence diagram.
2. The first causal factor is then analyzed, starting at the top of the predefined tree and working down the branches as far as the facts permit. If the category of a particular branch appears to be an appropriate cause of the incident, the branch is followed to successively lower levels until a subcategory is identified as an

appropriate root cause. (*Note:* In some circumstances, the facts may not allow root causes to be identified without further investigation.)

3. All branches and sub-branches should be considered because an individual causal factor can have more than one root cause.
4. As each branch is considered, the investigator should ask if there are other root causes associated with that category that are not listed on the tree. The team should ask, "Are there any *other* causes that anyone has in mind that have *not* been identified?" (Predefined trees are designed to capture most, but not necessarily all, root causes.)
5. The procedure (steps 2 through 4) is then repeated for each causal factor, in turn.
6. When all the root causes have been identified from the tree, the investigator should ask *why* to each one in turn as a test to ensure that they are really underlying root causes. If it is possible to identify a lower level cause, this lower-level cause should be recorded as the root cause. (*Note:* This is analogous to applying the 5 Whys.)
7. Finally, the investigator should consider other generic causes of the incident that are not identified by the predefined tree categories. For example, the investigator should consider the plant operating history. Other incidents may indicate repetitive failures that may indicate generic management system problems.

Predefined trees are relatively easy to use and generally require less training and effort to conduct root cause analysis than logic trees.

10.8.2 Example—Environmental Incident

The following is an example of the use of a predefined tree to analyze an environmental incident. While the structure (number of branches and levels) and terminology of predefined trees vary, this example demonstrates the basic method.

During a normal night shift at a process plant, a temporary water treatment unit, operated by contract personnel, overheated and released hot, low pH water to one of the plant's outfalls. This

release ultimately resulted in fish being killed in the local river. The overheating of the temporary water treatment unit occurred when a firewater hose providing cooling water to the temporary water treatment unit ruptured. The plant was provided with an automatic trip that apparently failed to work, as well as an alarm to which the operator did not respond.

The sequence of events is shown in Figure 10.24.

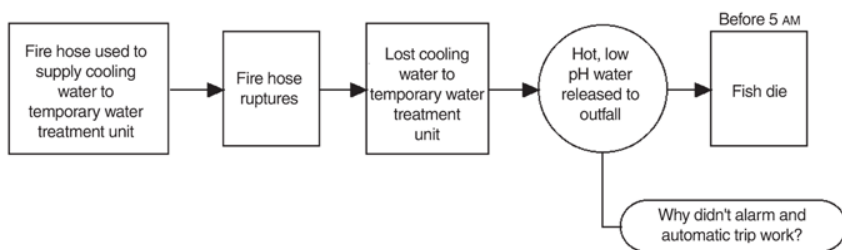


Figure 10.24 Incident Sequence

The investigation team interviewed all contract operators and their supervisor, the temporary water treatment unit vendor’s engineers, plant personnel at the process plant unit, procurement personnel, and operations management.

10.8.2.1 Causal Factor Identification

After the interviews and other evidence gathering activities are complete, the causal factors should be identified and, if appropriate, a causal factor chart can be developed.

Four causal factors were identified:

1. Contract operator falls asleep
2. Fire hose ruptures
3. Automatic shut-off jumpered
4. Sleeping contract operator can’t hear alarm due to nearby diesel (noise)

Each of the causal factors can now be analyzed for its specific root causes using a predefined tree, as shown in Figure 10.25. The causal factors are indicated by black triangles.

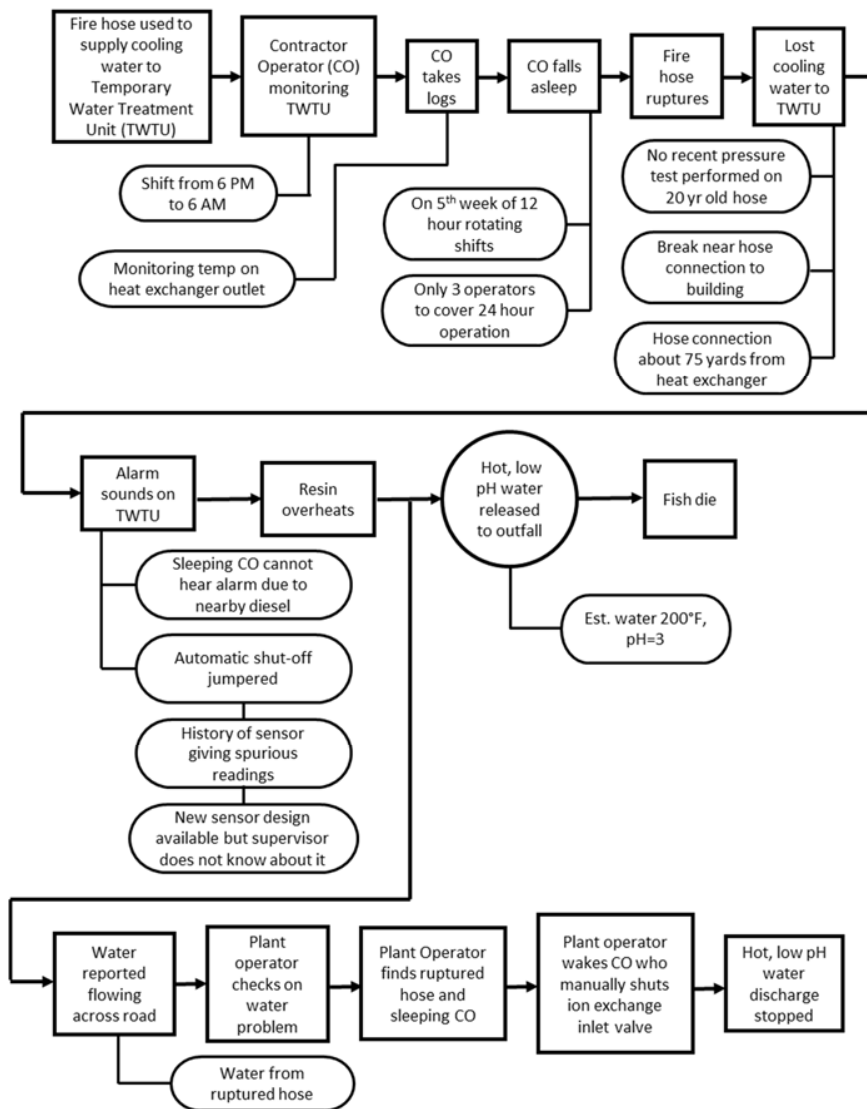


Figure 10.25 Complete Causal Factor Chart for Fish Kill Incident

10.8.2.2 Analyzing a Causal Factor

The following is an analysis of one of these causal factors: contractor operator (CO) falls asleep. The basic technique works with any of the predefined trees commonly used within the process industry. However, for the purposes of this example, a proprietary tool (Paradies, 2016) has been selected, and therefore the structure of the tree and the terminology used is specific to that tree.

To analyze the causal factor, the investigator starts at the top of the tree and works down the tree through a process of selection and elimination. The investigator asks and answers questions to identify the specific root causes for the causal factor.

In this case, the causal factor (contract operator falls asleep) is identified as a Human Performance Difficulty (one of the four major problem categories at the top of the tree, see Figure 10.26), and the other three categories are discarded. (Different predefined trees use different terminology and structure, but generally cover similar choices.)

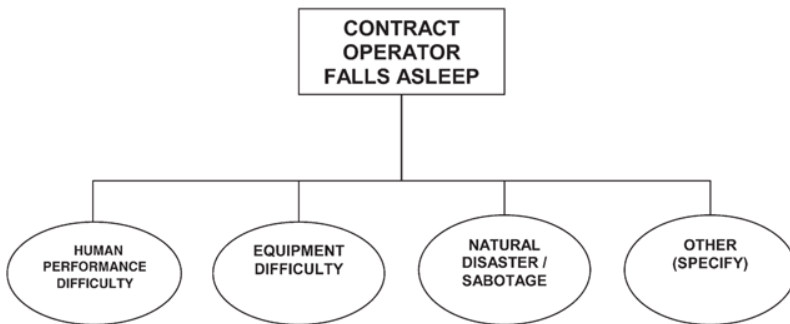


Figure 10.26 Top of the Predefined Tree

The investigator then follows the Human Performance Difficulty category through a series of questions (or subcategories). These questions help the investigator identify which of several human performance related branches (sometimes known as basic causes) to investigate further. (Some predefined trees use statements rather than questions, but the selection process is similar.

The human performance related branches are:

- Procedures
- Training
- Quality Control
- Communications
- Management System
- Human Engineering
- Work Direction

Each branch is investigated further to see if it is relevant; that is, if one or more related root causes contributed to the problem. If it is not relevant, the branch can be eliminated.

In the case of the fish kill incident, the first of the questions, shown in Figure 10.27, is answered YES because the contract operator was considered to be both fatigued and bored. This indicates that the cause may be related to Human Engineering and/or Work Direction.

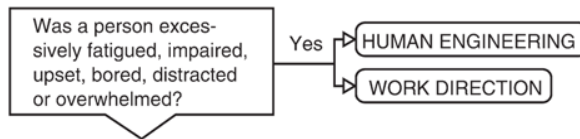


Figure 10.27 First Question of the Human Performance Difficulty Category

A different predefined tree may express this question as one or more simple statements, such as:

- Rest/sleep less than adequate (fatigue)
- Attention less than adequate

However, the basic method is similar.

When all the questions on the Human Performance Difficulty category are answered, the following branches of the tree are indicated for more investigation:

- Human Engineering
- Work Direction
- Management System
- Procedures

Figure 10.28 illustrates one of these branches, Human Engineering, showing three levels of the tree, designated as *basic cause*, *near-root cause*, and *root cause*. (Note that other trees may use different terminology for these levels, although “root cause” is a common term.)

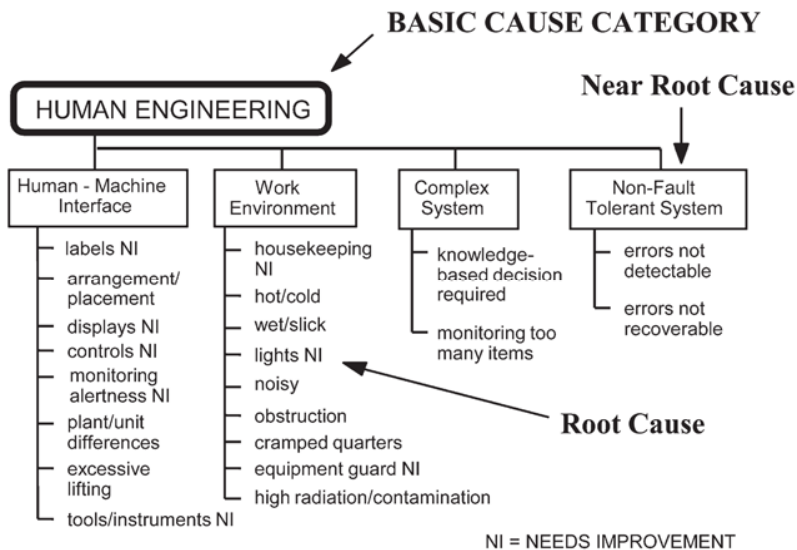


Figure 10.28 Human Engineering Branch of the Tree

Each lower sub-branch (near-root cause) is then considered in turn to determine if any of the potential root causes on that sub-branch is a valid reason for why the causal factor existed at the time of the incident. Valid root causes are recorded and invalid causes are eliminated.

In the Fish Kill example, the completed analysis of the Human Engineering branch is shown in Figure 10.29. Under the Human-Machine Interface sub-branch, *monitoring alertness needs improvement* is selected as a valid root cause, and the remaining subcategories have all been discarded.

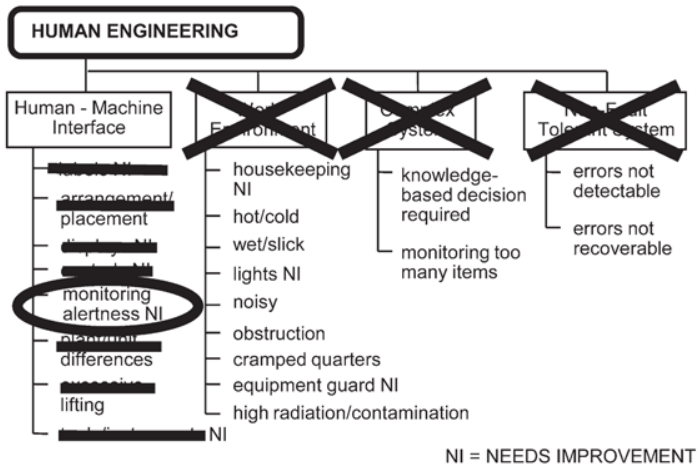


Figure 10.29 Analysis of the Human Engineering Branch

When the first causal factor is analyzed using the remaining applicable branches (i.e., Work Direction, Procedures, and Management System), the following root causes are identified:

1. Monitoring alertness needs improvement.
2. Shift scheduling needs improvement.
3. Selection of fatigued worker.
4. The “no sleeping on the job” policy needs to have a practical way to make it so that people can comply with it.

The investigation team then repeats the process by considering the remaining causal factors one at a time:

- Fire hose ruptures
- Automatic shut-off jumpered
- Contract operator cannot hear alarm due to noise

Finally, the investigation team considers generic causes that pertain to the overall management system for the process plant by considering the operating history and any other incidents that may have related causes.

Once all of the root causes are identified, the investigator is ready to develop the corrective actions, as described in Chapter 12.

10.8.2 Quality Assurance

There are a number of quality assurance checks that should be considered when conducting an incident investigation using predefined trees. Most of these checks have already been discussed, although it is useful to review them as they relate to the predefined tree approach.

Predefined trees are designed to capture root causes, but the predefined tree may not necessarily be comprehensive enough to identify *all* root causes. It is therefore necessary to conduct another *completeness* test. As each branch of the predefined tree is considered in turn, the investigator should ask if there are other root causes associated with that category that are not listed on the tree.

The 'root causes' identified by applying the causal factors to a predefined tree should be subjected to a *management system* test to ensure that they are management system failures. Some predefined trees are quite detailed, while some proprietary trees do not fully reach the underlying root cause level. The system test essentially applies the 5-Whys tool to each cause identified at the end of the relevant branches of the predefined tree. Typically, the team may need to ask "why?" a number of times to reach underlying root causes.

After the root causes have been identified, a *generic* cause test should be applied. By considering the plant operating history, especially other incidents that may indicate repetitive failures, the investigator may identify other generic management system problems. These generic causes would not necessarily be apparent from investigating the latest incident alone.

10.8.3 Predefined Tree Summary

Predefined trees are a convenient means of identifying root causes. Providing all of the causal factors have been determined correctly, use of a comprehensive predefined tree should ensure that most, if not all, root causes are identified, especially if the management system test is performed. Several other quality assurance tests should help identify any remaining root causes. Table 10.3 illustrates the strengths and weaknesses of predefined trees.

Table 10.3 Strengths and Weaknesses of Predefined Trees

Strength	Weakness
Structured, systematic technique for evaluating barriers	Requires skill as selection of poor/meaningless causal factor may invalidate the analysis
Simple, easy to teach and use	
Some predefined trees are very comprehensive & identify weaknesses in specific barriers and management systems	Can be insufficient in finding specific causes as some trees focus on general causal areas & lack detail
Can identify multiple root causes	Investigation team may stop at single root cause – requires persistence
Although best with knowledgeable investigation team, predefined tree may alert team to issues outside of their expertise	Requires “Out of the Box” thinking of issues not in the tree
Repeatable if causal factors correctly selected	Some predefined trees alone do not reach underlying root causes - Investigation team may stop too soon at a symptom or causal factor
Can be effective in identifying underlying root causes – some predefined trees are best used in combination with 5 Whys	
Applicable to all incidents including complex, high risk incidents	Some predefined trees are weak on process safety and focus on occupational safety

Several public and proprietary predefined trees are available for use, although the comprehensiveness of the different trees varies. Some do not fully reach root causes (i.e., management system weaknesses), while others are very detailed with numerous categories and sub-categories. The results from some predefined trees would benefit from the application of the 5 Whys technique to reach the underlying root causes.

10.9 CHECKLISTS

Checklists of varying content and detail are used in incident investigation methodologies as a user-friendly tool to assist root cause analysis. Sometimes a comprehensive checklist may be used as the primary root cause analysis tool; alternatively, a checklist may be simply used to supplement another primary tool.

Another situation where checklists can be very helpful is when the investigation team has no hypothesis as to what caused an occurrence. The checklist is an example of an inductive approach that can be used to get past a mental block.

Checklists used for process safety incident investigation share many similarities with predefined trees. They can comprise a series of questions or statements related to root causes based upon experience of safety management systems. Some checklists need care in use because the statements that they contain can infer blame to the casual observer, rather than discourage blame-seeking. Checklists also offer consistency and repeatability by presenting different investigators with the same standard set of potential root causes for each incident. This consistency facilitates statistical trend analysis of multiple incidents involving recurring problems within an organization.

While a checklist may not encourage the investigation team to think laterally of other potential causes, it can overcome a lack of experience within the team and present causes that the team would not have otherwise considered.

10.9.1 Use of Checklists

The use of checklists as a primary root cause analysis tool is virtually identical to the use of predefined trees. This is hardly surprising as most predefined trees are really a succession of checklists organized by subject matter (category) into an arrangement of branches within the tree.

A timeline or sequence diagram is first developed, and then causal factors identified. Care should be taken to ensure that the checklist is not used too early. Be sure to determine *what* happened and *how* it happened before determining *why* it happened. Otherwise, the team will think that they have identified the right root cause(s), when in reality only one or two of several multiple causes have been determined. The causal factors are then applied one at a time to each page of the checklist(s) to identify relevant root causes. Those pages that are not relevant to the particular incident of interest are discarded. Similar quality assurance checks should be applied as those described for predefined trees.

The use of checklists to supplement another root cause analysis method can be an effective technique; for example, human factors checklist(s) may be used in conjunction with logic trees. The checklist may be used as a guide during development of a logic tree, or as a check after the tree has been

developed. The checklist essentially acts as a memory jogger to direct the investigation team. This is especially helpful if the team lacks previous experience in the subject matter. However, care should be taken to apply the checklist to a causal factor and not to the incident as a whole. As with any root cause analysis technique, the investigator should avoid assigning blame and seek management system weaknesses that allowed the incident to occur.

Checklists may also be used in combination with structured brainstorming tools, such as What If Analysis (CCPS, 2008).

10.9.2 Checklist Summary

Checklists represent a root cause analysis tool that has similar advantages to, and ease of use as, predefined trees. They also share similar weaknesses as predefined trees (Table 10- 3).

A variety of public and proprietary checklists are available that vary in comprehensiveness. There is no reason for an organization to start from scratch in developing a checklist. A human factors checklist and tables are included in Chapter 11. Examples of checklists that can be modified for the readers use are included on the CCPS website.

10.10 HUMAN FACTORS APPLICATIONS

Investigators are discovering that an increasing number of failure causes are related to inadequately addressing human factors or the relationship of the human to the machine/system. Human factors is a discipline concerned with matching the system to human capabilities and limitations. A mismatch leads to human performance deficiencies that often result in repeated incidents.

There is an opportunity to improve process safety management performance by improving human performance and human reliability. Although technology advances have resulted in increasingly complex and highly automated processes, the facilities do not run themselves. Proper operation requires periodic and sometimes constant intervention from humans. System designers are now realizing this and are considering the expectations placed on the operator by management and the physical systems.

The following example illustrates the importance of correcting weaknesses that led to human error by an individual:

If a component fails because of a human error, “counseling” the worker may prevent him or her from performing the same error again, but what of the other members of the operating crew? Conditions that led to the original failure remain, so others are still prone to committing the same error. Many repeat occurrences could be avoided if the correct information and reasons for those errors are uncovered by the investigation team and (1) corrected and/or (2) communicated to others who might also be at risk of committing them.

Structured root cause analysis uncovers the underlying reasons for human error and consequently provides guidance on suitable corrective actions. Humans make errors, so it is important to design systems that detect and correct an error before it leads to a serious consequence. Chapter 11 provides extensive information related to human factors that is applicable to root cause analysis.

10.11 SUMMARY

The success of the cause analysis is a direct function of the quality of available and discovered information as well as the perceptiveness of the incident investigation team. The goal of the cause analysis is to find the information needed to determine cost effective and practical preventive measures.

Simple and minor incidents may be satisfactorily investigated using the 5 Whys methodology, providing its inherent weaknesses are understood and appropriately managed. It may also be used to supplement other techniques.

For more complex events, the use of more structured methods, such as the logic tree and predefined tree techniques, can ensure that multiple underlying root causes can be found. By applying the iterative loop, testing the facts, and systematically applying quality control tests, incident investigators can uncover the multiple underlying causes that could otherwise result in future incidents.

11 THE IMPACT OF HUMAN FACTORS

“For a long time, people were saying that most accidents were due to human error and this is true in a sense but it’s not very helpful. It’s a bit like saying that falls are due to gravity.”

—Trevor Kletz

Humans are involved in all aspects of the workplace. Humans manage facilities, design equipment, operate equipment, and maintain equipment. Yet historically, incident investigators have overlooked or provided cursory treatment of human factor contributions to incident causation. Contributions made by mechanical issues related to pressure vessel failures, pipe leaks, process upsets, mitigation system malfunctions, etc. are often readily identified. However, the real difficulty is to answer *why* these deficiencies occurred, and the answer is often related to human behavior. For instance, a broken shaft may be obvious but to identify *why* the shaft broke may involve more rigorous examination. Were company inspection, material selection, operational controls, production procedures, standards, priorities, etc. contributing factors? The shaft may have broken due to poor supervision of operations or maintenance procedures, an engineering design that made it all but impossible to inspect the shaft, material selection that is no longer compatible with current production rates, etc. All underlying factors should be probed for *why* it happened. Meaningful solutions can be developed only after the investigator understands the true underlying causes. In many investigations, however, the *why* as it relates to human factors is sometimes underdeveloped.

Incident investigation teams should attempt to determine what management system improvements could be made to remedy the particular human performance problem associated with the incident under investigation. Oversimplifying a human performance to “human error” is an easy mistake to make but can be avoided if proper technique is used. In almost every case, there are underlying reasons for the human performance beyond the simple assumption that the worker failed to follow procedure. A system failure, design flaw, incorrect procedure, workload imbalance, or training deficiency may be the foundation of the performance problem. A good root cause identification process should identify the underlying reasons. A good investigation recommendation seeks to set up the human for future success.

Historically, investigations have attempted to identify causal factors. This has helped ensure that specific cause is not repeated, preventing accidents. However, if the investigation root causes include human factors, then the identified issues that prompted the human performance for that incident when addressed will apply to those for other potential incidents with similar performance requirements. This potentially prevents many more incidents. It can also improve employee morale, increase productivity, and complement positive cultural change. This chapter addresses the following human factors topics:

- Human factors concepts
- Incorporating human factors into the incident investigation process

11.1 HUMAN FACTORS CONCEPTS

The term *Human Factors* is defined differently by various organizations. The CCPS glossary defines human factors as:

“a discipline concerned with designing machines, operations, and work environments so that they match human capabilities, limitations, and needs. Includes any technical work (engineering, procedure writing, worker training, worker selection, etc.) related to the human factor in operator-machine systems” (CCPS, 2018).

The UK Health and Safety Executive (HSE, 1999) defines it as:

“environmental, organizational and job factors, and human and individual characteristics which influence behaviour at work in a way which can affect health and safety.”

A common model for human factors in the process industries is shown in Figure 11.1. This model is included in the CCPS book *Human Factors Methods for Improving Performance in the Process Industries* (CCPS, 2007) and is based on the IOGP model (IOGP, 2005).

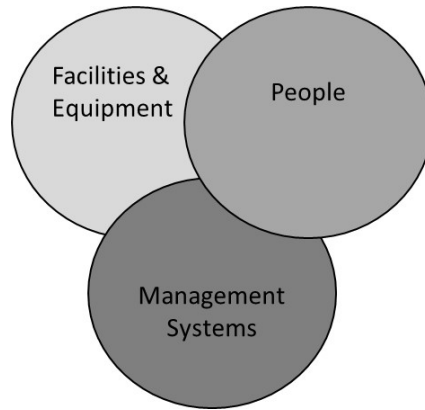


Figure 11.1 Common Human Factors Model (CCPS, 2007)

Workers interact with facilities and equipment and management systems every day. Human performance problems are typically the result of these complex interactions.

Facility designers should strive to design equipment to meet workers' expectations, which may vary throughout the world. For example, to turn on a light switch in the US, the switch is pushed up, but to turn it on in Europe it is pushed down. Color-coding schemes may vary from plant to plant. The best approach is to ask the end users about any local practices for equipment operation.

A good human factors design is important. For most normal operating conditions, the human operator can cope with the incremental additional mental load of inconsistencies. During emergencies or other high-stress periods, however, each additional mental task is an opportunity for error.

Examples:

1. *Conforming to certain expected conventions and meeting normal patterns of actions and habits can enhance human performance. The incident investigation team should be alert for built-in design deviations from normal conventions.*

In some countries, people expect the hot water tap to be on the left side and the cold water on the right side. When this is not the case, they can become confused and make mistakes. Rising-stem gate valves are expected to close if the handle is turned in a clockwise

rotation and to open if the handle is turned counterclockwise. Deviating from normal convention, expected actions, and established habits can be an underlying cause of human error.

2. Over time, minor modifications and changes can individually or collectively cause human performance problems.

A fourth pump was added to a group of three existing pumps. In the field, the fourth was added in sequence alongside pump C. The arrangement was A-B-C-D. However, there was no room on the control board for the new switch to be added after the "C" switch, so it was added beside the "A" switch where there was space (Figure 11.2). Consequently, in the control room the corresponding switches were configured in D-A-B-C sequence. In an emergency, the operator could easily mistakenly flip the first switch (the new "D" switch) thinking it is the familiar "A" switch in that position. This ergonomic trap proliferates as time goes on and changes are made without consideration for operator habits, tendencies, and normally expected actions.

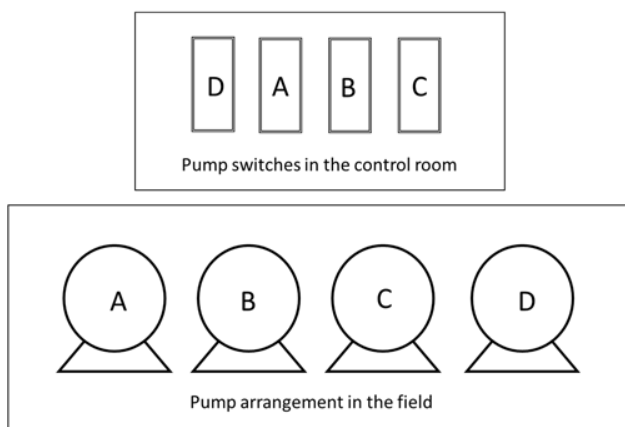


Figure 11.2 Example of Poor Pump and Switch Arrangement

It may be helpful to use examples to illustrate how human factors appears in the workplace and how it may play a part in incidents. Building on the model in Figure 11.1, topics in each of the three areas (CCPS, 2007) are listed along with examples of how human performance may be affected.

Facilities and equipment affect:

- Process equipment design – a person’s ability to reach or operate equipment
- Process control systems – an operator’s trust of a system will be greater if it operates well without nuisance trips
- Control center design – the ability of the operator to see all the needed data
- Remote operations – the operator’s ability to control operations is greater with good infrastructure and logistical support
- Facilities and workstation design – the response of the worker, in that designs conforming with cultural and local norms are more likely to be operated as intended
- Human computer interface – the human’s decision-making and troubleshooting ability is greater when critical alarms are prioritized and displays are consistent
- Safe havens – an operator’s ability to control a process during an emergency from a safe location depends on infrastructure of that safe haven
- Labeling – the operator or maintenance technician to positively identify equipment as opposed to relying on memory or assumption

Management systems affect:

- Safety culture, including rewards/punishments and individual/organizational goals – the way everyone on the site will work and where they will place priority
- Behavior based safety – the importance the workers place on working safely
- Project planning, design and execution – the clarity people will have on the work priorities, their role in the work, and the support available
- Procedures and other such documentation – directly the way the tasks are completed
- Maintenance – the completion of tasks and returning equipment to

normal mode

- Safe work practices and permit to work systems – the attitude of a worker toward safety as a priority
- Management of change – a person's understanding on what is a change and what level of hazard assessment may be warranted for a change
- Qualitative hazard analysis – a person's understanding of what hazards are present
- Quantitative risk assessment – a person's interpretation of the level of importance the company puts on evaluating risks and what risks are not tolerable
- Safety systems – a person's diligence in using these systems may depend on how well the company controls and maintains them
- Competence management – a person's capability to perform the job
- Emergency preparedness and response – a person's understanding of what is expected of him and what actions are appropriate for him to take in an emergency
- Incident investigation – whether or not human factors issues involved in an incident are investigated and understood

The **People** aspects include:

- Training – a person's knowledge of what is expected in performing the job
- Communications – a person's clear understanding of the instruction
- Documentation design and use – a person's understanding of intended operations
- Environmental factors – human performance as the human operates well in a fairly narrow range of temperature, sound level, lighting level, agility
- Workloads and staffing levels – a person's individual performance as well as the team performance
- Manual materials handling – the human's ability to handle the material without personal injury

Incident investigators should be alert for human performance problems caused by a mismatch between the system design and reasonable expectations of human performance. Sometimes the designers of chemical

processing systems fail to consider reasonable human capability limits and patterns of habit. The result can often be a system that promotes human errors rather than discouraging them. Donald Norman addresses these mismatches comprehensively in the book *The Design of Everyday Things* (Norman, 1988).

Human performance problems occur several ways. Reason outlined several types of involuntary or unintentional human actions (Reason, 1990). The Skills, Rules, Knowledge (SRK) model was developed by Rasmussen (Rasmussen, 1983) to help designers combine information requirements for a system and aspects of human cognition. As an investigator uses tools such as 5 Whys to identify potential root causes, considering these models can help focus in on specific areas for improvement to support the desired human performance.

11.2 INCORPORATING HUMAN FACTORS INTO THE INCIDENT INVESTIGATION PROCESS

As stated at the beginning of this chapter, humans are involved in all aspects of the workplace. In addition to managing, designing, operating, and maintaining, this also includes investigation and learning. Thus, nurturing a blame-free, open culture within an organization is essential for the success of the incident investigation process. The investigation must focus on understanding:

- What happened?
- How did it happen?
- Why did it happen?
- What can be done to prevent it from happening again?
- How can the risk be reduced?

There are a number of references specifically addressing human factors as related to incident investigation that the reader may find useful. Two of note are the Energy Institute's "Learning from incident, accidents and events" (EI, 2016) and the International Association of Oil & Gas Producers' "Demystifying Human Factors: Building confidence in human factors investigation" (IOGP, 2018).

11.2.1 Human Factors Before and During the Incident

Leadership sets the tone on the importance of incident investigation and learning from incidents. Leaders and investigators are not out to assign blame. Actions taken to “blame and shame” are not constructive and generally do little to prevent similar incidents from occurring. Therefore, it is necessary to foster an open and trusting environment where people feel free to discuss the evolution of an incident without fear of reprisal. Without such a supportive environment, involved individuals may be reluctant to cooperate in a full disclosure of occurrences leading to an incident (Rothblum, 2002) and the incident investigation may be concluded prematurely with the root causes left uncovered.

Example:

“An incident involved a control board operator, who was an introvert and had few, if any, friends at the workplace. Other members of the crew apparently played jokes at his expense. One day, the board operator closed a valve in error, whereas another crew member monitoring the process understood the error but intentionally delayed communication of the error to the board operator. By the time the crew member rudely informed the board operator of his error, it was too late to prevent the incident. It was also found that the board operator spent considerable time on non-work-related telephone calls while the process was out of control.” (Broadribb, 2012)

Operational discipline is a very important topic in human factors and process safety. Operational discipline is not about punishing a worker who may have made an error. Instead, it is about enabling people to perform every task correctly every time. (CCPS, 2011) This is done by clearly defining how processes will be managed providing needed resources and establishing clear expectations for following the procedures. This operating discipline is supported by leadership, organization, communication, teamwork, resourcing, and documentation. These topics may underlie why a human has behaved in a certain way. Topics relating to operational discipline are included in Table 11.1 listing potential human factors issues.

Human factors issues can also impact the performance of the investigation team itself. They may be subject to human biases that will lead them to assume they know what happened or to rely on judgements already established about the persons involved in the incident. (IOGP, 2018) It is

important that the investigators rely on facts based on evidence in developing the incident scenario.

Example:

“On arriving at the site of a major incident, an investigator was informed by a local manager that data from the control room were useless as the instrument air to the pneumatic instruments had failed during the ensuing fire. Ignoring this advice, the investigator studied the data and was able to exactly determine all process parameters at the time of the incident, which ultimately confirmed a different scenario from that being supported by local management.”
(Broadribb, 2012)

11.2.2 Human Factors during the Causal Analysis

“Failure to follow established procedure” is a common premature stopping point for incident investigation related to human factors. In many cases, the investigation team identifies the fact that a person failed to follow established procedures, then does not attempt to investigate further and determine the underlying reason for the behavior. In most cases there is an underlying correctable root cause that should be identified and fixed. The *failure to follow established procedure* behavior on the part of the employee is not a root cause, but instead is a symptom of an underlying root cause and warrants further root cause analysis. For example, if an employee failed to follow an established *correct* procedure, the root cause may involve training. However, if the employee failed to follow an established *incorrect* procedure, this would be a symptom of a root cause involving the development of procedures.

Chapter 10 addresses root cause analysis in detail.

The investigation team has an obligation to try to find the underlying cause for the *failure to follow established procedure* behavior. Typical symptoms and corresponding underlying system defects that can result in an employee failing to follow procedure include:

- Out-of-date written procedure that no longer reflects current practices or current configuration of the physical system, **due to** defects in the process safety information, or operating procedures management systems
- Employee perceives that his or her way is better (safer or more effective), **due to** deficiencies in the system for establishing and

- maintaining a specific competency and qualification level or effective operational discipline
- Employee previously rewarded for deviating from the procedure, **due to** a culture of rewarding speed over quality, resulting from and reflecting a defective quality-assurance management system and a defective operational discipline system
 - Employee following personal example set by his supervisor, **due to** a defective system for establishing and maintaining supervisory performance standards or operational discipline
 - There are multiple accepted practices (daytime versus weekends for example), **due to** the presence of dual standards, **due to** defects in the supervisory or auditing management systems or operational discipline system
 - Employee is experiencing temporary task overload, **due to** defects in the scheduling and task allocation system, and/or **due to** ineffective implementation of downsizing
 - Employee has physical/mental/emotional reason(s) that causes him or her to deviate from the established procedure, **due to** defects in the fitness-for-duty management system
 - Employee believed he was using the correct version of the procedure, but **due to** defects in the document management system, he was using an out-of-date edition
 - Employee was improperly trained **due to** defects in the training system
 - Management's expectations for procedure use. Depending on the complexity of the process and the activity, a procedure could be written with the intent that it be followed at a detailed level or it could be written for training and reference. Consequently, the procedure type/style could also be a defect.

In some instances, the *failure to follow established procedure* may be due to inadequate knowledge. The classic recommendation that accompanies this symptom is to provide training (or refresher training) to ensure the person understands how to follow the established procedure. An example of a typical recommendation associated with this mistake is "review the procedure with the employee to ensure that he understands the proper action expected." The training activity may be beneficial to the person(s) who receive it, but in most cases, the training fails to identify and address the underlying cause(s) of the deficiency in the knowledge/competency system

that resulted in the person failing to follow the procedure. In many cases, the other employees may also remain inadequately trained.

James Reason offered another useful model, often referred to as the “Swiss cheese model” (Reason, 1990), that explains how the many factors can converge to result in an incident. A company tries to prevent catastrophic incidents by putting into place layers of system defenses, barriers, depicted as slices of Swiss cheese. This model recognizes that each barrier has weaknesses or holes.

The Energy Institute (EI, 2016) in their document, “Learning from incidents, accidents, and events” has built on this model illustrating how the human, being affected by the environment (facilities and equipment and management systems), interacts with these barriers. This is shown in Figure 11.3. The addition of the perpendicular tangent illustrates moving from causal factors to underlying (root) causes.

- Barriers may be physical barriers such as a bund or a safety device or administrative barriers such as procedures and permits-to-work.
- Barriers fail due to human action or inaction or the human decision that created an unsafe condition. These causes may also have been made by engineers or supervisors in the past that came to light in the incident.
- There are factors, either psychological or situational, that influence the human’s behavior at the time of the incident. These are sometimes referred to as performance influencing factors (PIFs). Annex C of the above-mentioned EI document includes a list of PIFs. The existence of such a factor does not mean that a causal factor will happen; it means that there is an increased likelihood that the causal factor will happen.

An example illustrating these relationships is as follows. The failed barrier may be a failed piece of machinery. The person may have used a faulty piece of equipment in a past repair of the machine. The factors that led to that may have been that the person was keen to get the repair job done and so chose a different piece of equipment that was easier to access. The underlying root cause may have been production pressure to get the job done and a poorly described task that did not specify a required equipment type.

By working through this logic, the underlying causes can be identified. These are often organizational decisions, leadership or culture (EI, 2016).

Identifying these underlying causes helps to explain why a person may have behaved a certain way and that the behavior was prompted by underlying causes that were not in his control. This can help dissuade the blame approach and help the operators/maintenance technicians to understand that it is not about something they did but more about something that prompted them to do what they did.

Human factors issues may underlie both the prevention and mitigation barriers in Figure 11.3. One simple approach to understand why a human might have behaved the way he did is to continue to ask “why?” In doing this, the underlying cause(s) is eventually reached. In knowing why the human behaved a particular way, and monitoring performance, data can be gathered and action can be taken to improve the workplace.

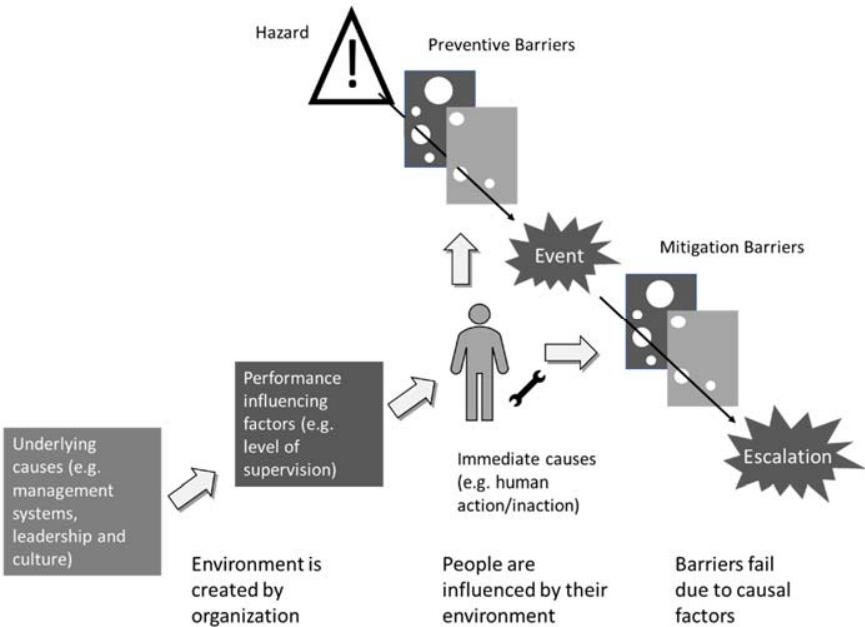


Figure 11.3 Incident Causation Model (EI, 2016)

Example:

Twenty-five to forty percent of all loss of primary containment incidents causes are due to operator line-up error – a human factor. Celanese set out to determine why the operator made the line-up error. They found 3 groups of causes – all related to management

discipline. In summary, the management did not give the operator the right tools. Celanese created and implemented a group of conduct of operation tools called Walk the Line (WTL). In the five years since implementing WTL, Celanese has seen an 86% reduction in Tier 1 and Tier 2 LOPC events. (Forest, 2018)

Potential human factors issues that may be underlying causes of an incident are listed in Table 11.1.

Table 11.1 Human Factors Issues

ORGANIZATIONAL FACTORS		
Resource Management	Organizational Climate	Organizational Process
Management of human resources	Organizational structure	Established conditions of work
Management of monetary resources	Organizational policies	Adequacy and availability of procedures
Design and maintenance of facilities	Safety culture	Oversight
	Rewards/punishments	Complexity of work
SUPERVISORY FACTORS		
Supervision	Planned Operations	Known Problem
Guidance provided	Correct data available	Documentation error
Operational doctrine	Adequate briefing time or work preparation time provided	At-risk behavior
Oversight	Proper staffing available	Initiate corrective action
Training	Adequate operational procedure or plan	Report unsafe tendencies
Qualifications monitored	Adequate opportunity for worker rest	
Performance monitored		
Management of hazards		

Table 11.1 Human Factors Issues (cont.)

<i>PERSONNEL FACTORS</i>		
Mental States	Physiological States	Physical/Mental
Focused attention	Physiological state	Reaction time
Complacency	Physical health	Vision/hearing
Distraction	Influence by medication	Knowledge
Mental fatigue		Physical capability
Haste		Fatigue
Situational awareness		
Motivation		
Task saturation		
Language/cultural differences		
Shift cooperation/teamwork		
<i>WORKPLACE FACTORS</i>		
Design	Maintenance	Environmental
Instrumentation clarity	Poorly maintained equipment	Illumination / visibility
Layout work space, access	Poorly maintained workspace	Storm
Communications equipment	Poorly maintained communications equipment	Temperature (hot or cold)
Equipment provided for the job	Labeling	Wind
		Noise level

Incident investigations must include human performance considerations and human factor issues. The use of checklists and flowcharts is a helpful technique to aid investigators in addressing human performance issues. For example, checklists can be built using the information in the tables shown above in this section. Checklists may be strengthened with input from a human psychologist, an expert on human reliability analysis, and experienced incident investigators. Numerous interface devices have been developed that translate theoretical models of human error causation into easy-to-understand engineering terms. Some of these devices are in the form of logic trees or checklists.

Chapter 10 describes the use of checklists in root cause analysis.

11.2.3 Human Factors in Developing Recommendations

In the past, recommendations to incident findings may not have questioned why a human behaved the way observed. This limited the possible recommendations. Management may have tried to threaten or entice workers into not making errors. In retrospect, this approach made little sense because proper motivation is not able to overcome poorly designed equipment and inadequate management systems. In other words, in the past the human has been expected to adapt to the system. This usually does not work. Instead, what needs to be done is to *adapt the system to the human* (Rothblum, 2002).

The previous sections described the importance of getting to the root causes of why humans behaved the way they did. Having identified these root causes, it is then possible to draft recommendations addressing root causes such as management systems that allowed deficiencies in the work environment to exist. The recommendations might encourage revising practices to clarify responsibilities in following up on action items, review of work assignments to address worker fatigue or overload, or modification of employee goals and rewards to focus on safe and productive performance. The recommendations should have the intent to *set up the worker to succeed, not set up the worker to fail*.

11.2.4 After the Investigation

Leadership support for learning from incidents and the strength of the management systems will impact the ability of an individual and the organization to learn from an incident.

After the recommendations have been made, as discussed in the preceding section, they must be acted upon. Again, although the management system may state that recommendations are to be closed in a given timeframe, the workload and priorities may impact if and how quickly these recommendations are completed.

The management system may also affect the way that the learning is handled through time and institutionalized. Is it simply emailed around and then lost in the volume of email? Or is it codified in a way that a future operator or engineer can access it easily and understand why it is important through recognizing how it was involved in a past incident?

11.3 OTHER REFERENCES

The CCPS *Human Factors Methods for Improving Performance in the Process Industries* (CCPS, 2007) provides a basic overview of human factors topics in the process industries. The *El Learning from Incidents, Accidents and Events* (EI, 2016) describes the learning from incidents process, from investigating to learning. The UK Civil Aviation Authority *Flight-crew human factors handbook* (Civil Aviation Authority, 2014) includes a very good theoretical explanation of human processes and behaviors presented in a simplified way.

11.4 SUMMARY

This chapter discussed human factors concepts including human action types and classes of human failures. It also presented human factors models including the facilities/equipment, people and management system model presented by CCPS (CCPS 2007) and the SRK (Rasmussen, 1983) mental processes model. The other references noted in Section 11.3 provide greater detail on the topic of human factors.

Human factors are important before, during and after an accident investigation. Before the investigation, leadership can set the tone about the importance of learning from incidents (as opposed to placing blame). During the incident digging beyond the causal factors to understand why a human behaved a certain way can lead to underlying root causes in management systems. Creating recommendations that address these underlying root causes will aid in preventing a wide range of similar incidents (and not just prevent the one incident from recurring). A good investigation considers the impact of human factors, strives to understand the underlying root causes in human factor/management system terms, and then makes recommendations aimed at setting the human up for success.

12 DEVELOPING EFFECTIVE RECOMMENDATIONS

Using structured approaches such as those described in the preceding chapters, an investigation team identifies the causal factors and root causes of the incident. These approaches provide the mechanism for understanding the interaction and impact of management system deficiencies. When the investigators understand what happened, how it happened, and why it happened, they can develop recommendations to help prevent a recurrence of the incident.

Effective recommendations can reduce risk by improving the process technology, upgrading the operating/maintenance procedures or practices, and most critically, improving the management systems. Recommendations that correct management system failures should either eliminate or substantially reduce the risk of recurrence of the incident as well as other similar incidents.

This chapter describes the characteristics of high quality recommendations necessary to prevent future incidents, as detailed in Chapter 14. The first section is a presentation of the major concepts related to recommendations, such as attributes of good recommendations, management of change, and inherent safety. The second section expands on the attributes and presents a systematic discussion of the flowchart for recommendations.

12.1 KEY CONCEPTS

Figure 12.1 presents an overview of the activities in this chapter, beginning with the system-related causes already identified. The cause(s) should be addressed by recommended preventive or mitigative action item(s). In some cases, the incident investigation team is responsible for developing the recommended actions, and then presents these recommendations to the management team responsible for accepting, modifying, or rejecting these recommendations. Consultation with the management team is important in order to establish ownership of the recommendations and to address issues such as priority and timeline. In other cases, the responsibility for developing some or all of the recommendations lies with the management team,

depending on the nature of the recommendations, jurisdiction, and legal considerations. For example, a management team may be best qualified to develop a recommendation to change a management system, whereas the investigation team may be best qualified to develop a recommendation to address a technical, operational, or maintenance issue. When a management team will develop one or more recommendations, the investigation team is responsible for presenting the causes of the incident to the management team in a clear and concise way, such that the management team can develop the most effective recommendations. The investigation team can still be involved in the process of developing the recommendations, as needed.

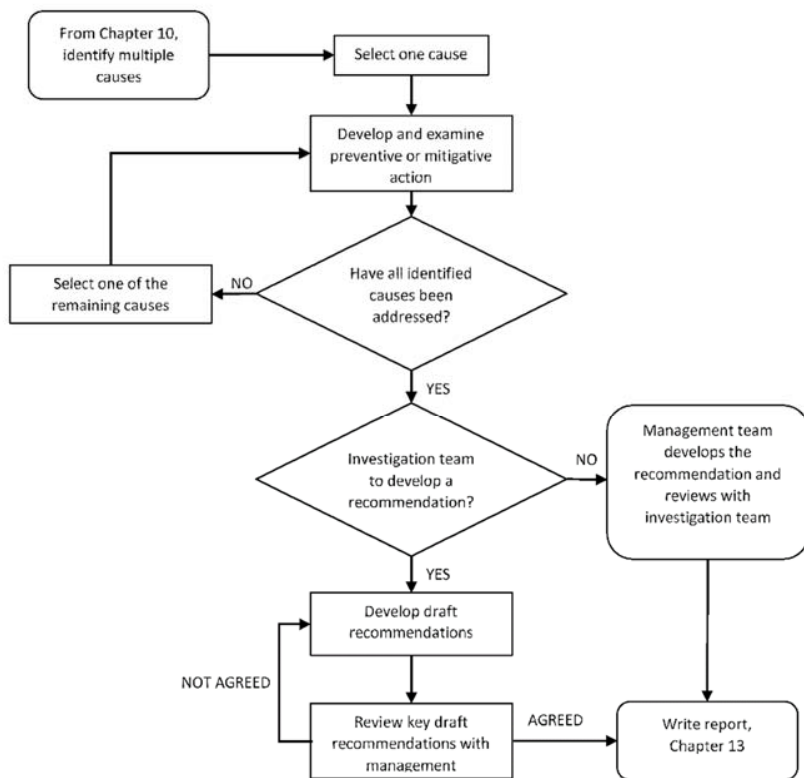


Figure 12.1 Incident Investigation Recommendation Flowchart

A key issue is to ensure that investigation teams assign corrective actions that are consistent with the cause(s) identified. It can be tempting for teams to make too many recommendations; quality and relevance are more important than quantity.

Recommendations should be written clearly and should be practical to implement. Writing and implementing specific recommendations which address the root cause is critical for a successful learning process (IChemE, 2018). Most recommendations that require a change to equipment or process safety information or that otherwise have a bearing on safety should undergo a Management of Change (MOC) evaluation to identify and consider the impact and risks associated with any changes *before* they are implemented.

12.2 DEVELOPING EFFECTIVE RECOMMENDATIONS

12.2.1 Team Responsibilities

The organization has to determine whether the responsibility for making recommendations lies with the investigation team, a management team, other stakeholders, subject matter experts, or a combination of these parties. However, it is the responsibility of management to approve, modify, reject, prioritize, communicate, implement, and follow-up on the recommendations, including:

- allocating sufficient personnel and capital resources for timely completion, and
- implementing changes and following up with those affected by the changes to assure measures are working as expected.

12.2.2 Attributes of Good Recommendations

A well-written recommendation clearly and concisely shows how it was derived from the findings of the investigation. It also specifically describes and defines successful completion in clear and measurable terms. Recommendations should be “SMART” (Specific, Measurable, Agreed/Attainable, and Realistic/ Relevant, with Timescales) (HSE, 2004 ; RSSB, 2014).

Recommendations should transfer full responsibility and ownership to the receiving department or to a specific individual. The recommendations should also include guidance on priority, for consideration by management. A common way to assign priority is to consider the risk and/or consequences

of continuing to operate without implementing the recommendations, possibly by the use of a risk matrix. Although the investigation team can indicate their assessment of priority, it should not be the responsibility of the investigation team to specify a due date. Management should be consulted in establishing completion dates for actions, although the investigation team should emphasize when specific action should be completed before the process is restarted.

Some organizations consider it useful to consider recommendations under two categories:

a) Prescriptive: A specific, defined action, e.g. *“Replace stainless steel pivot bolt with a titanium bolt as specified in XYZ engineering standard ...”*. This is the best kind of recommendation when a specific established requirement must be met.

b) Performance Based: Describes the desired condition after the recommendation is implemented, e.g. *“Develop and implement design and/or process changes which reduce the potential for erosion...”*. This is typically more appropriate when there is more than one way to meet the intent and/or when the investigation team are not best placed to define how the condition is met).

A good practice is to word the recommendation as a stand-alone statement that describes, in sufficient detail:

- What needs to be done (The required changes or improvements)
- Why the changes are required (The consequences to be avoided)
- A defined desired state that indicates the recommendation has been effectively implemented

The recommendation should not include assertive or prescriptive directives that simply order the recipient to carry out an activity. For example, instead of *“Rewrite the operating procedures,”* a recommendation that addresses higher level causal factors might be worded as follows:

- *Conduct a step-by-step review of the reactor charging operating procedures with a multi-disciplined team and update the procedures to fill gaps in the procedure. The incident investigation team identified several steps in which details seem to be missing: purging, blocking in reactant A, and disconnecting trailer that have led to leakages from joints and valves.*

The team may also make appropriate higher-level recommendations that address root causes, such as:

- *Set up a system to review and update procedures and train staff on an annual basis and after changes occur to prevent mal-operation of process unit, or*
- *Establish a system of audits on a quarterly basis to ensure compliance with critical operating procedures.*

Clearly written recommendations allow little opportunity for confusion and should not include vague or ambiguous terms/phrases such as “appropriate safeguards” or “improve the quality of training”, unless they are expanded upon and specifically define performance objectives.

Recommendations can focus on changes to improve:

- physical systems, such as hardware, equipment, and tools,
- administrative systems, such as procedures, methods, training, or
- overall management systems.

Appendix D is an example case study on a fire and explosion. The recommendations for this hypothetical case study are typical of the range of detail that can be found in recommendations that address changes in management systems.

Attributes of successful recommendations include the following.

1. They are SMART (see above)
2. They address the causal factors and root causes of the incident.
3. They clearly state the intended action, why it is needed, what it should accomplish, and the timeframe required for implementation.
4. They are sustainable.
5. They add or strengthen a layer of protection.
6. They eliminate the hazard, reduce the consequences, or decrease the probability of recurrence.
7. They address lessons learned, particularly lessons that may be applied in other areas. See Chapter 16.
8. They are compatible with other organizational objectives such as protecting the community and the environment.

Some examples of well-written recommendations from Appendix D are provided below:

- Review the rest of the asset integrity management program to ensure all critical equipment, piping, and pumps are included and have an established inspection program with guidelines for repair. Include inspection and repair of fireproof insulation in the program. (*By “date”*)
- Establish a weekly fire pump start and check program to be sure that this equipment works as intended. Revise the procedure to run the diesel pumps for a minimum of 30 minutes to detect overheating problems. (*Before startup*)
- Establish a preventive maintenance program to oversee all the maintenance on all the fire water pumps. Establish a high priority (Priority 1) for repairs on the fire equipment. (*Before startup*).

12.3 TYPES OF RECOMMENDATIONS

Successful recommendations can either reduce the likelihood of an incident recurring or reduce (or eliminate) its consequences. The following sections give examples of recommendations that could be developed by an investigative team. There are several different approaches to categorizing recommendations—for example:

- Recommendations specifically targeted at reducing the frequency of a given incident, for example:
 - (a) Increasing preventive maintenance inspection programs to reduce the probability of simultaneous failure of critical circulating pumps and back-up pumps.
 - (b) Providing additional hardware, such as a second independent alarm or trip.
- Recommendations specifically intended to eliminate or reduce the consequences of a given incident, for example:
 - (a) Reducing inventories of hazardous materials.
 - (b) Reducing personnel exposures by relocating non-critical groups of workers to areas remote from potential toxic or blast zones.

Recommendations targeted at “softer” issues, such as human and organizational factors including the work environment, safety culture, leadership and management.

12.3.1 Inherently Safer Design

Recommendations that lead to inherently safer designs are preferred to those that add extra mitigative or preventive features (Kletz, 1985). Inherently safer designs limit reliance on human performance (e.g., following procedures), equipment reliability (such as control systems and interlocks), and properly functioning preventive maintenance programs for the successful prevention of an incident. Inherently safer design features are more practical and economical if they are implemented during the design stages of a facility. Making design changes to an existing process may not be feasible or practical. Nevertheless, the investigation team should consider whether there is an opportunity to recommend a study on possible design changes that incorporate inherent safety concepts.

An early reference to inherent safety was the subject of a lecture by Trevor Kletz in 1977 entitled: “What you don’t have, can’t leak.” This principle has evolved over the years and is typically presented in a hierarchy (minimization, substitution, moderation and simplification (Amyotte, 2018), as explained below:

1. **Minimize:** Advancements in process control, improvements in logistics and changing acceptable risk standards may have removed the initial justification for large inventories of hazardous raw materials, intermediates or products. For example, tight quality control of on-time deliveries of hazardous raw materials may allow for a one or two day supply on hand versus a one- or two-week supply.
2. **Substitute:** Sometimes substitution of a less hazardous material is feasible. For example, many chlorinating systems for water purification have been converted from pressurized cylinders of liquid chlorine to a pelletized, hypochlorite salt.
3. **Moderate:** Sometimes it is possible to achieve significant reductions in reactor size (and inventory) with improved mixing technology. Another example of intensification is changing from a batch operation to a smaller scale continuous operation.
4. **Simplify:** It may be possible to use a totally different process or method to accomplish the same objectives.

The incident investigation team should consider including recommendations that examine inherently safer design. Changes can be either beneficial or detrimental, so investigators should be alert for features in recommendations that are inherently less safe. Two common examples of design changes that can *increase* overall risk are the use of flexible joints and the use of glass (rotameters, bulls eyes, sight glasses, or additional control room windows) (Englund, 1991). Seal-less pumps are generally considered to be inherently safer than pumps with mechanical seals. The failure mode(s) of any recommended new equipment should be carefully considered before a decision is made to implement the change.

12.3.2 Layers of Protection

The concept of multiple layers of protection (barriers) has widespread support throughout the refining and chemical processing industry. By providing sufficient layers of protection against an accident scenario, the potential risk associated with that accident can be avoided or at least reduced. For a given scenario, only one barrier must work successfully for the consequence to be prevented. However, since no single barrier is perfectly reliable, multiple layers of protection are often provided to render the risk of the incident tolerable. It should be understood that these multiple layers of protection are fully independent; otherwise, there could be fewer barriers than expected. This is illustrated in Chapter 2, where the “Swiss Cheese Model” is discussed.

The failure of one or more barriers might be identified as part of an incident investigation. Recommendations arising from an individual barrier failure can be made at various levels. Trevor Kletz said that accident investigation was like peeling an onion: “The outer layers deal with the immediate technical causes while the inner layers are concerned with ways of avoiding the hazards and with the underlying causes, such as weakness in the management system.” He identified three layers of recommendations, as follows: (Kletz, 1988)

- **First layer remedies use immediate technical recommendations targeted to prevent a particular incident.** Consider the case where an employee is injured by inhalation exposure while taking a liquid chlorine process sample. First-layer recommendations would address such items as changes to the sampling procedure, refresher training, and selection and use of personal protective respiratory equipment.
- **Second layer recommendations focus on avoiding the hazard.** A deeper and broader perspective is used for this second layer, and

often the focus is on improving the normal barrier measures placed between the person and the hazard. Typical remedies for the above chlorine incident might include modifications to the sampling apparatus, sampling at a different location, or perhaps installing an in-line analyzer, which would eliminate the need for manual sampling.

- **Root causes are addressed in the third layer by identifying changes in the management systems.** These third-layer recommendations act to prevent not only this particular incident, but also similar ones. Preventive measures, which result in changes in management systems, are in theory more consistent and enduring. Again using the above example, a recommendation could be to introduce a management system across the facility that requires periodic safety reviews of all routine process operating procedures, including sampling, where staff could be exposed to process material.

Recommendations that address all three layers can bring value and reduce the likelihood of a recurrence. However, addressing the root cause is the most effective means to prevent a similar incident, as well as other incidents that could result from a failure in a particular management system.

Another concept of the use of layers in developing recommendations is the safety layer model. A general sequence of safety layers is shown in Figure 12.2, which is from International Electrotechnical Commission IEC 61511-1, and presented as a paper (Foord, 2004). This sequence starts with process design, progresses through basic process control and operation, prevention systems, mitigation systems, and emergency response.

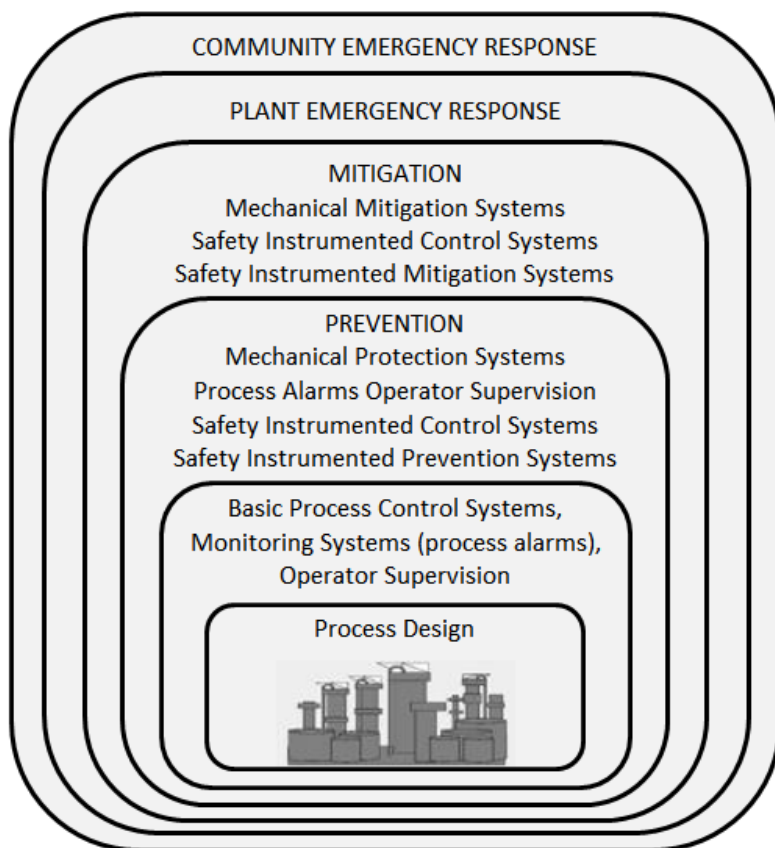


Figure 12.2 Layers of Safety (Foord, 2004)

When considering the recommendations, the incident team should identify the layers of protection that are in place, particularly those that failed and their associated management systems. This can be particularly valuable when investigating near-misses, where other barriers were still in place, thereby preventing a more significant event. The use of Bow-Tie diagrams is becoming popular as part of the incident investigation process (CCPS 2018). This is a particularly valuable tool for developing and communicating recommendations, as shown in Figure 12.3. The prevention barriers are presented to the left, the hazardous event (typically loss of containment) in the center and the mitigation barriers to the right. These diagrams were

originally developed by ICI in the 1970s and were referred to as “butterfly diagrams.”

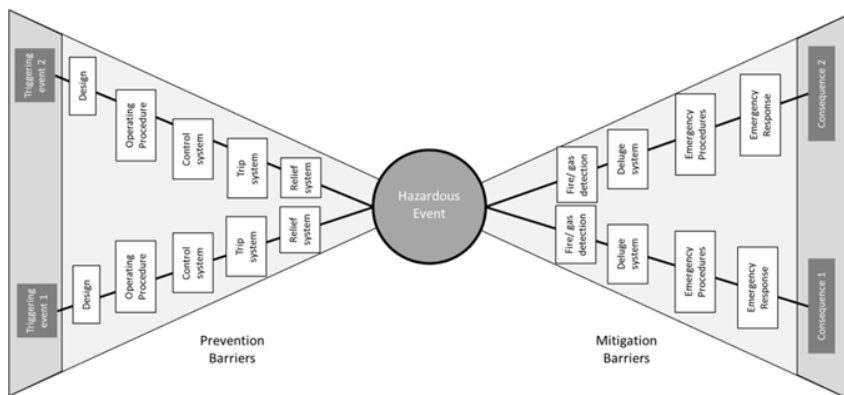


Figure 12.3 Bow-Tie Barrier Method

Using the bowtie and considering the chlorine exposure case, the investigators would consider the barriers that did not perform as intended and recommend improvements such as:

1. **Improvements in the procedure used to design the process sampling system.** (Who participates in the decision? What are the criteria for determining location method and devices? Who authorizes? Is there a periodic audit or re-evaluation?)
2. **Improvements in the management system for establishing, evaluating, and monitoring standard operating procedures.** (Are the procedures adequate, understood, and consistently performed? Is the task still necessary?)
3. **Improvements in the processes for systematically reviewing operations for potential hazards.** Is there a routine mechanism such as Job Safety Analysis (JSA) in which tasks such as this are systematically reviewed for potential hazards? JSA is a procedure that systematically identifies: (1) job steps, (2) specific hazards associated with each job step, and (3) safe job procedures associated with each step to minimize accident potential.

In summary, there are various techniques available to help the investigation team identify the layers of protection (barriers) that have failed. The recommendations should address the root causes of the failure of the management systems that have been insufficiently robust to maintain the barriers effectively.

12.3.3 Commendation/Disciplinary Action

When an investigation reveals an employee action worthy of commendation, the incident investigation team should acknowledge the individuals directly, but not name them in the formal investigation report. Cool and rational actions in the midst of an emergency often limit the consequences of an incident, but naming an individual publically could bring undesired attention or could be culturally inappropriate.

Disciplinary action is outside the scope of the investigation team's remit. Even the perceived threat of disciplinary action has a detrimental effect on an investigation and may discourage cooperation during interviews. In the event that disciplinary issues should be considered, this should be part of a separate management process, involving a different team and in line with the company's internal disciplinary procedure.

12.3.4 The "Further Action Required" Recommendation

Another special case is the recommendation for further work; for example, the investigation team may recommend re-evaluation of an existing safeguard, evaluation of a new safeguard, or consideration of an inherently safer design. This does not mean that the investigation team has failed to complete its task. It is common for an investigation team to generate a recommendation to confirm whether an existing physical system or administrative measure (such as written procedures or training program) provides adequate protection. It could be that specialists, who had not been available to the investigation team, are needed to conduct further work or engage additional expertise outside the main investigation process. It is not appropriate for an investigation team to attempt to engineer a solution in an area in which they are not qualified. In these instances, the team should specify, for example, what action is necessary if the safeguard is found to be inadequate. If the team only specifies a vague action such as "review the start-up procedure," then the implemented action may or may not meet the team's intentions.

An example of being more specific in the case above would be to create two recommendations as follows:

- (a) Conduct a risk assessment of the start-up process.
- (b) Revise the procedure to ensure that safe operating limits are not exceeded.

Alternatively, the investigation team can pull-in support personnel as needed to generate an effective recommendation.

12.4 THE RECOMMENDATION PROCESS

12.4.1 Select Each Cause

The process of developing recommendations is summarized in Figure 12.1. Starting with the set of multiple causes (determined previously in Chapters 3 & 10), each cause is evaluated individually to consider actions that would prevent or satisfactorily mitigate a recurrence. Potential options for recommendations should be evaluated for technical merit, feasibility, effectiveness, reliability, cost, and other important factors. Some recommendations that address one particular cause may also be relevant in addressing other causes. The investigation team considers all these factors when determining the final set of recommendations to propose.

12.4.2 Perform a Completeness Test

The next activity in the sequence is to check for completeness, such as, "Have all the identified causes been addressed by the recommendations?" Most events will have multiple causes, some of which may appear to be quite remote from the incident itself. This is particularly the case with management system failings, where the recommendations may address administrative and procedural matters that may also help prevent other types of incidents from occurring. For example, an incident that was caused by a new type of valve design may result in the team recommending improvements to the MOC process. The revised MOC procedure might prevent another incident from occurring as a result of a change to an operating procedure where the safety implications were not fully considered.

12.4.3 Assessing the Effectiveness

Once the recommendations have been made, their effectiveness should be assessed to ensure that:

- They can be implemented as intended
- They can stand the test of time

Examples of ways to monitor effectiveness of recommendations are provided in Figure 12.4 below. Further details on monitoring and improving the performance of the incident investigation system are shown in Chapter 15. Once the effectiveness of recommendations has been confirmed, the investigation team finalizes the list of recommendation.

12.4.4 Prepare to Present Recommendations

If the investigation team is responsible for making recommendations, when preparing to present them to management, the investigation team should consider grouping the actions by:

- Risk Priority/ timeframe for implementation (See 12.2.2)
- Systems affected
- Individuals assigned
- Cost (or level of approval required)
- Need for outside resources (such as further research or special expertise)

The team should also anticipate potential challenges to recommendations. They should research and resolve expected questions and concerns from line management and operating personnel. If information is available to compare the recommendations to other similar operating processes, that should also be taken into consideration when preparing the recommendations for review by management.

Example Recommendation	How Its Effectiveness May Be Assessed
Revise the procedure to change the warning to an action step	Review the revised procedure to determine that all action steps are included and all warnings and cautions do not contain action steps. No inappropriate steps, cautions, or warnings should be found in the procedure
Review and revise all existing procedures to ensure proper format is used for information contained in the procedure (steps, cautions, warnings, notes, etc.)	Periodically review existing procedures to determine format errors. No inappropriate steps, cautions, warnings, notes, should be found
Revise the procurement specifications for the gaskets used in this line	Verify that the revised procurement standard contains the specification for the proper gasket
Perform a review of other gaskets in the lines carrying the material to determine the proper gaskets are being specified. This review should start with at least a 10% sample of current applications	Verify that existing procurement standards contain the specification for the proper gasket Review maintenance work orders to determine the number of gasket replacements that are performed as a result of the inappropriate gasket materials
Revise the design standard used to design lines carrying this material	Periodically review the design of equipment carrying this material to ensure that the proper gaskets are being specified Review maintenance work orders to determine the number of gasket replacements that are performed as a result of the inappropriate gasket materials
Train the engineering staff on the revised standard	Periodically review the design of equipment carrying this material to ensure that the proper gaskets are being specified Review maintenance work orders to determine the number of gasket replacements that are performed as a result of the inappropriate gasket materials
Provide an additional communication system, such as portable radios, that maintenance personnel can use to communicate with supervisors and planners. This should allow the current paging system to be used exclusively by operations	Periodically monitor communications on the paging system to determine if other groups are using the system Assess the traffic load on the new maintenance communication system to ensure that it has adequate capacity Periodically survey the maintenance personnel to determine if they are having difficulty with the communication equipment Periodically survey operations personnel to determine if they have problems with other groups using the paging system
Modify the overtime policy to limit the number of hours of overtime that can be worked in a given time period	Monitor the number of overtime hours being worked. Determine if individuals are exceeding the guidelines that the new policy outlines

Figure 12.4 Example Recommendations and Assessment Strategies (ABS, 2001)

12.4.5 Review Recommendations with Management

As shown in Figure 12.1, the next step is a presentation and review with the members of line management who have responsibility for operation of the affected unit. Management may then approve, modify, reject, or implement the recommendations. This is discussed further under section 4.2.9 – Recommendation Responsibilities.

At this stage of review, it is often the case that the full incident investigation report has not yet been written, and only the essential recommendations have been developed. Line management will consider these key recommendations as a priority, and the other, less critical recommendations may not be reviewed with management until the report has been drafted at a later time.

The investigation team should provide guidance to management on the risk priorities of the various actions, including those that should be implemented before restart, where applicable. However, management is responsible for resourcing the recommendations and assigning priorities for the actions. This would typically be expressed in the form of a due date. Where no specific due date is assigned, there should be clear guidance provided by management on the timing such as: “Before restart”, “During next turnaround”, or “Before the year end”. The definition of “priorities” (e.g., 1, 2, 3 etc.) should be clearly specified, and will vary between organizations and investigations. A common way to assign priority is to consider the consequences of continuing to operate without implementing the recommendations. At times, it may be necessary to conduct a more thorough risk assessment in order to prioritize the actions.

Once the recommendations have been made and accepted, they should be communicated effectively throughout the organization. The implementation of the recommendations is further discussed in Chapter 14.

12.4.6 Tracking and Closure of Recommendations

The progress and implementation of recommendations should be closely monitored using metrics as detailed in Chapter 15. This should include:

1. Leading indicator metrics assigned and frequently reviewed (e.g., item priority, no action, in progress, due in 30 days, 30 days overdue, closed, etc.).
2. Be tracked to completion with periodic management review.

3. Have a defined work process for deviating from original intent or due date.
4. Documented closed with evidence.
5. Have an approval process for closure.
6. Where appropriate, have an effectiveness check after closure.

12.5 SUMMARY

This chapter discussed tools and techniques for developing recommendations that will be both effective and lasting. The recommendations are developed once the causal factors and root causes have been established. Recommendations can either be produced by the investigation team or the management team although in either case, the two teams should work together to produce the recommendations. The most effective recommendations are those that deal with the root causes, which will usually be addressed by improvements to management systems. They should be SMART, which includes ensuring that the recommendations are specific and the timescales and priorities are fully understood and agreed by all parties. The concepts of inherent safety, safety layers and barriers were discussed. If it is not feasible or practical to apply inherent safety design, the recommendations should address the root causes of the failures of these safety layers and barriers. Recommendations should add or strengthen protection layers as appropriate for the potential consequences. Finally, there needs to be a process to check that the recommendations have addressed all the root causes and that they are effective and adequately tracked to completion.

13 PREPARING THE FINAL REPORT

With information gathered, causal factors determined, root causes analyzed, and recommendations formulated, the incident investigation team sets about the task of preparing the written incident investigation report. What are the attributes of high-quality incident investigation reports? How do they differ from other communications such as interim reports? This chapter describes practical considerations for written incident investigation reports. Attributes of quality reports are presented with special focus on the report reader or user. A generic report format is presented along with a discussion of avoidable common mistakes.

Before embarking on writing an incident investigation report, the company's legal counsel should be consulted. There are numerous legal issues that may influence report content, including company proprietary information, legal privilege, regulatory compliance and enforcement, civil litigation, and possibly criminal litigation. The investigation team needs instruction from legal counsel on report content as well as guidance on the handling and storage of report drafts before starting to write a report.

Report authors should be experienced in writing investigation reports and have the knowledge and experience to draft their portions of the report. Incident investigation report writing is challenging due to complexity of the incidents, scrutiny that will be given the report by stakeholders, clearly communicating the investigation findings and recommendations, and legal issues. Authorship of the report should be carefully selected with oversight being provided by an experienced and qualified individual. Besides the report, short briefing documents used to share lessons should also be authored by the incident investigation team to ensure accuracy of the briefings.

13.1 REPORT SCOPE

The scope of incident investigation reports should be focused on the incident investigation and not ancillary topics, unless such factors are directly relevant to the incident consequence. Ancillary topics refer to items such as emergency response, public relations, and other activities that occur during a major incident but are outside of the scope of the incident investigation. (If there are significant shortcomings or concerns regarding ancillary topics,

management may commission a separate investigation to address these issues.) On occasion, incident investigation teams uncover an issue that has no bearing on the incident being investigated but is an opportunity for improvement. Such an issue should be communicated separately to management. An avoidable mistake in incident investigation reports is report scope creep, meaning expansion of the report scope beyond investigation of the subject incident. Report scope creep results in a larger report with an increased number of recommendations and a more diluted focus.

The extent of the content of incident investigation reports depends on many factors including audience needs, company culture, incident classification, technical complexity of the findings, regulatory requirements, and legal considerations. There is no standard format or guideline for investigation reports. Reports should be customized to best meet the organization's needs (see NFPA 921, 2017; API RP-585, 2014).

13.2 INTERIM REPORTS

Some process safety investigations will be extensive in duration, particularly where serious or high-potential incidents are involved. For complex incidents, evaluation of all scenarios and causal factors may require a lengthy period—months and perhaps years. Rather than waiting for the entire investigation to be completed, the team may write an interim report, indicating initial findings and open investigation activities. The interim report content should be as accurate and factual as possible, yet should remain flexible and responsive to new information. It should communicate where the investigation is at that point in time, what is known, and investigation activities that are ongoing.

Interim reports may be issued before all of the causal factors have been determined and a root cause analysis has been performed. The interim report should not include content beyond what is factually known and proven. Including speculation that is later retracted, or revising conclusions and recommendations, can cause stakeholders to question the credibility of the investigation. In addition, readers of an interim report may take action, only to find the action was inappropriate if the report is later revised.

Depending on the status of the investigation and content of an interim report, the interim report may not have sufficient information for management to decide if a process can be restarted. The investigation team

leader should discuss investigation status and any recommendations that affect startup (if formulated) with management so that management can make an informed decision about the timing of a process restart.

As the investigation proceeds new issues may arise, open items may be resolved, and, recommendations modified accordingly. Interim report documents should be updated or annotated as necessary. Each report issued by the incident investigation team should be retained and its distribution documented. The team leader should coordinate all such interim reporting activity. Someone should serve as the appointed liaison between the incident investigation team, management, and external organizations. This is often the team leader, but others with special training may also fill this function. A single communications channel is especially helpful when team members must deal with external regulatory agencies.

13.3 WRITING THE REPORT

The written incident investigation report is the vehicle for documenting and communicating the investigation results. Process safety incident investigations cover a wide variety of topics, but unless a report is well laid out, the impact of its presentation is not as effective as it could be. A quality report can be extremely useful, leading to process safety improvements, and extending the impact of the team's investigation. Likewise, a poorly prepared report may fail to convey important information, negating weeks or months of productive investigation.

A mechanism for capturing and documenting the results of the investigation should be an integral part of the management system for process incident investigation. *Guidelines for Technical Management of Chemical Process Safety* (CCPS, 1989) states that, "The lessons learned from an incident investigation are limited in usefulness unless they are reported in an appropriate manner." The American Chemistry Council recognizes this need by including it as one of the twenty-two management practices in the Responsible Care®, Process Safety Code of Management Practices (ACC, 1990). The written report should convey the findings and recommendations of the investigation clearly and succinctly.

It is helpful to identify the audience before drafting a report and to ensure that the report writers understand the needs of the entire audience. For example, the audience may include varying levels of management, operators, maintenance workers, engineers, future PHA teams, other sites,

and regulatory agencies. Although it may be unreasonable to expect that all the needs will be met completely, considering them during the writing phase will help approach that goal. The large variation in the readers' technical backgrounds, the need to include technical information and the need to be reasonably concise may limit the usefulness of a single report, although this challenge may be addressed by including an executive summary or similar section in the report for those with a less technical background or less need/desire to know the details. Every report represents a balanced trade-off of content, details, quantity of information, to meet the expected needs of the readers and users. It is reasonable to expect that the report user has some general knowledge of chemical process technology and hazards. It is also reasonable to expect that the readers have some genuine interest and a desire to gain from understanding and applying the available lessons. The report should not only document and communicate the findings and recommendations, it should also be a tool to motivate or inspire action.

Carper, in his book *Forensic Engineering* (Carper, 1989), recognizes multiple audiences. Carper acknowledges the reality that the report should not be expected to reach all audiences equally and satisfy all questions. *Professional Accident Investigation* by Kuhlman develops the concept that different levels of management have different needs and priorities (Kuhlman, 1977).

Although it is the most important single document, the investigation report is only a portion of the overall record of the investigation. Other parts of the investigation record include photographs, measurements, process data, witness accounts, laboratory analyses, engineering analyses, and other facts and analyses that support determination of causal factors and root causes. Consideration should be given to compiling and maintaining a full and complete set of documents for future reference. This systematic documentation package is sometimes referred to as the *audit trail*. It provides subsequent reviewers and investigators with the opportunity to understand the team's decisions and analysis more completely. The document set should contain lists of relevant files. All documents associated with the investigation should be preserved according to company records retention policy.

An investigation report:

- Describes the incident in full detail (with timelines if possible),
- Explains the sequence of events and failures that led to the

- incident,
- Describes the management systems that should have prevented the occurrence,
- Identifies factors that contributed to an escalation of the incident consequences,
- Details the system root causes, and
- Provides management with suggested recommendations to prevent or lessen recurrence and/or associated consequences.

The report should include relevant information, stated factually and accurately. If there is uncertainty about an event sequence or some other aspect of an investigation, the uncertainty should also be conveyed in the report tone and the choice of words used in the report should reflect the attitude of preventing a similar incident rather than affixing blame.

13.4 SAMPLE REPORT FORMAT

The report format and content will depend on the needs of an organization (NFPA 921, 2017) and the complexity of the investigation (API RP-585, 2014). Because there is no single universal report that simultaneously satisfies all needs of all organizations and potential readers and users, the sample format presented below provides a variety of content and detail. Organizations can select the format best suited to their needs. Table 13.1 includes a list of sections that may be included in an incident investigation report. Most sample reports answer basic questions such as:

- What happened?
- How did it happen?
- Why did it happen?
- What were the multiple management system-related root causes?
- What can be done to prevent a repeat or lower the risk?

The subject matter of the report may influence aspects of a report's layout. The guidance below presents a logical sequence of sections that allow someone reading the report to understand the circumstances, findings, causal factors, root causes, and recommendations. Some organizations develop standardized report formats, which can vary by categorization of the incident (API RP-585, 2014).

Table 13.1 Sample Sections of an Incident Investigation Report

Title Page	Include the date of the report.
Table of Contents	
Executive Summary	Summary of occurrence, consequences, causes, and recommendations.
Introduction	General summary including date, time, facility location, process area of the incident, terms of reference, conduct of the investigation (including the date and time the investigation began), team description including team members, areas of expertise, years of experience.
Background	Process description, purpose, and scope of investigation, conditions preceding the incident. Historically significant issues may be discussed.
Sequence of Events and Description of Incident	Description of the occurrence scenario, sequence, consequences (actual and potential), and response summary.
Findings	Factual findings including evidence.
Causal Factors	Identification and discussion of causal factors.
Root Causes	Identification and discussion of root causes.
Recommendations	Recommended preventive actions or actions to lower the risk.
Noncontributory Factors	Discussion of particular factors that were found to be in no way responsible for the incident but are beneficial learnings.
Attachments or Appendices	Miscellaneous back-up information such as: discussion of disproved or less-probable scenarios, documents of special interest or value, method and conduct of the investigation and team membership, photographs, diagrams, calculations, lab reports, metallurgical reports, references, noncontributory factors, terms of reference.
References	Documents that the team relied upon to draw their conclusions.

13.4.1 Executive Summary

The executive summary should be a brief summary describing the occurrence and key (or main) consequences, significant findings, causal factors, root causes, and recommendations. It is usually helpful to present a simplified summary of the occurrence in the first one or two sentences. The purpose is to provide a high level summary of the occurrence; it is not a separate version of the report itself. For most reports, the executive summary is written after completing the other sections. The executive summary is typically no more than one-to-two pages long, including all headers, footers,

legal disclaimers and other legal information. The executive summary is a part of the report—not a standalone or separate version of the report. The short layout can make the executive summary a good section for sharing results through internal web pages, bulletin boards, safety meeting bulletins, and training manuals.

13.4.2 Introduction

The body of the report may include an introduction summarizing the purpose and scope of the investigation, the incident investigation team members, and the conditions at the time of the incident occurrence.

13.4.3 Background

The background section provides information that the audience will need to understand subsequent sections of the report. This section sets the stage for information that follows. The background section presents an overview of the process (history, age, size, expansion projects, etc.) leading up to the incident. If a particular program such as a periodic inspection program, reliability history, or job safety analysis is involved in the incident, it can be referenced or explained in the background section. Information about the existing management systems, procedures, and policies that are relevant to the incident may be included in this segment, as are any unusual internal or external occurrences such as a change in plant ownership, maintenance shutdowns or turnarounds, and interruptions or distractions (for example, a power outage, severe weather, etc.).

The background of the individuals involved in the incident can be addressed, such as experience level, qualifications, experience with the particular task involved, time in the position, years of experience, time at that task that day, whether working overtime or rotating shift, etc.

The environmental conditions present at the time may be included, as they can be significant. Conditions may include time of day, temperature, lighting, and weather conditions such as rain, fog, ice, snow, wind direction, wind speed, etc.

Significant process conditions preceding the incident may be identified, especially if the process is a batch operation or if there was any known deviation from normal conditions of sequences, flows, pressures, concentrations, temperatures, pH, or other process parameters. Often it is helpful to separate the background conditions into several distinct periods. One category may be normal conditions, a second category may be the

conditions during the time period from 48 hours up to 1 hour before the occurrence, and a third section may address the background immediately (1-60 minutes) before the occurrence.

The background sections may also include information on past incidents in the process unit, including past incidents that are identical or nearly so to the actual incident (a “repeat incident”). Near-misses and minor incidents are of interest to determine if there were any precursor events.

13.4.4 Sequence of Events and Description of the Incident

In this section of the report, the occurrence is described (usually in chronological order) and the outcomes are identified. This is the WHO–WHAT–WHEN–WHERE portion of the report. It includes the actions taken to deal with the situation throughout the timeline of the event. It may give precise and specific information, such as identification numbers and location of process equipment involved in some facet of the incident. The extent of injury, details of the damage, and an estimated out-of-production time can be included in this section. Diagrams are often more useful than long paragraphs. If a timeline has been developed, it may be included in the report. The observations can be backed up with statements from those involved. Supporting documentation in the form of drawings, photographs, flow diagrams, and calculations can be included.

13.4.5 Findings

Factual findings are presented in this section. The findings flow from all investigation activities including witness interviews, scene and equipment inspection, process data, laboratory tests, equipment testing protocols, engineering analyses, modeling, etc. The findings provide the foundation for subsequent causal factor identification and root cause analyses.

It may be helpful to mention the various types of evidence that support the causal factors and root cause conclusions:

- People (interviews)
- Physical (for example, equipment, machinery, parts, analytical analysis, metallurgical analysis, testing)
- Electronic (for example, operating data recorded by a control system, both current and historical, and controller set points)
- Positions (people and equipment)
- Paper (for example, procedures, checklists, process data, permits, etc.)

It may also be helpful to discuss how the various items of evidence relate to events before, during, and after the incident. For example, positions of valves observed post-incident reflect the valve line-up at the time of the incident, but may not be indicative of the positions in the hours leading up to the incident. Each item should be placed in proper context in the timeline. This can help explain how and why the incident occurred, leading to the root causes.

Each finding may be tabulated as a separate item so that the individual subject matter under discussion is sufficiently and clearly separated from other points. One example of a tabulated format is shown in Table 13.2; for each finding, causal factors and root causes are shown. The hypothetical case in Table 13.2 was a tank explosion just outside of a power house at a chemical plant. The power house had boilers for steam generation. Waste chemicals from process units were pumped to the holding tank and consumed as a fuel in one of the boilers. The practice of using waste chemicals as fuels had been in place for about 30 years. The holding tank exploded on a warm day due to a chemical reaction in the tank. Table 13.2 presents relevant findings, causal factors, root causes, and recommendations for this hypothetical event.

The findings can also summarize any specialized studies or analyses that were commissioned to explain the circumstances of the incident. For example, studies such as metallurgical analysis of components, chemical reactivity, and supporting documentation could be included in the report appendices.

13.4.6 Causal Factors

Causal factors are identified and discussed in this section of the report. Process safety incidents are typically the result of multiple factors; therefore, singling out one cause is rarely the proper approach. If a fault tree or causal factor chart was developed as part of the investigation, it may be incorporated in an appendix to facilitate understanding.

The causes of incidents may not always be determined with certainty. Explosions and fires damage evidence that may be needed to make a definitive determination of cause. When sufficient evidence, analyses, and facts exist to determine the probable cause, the team's opinion should be stated with the basis for the assessment that the cause is most probable. Where the cause of the incident cannot be definitively ascertained, the cause

should be reported as undetermined (NFPA 921, 2017). In such instances, the possible causes that were investigated can be reported.

13.4.7 Root Causes

Root causes are identified and discussed in this section of the report. The root causes should address and explain how they relate to the causal factors. Root causes go beyond the physical causes of the incident as explained in prior sections, and it may be necessary to provide additional information in the root cause section on the management system weaknesses that contributed to the incident. An important objective of the root cause section of the report is to communicate the linkage between management system weaknesses and causal factors.

13.4.8 Recommendations

The attributes of successful recommendations are addressed in detail in Chapter 12. The incident investigation team typically has the responsibility to develop and submit the recommendations. It is management's responsibility to approve, act on, and resolve the recommendations. Typically, the final report includes only those recommendations accepted by management for implementation. Effective recommendations include a specific primary responsible person and a due date. Management determines priorities, target dates, and assignment of responsibility. As a result, feedback is needed from management in order to include assignment of responsibility and target dates in the report.

Principal or main findings and recommendations may be highlighted to emphasize their importance. For completeness, all suggested improvements should be logically linked from findings into recommendations.

Table 13.2 Findings, Causal Factors, Root Causes and Recommendations

Finding	Causal Factors	Root Causes	Recommendations	Who	By
Waste product streams flowing from multiple process units to the power house holding tank were chemically incompatible. An exothermic reaction started in the waste material holding tank resulting in overpressure of the tank.	The waste material holding tank was originally designed as a storage tank. It was not designed with cooling or pressure relief for a chemical reaction.	<ul style="list-style-type: none"> •Management of Change (MOC) procedure was not correctly followed when additional waste streams were supplied to the tank •Staff carrying out the modifications did not remember to follow the MOC procedure 	1. Review the MOC procedure to ensure it complies with corporate practices and requirements.	Mike	Feb
			2. Issue safety bulletin to demonstrate the need to follow MOC procedure.	Ben	Mar
			3. Include a training pack on MOC procedure with the annual safety refresher training.	Sue	Jul
	The chemistries of the processes that send chemicals to the holding tank have changed in the 30 years since the power house process was modified allowing waste products to be used as a supplementary fuel supply to the boiler. No control of the waste materials being sent to the power house by various process units.	<ul style="list-style-type: none"> •Failure of management and staff to recognize the risks associated with uncontrolled mixing of waste chemicals •No PHA assessments carried out on the mixed waste streams from the processes 	4. Conduct a PHA assessment of all waste and intermediate streams where mixing of chemicals can occur. 5. PHA on boiler fuel waste to be completed before restart of waste stream	Bob	Dec
	PHAs have not been conducted on the process for over 10 years.	<ul style="list-style-type: none"> •No program for redo of PHAs on the power house 	6. Review scope of PHA program to include power house and to ensure that all services areas are included.	Ted	Dec
Warm weather on the day of the incident likely escalated the reaction rate.	<ul style="list-style-type: none"> •Failure of management and staff to recognize the risks associated with higher ambient temperatures 	7. Ensure that PHA scope includes consideration of ambient temperatures up to 50 °C.	Dan	Dec	

Each recommendation should be brief (two or three sentences), sufficient to identify a particular topic, and individually numbered to facilitate management of follow-up and resolution. If appropriate, each recommendation may have appended a cross-reference number to enable a fuller explanation, description, or reference from other sections of the report.

13.4.9 Noncontributory Factors

Numerous factors are investigated in process safety incidents, and some of them may be found to be noncontributory. In some instances, it may be appropriate to report that noncontributory factors had no bearing on the incident to assuage concerns about the factor being dispelled too quickly or subject to misunderstandings. Recording noncontributory causes also provides documentation that the causes were evaluated by the team and were not overlooked in the investigation. However, reporting on noncontributory factors can increase the volume of a report and be a distraction to the more important subjects. If not included in the report, the investigation team's notes should include a record of noncontributory factors, both human and system-based, that were analyzed and found not to be relevant to the main consequence.

13.4.10 Attachments or Appendices

The remaining contents of a written incident investigation report can vary depending on circumstances. A collection of data and additional reference information that some, but not all, readers may need is often included as an appendix.

Examples of supplemental information include:

- A description of investigative methods and approaches used
- Flow sheets
- Diagrams
- Photographs
- Safety data sheets (SDS)
- A list of reference materials consulted
- A glossary of terms and acronyms
- Log sheets
- Computer printouts
- Pertinent extracts from witness interviews
- Maps
- Copies of work permits
- Injury summary

- Equipment damage information
- Lab analysis reports
- Engineering analysis reports
- Witness interviews
- Timeline

If a map is used, it should focus on the area of interest, and should minimize the amount of nonessential information shown.

Medical evidence is usually omitted from incident investigation reports due to the need to respect and protect medical information. Names of injured and other participants are also frequently omitted for privacy reasons. Descriptions such as Operator 1, 2, or 3 can be substituted.

It is a good documentation practice to include the reasons for eliminating other possible causes and alternate scenarios. This can be extremely useful and enlightening to subsequent investigators or analysts who may follow years later.

13.5 REPORT REVIEW AND QUALITY ASSURANCE

13.5.1 Reviewing the Report

All members of the incident investigation team should review and reach consensus on the content of the report before it is finalized. All report content should be reviewed and checked for accuracy. An example checklist is shown in Table 13.3. Reviews may be needed by management and legal teams for protection of company intellectual property and other legal rights. It may be appropriate for investigation team members to sign the final report depending on local practice. This is an indication of personal endorsement of the team consensus.

Many companies have an incident investigation report approval process. The level of approval is often tied to the categorization of the incident, which typically corresponds with the actual or potential severity of the incident. Generally, higher severity categorization requires a higher management level review and approval.

Table 13.3 Example Checklist for Written Reports

CHECKLIST FOR WRITTEN REPORTS	
<input type="checkbox"/>	Intended reader/user identified and technical competence level chosen
<input type="checkbox"/>	Purpose of report identified
<input type="checkbox"/>	Scope of investigation specified
<input type="checkbox"/>	Summary/abstract length is no longer than one page
<input type="checkbox"/>	Summary/abstract answers what happened, why, and general recommendations
<input type="checkbox"/>	Background—describes process, investigation scope
<input type="checkbox"/>	Sequence of events—clearly describes what happened and timeline
<input type="checkbox"/>	Findings—factual findings are presented
<input type="checkbox"/>	Causal factors – what happened is determined
<input type="checkbox"/>	Root Causes—identifies multiple and underlying causal factors
<input type="checkbox"/>	Recommendations—describes specific action for follow-up
<input type="checkbox"/>	Other—necessary charts, exhibits, information
<input type="checkbox"/>	Content agreed to by team members
<input type="checkbox"/>	Distribution identified

13.5.2 Avoiding Common Mistakes

For improved quality of written incident investigation reports, the incident investigation team should follow these guidelines:

1. Avoid jargon specific to the process that the intended reader may not understand. One good guide is to ensure that the written report is understandable to the intended reader who does not have detailed knowledge of the specific process involved.
2. For increased readability and comprehension, limit the use of abbreviations and acronyms. Most of these can be avoided. Define each abbreviation and acronym used.
3. Decide on the selected reader's level of technical competence and then be consistent in writing to that level. Assume the reader has a certain minimum knowledge of the chemical process industry.
4. Avoid intermixing opinions, speculation, and other judgements when presenting the factual findings. The report should convey the factual basis for the causal factors and root causes. The investigation team may have to make judgements and identify probable and possible causes when data are insufficient for a definitive determination. The report should clearly indicate when judgments were made. Separating

investigation team judgements into a separate report section from the factual findings can sometimes avoid confusing the reader while accurately stating the investigations position.

5. Write recommendations to be self-contained and make sense when removed from the context of the report. Recommendations are often placed in tracking systems, and the recommendations should make sense to users of the tracking system and all personnel who are taking action on the recommendation without needing to reference the report.
6. Be sure to include a list of reference materials used during the investigation. Subsequent investigators or analysts who review the report years later should be able to substantiate the conclusions reached by the investigation team.
7. Identify multiple system-related root causes after a systematic analysis by the investigation team.
8. Include descriptions and details of equipment involved in the incident, because omission can cause problems for readers in other process units or facilities who may have the similar equipment and remain unaware of its hazards.
9. Avoid downplaying human performance factors when drafting the report. There is a natural hesitancy to state performance gaps by people as these are sometimes interpreted as blame. In fact, performance gaps should be clearly stated as to who performed what action or task incorrectly (using terms like Operator 1, not actual names).
10. Publish only one official version of the final report. Sometimes the team may release a preliminary draft copy that differs from the final version. This can sometimes cause unnecessary and avoidable confusion if the interim report is not handled carefully. If a preliminary draft is published, the team should ensure that all copies of the preliminary version are replaced with the final edition. A preliminary report should be conspicuously identified as a draft. Consider including a watermark or printing a message on each page's footer or header such as *Draft— not a final report—subject to change*.
11. Delay writing the executive summary until after the main body of the report has been drafted. This will ensure that the executive summary accurately reflects the contents of the final report.

Start writing portions the report as soon as the investigation begins. Focusing on the result can help keep the team focused on the investigation process and the product.

13.6 INVESTIGATION DOCUMENT AND EVIDENCE RETENTION

The investigation team's work often ends with the approval and distribution of the report and recommendations. Once the investigation team disbands, investigation records may be lost over time or destroyed in accordance with company retention policy. Some jurisdictions require that incident reports and other documents be retained including drafts, all documents reviewed during the investigation and emails pertaining to the incident report. Litigation may impose other record retention requirements. Consult with the company's legal representative to determine the record retention requirements.

Investigation record retention may differ from normal company record retention policies. The report and its associated linked and referenced documents can be an issue. If the documents are not categorized and stored properly, corporate record retention systems can delete them. If links are used, and files are moved, the links can be broken. Investigation documents may have to be compiled and stored in a location that is protected from automated deletion.

Physical and electronic evidence may also have to be retained, sometimes for years due to litigation. Longer term evidence preservation and storage should be arranged. Items that are weather or temperature sensitive should be stored in an environmentally controlled room or building. Chemical samples and fracture surfaces pose challenges due to aging in storage, even in environmentally controlled conditions. Performing analyses while evidence is fresh and producing good documentation is often the best approach when long term degradation is unavoidable. The documentation should be retained for the duration of the legal proceedings.

Corporate counsel and management will ultimately decide when certain investigation materials and evidence may be discarded. Some materials may be retained permanently, such as the incident investigation report and the documentation of resolution of the action points.

13.7 SUMMARY

The incident investigation report is the vehicle for documenting and transmitting the investigation results. It is important to capture and preserve the essence and details of the incident to allow the stakeholders to understand what happened, how it happened, why it happened, and what actions will be taken to prevent or lessen the likelihood of recurrence, and/or the resultant consequence. The report also becomes a long-lasting reference document to teach future generations in the company of the lessons learned in the past, to provide factual information when needed in future investigations, and to contain helpful information for trending of incident patterns. A well written incident investigation report is also useful in improving future designs and processes of the organization.

There are numerous legal considerations that arise in incident investigations that impact the content of reports. Legal counsel is needed to guide the investigation team on content. Similarly, legal counsel can address retention of documents and evidence after the investigation concludes to ensure that regulatory, enforcement and litigation requirements are met.

The report contains a description of the incident, including the sequence of events and a timeline if developed. Factual findings from all of the investigation activities are presented. The factual findings provide the basis for identification of causal factors that are explained in the report. Root causes are identified and explained, and recommendations to address the root causes are presented. A reader of the report will have a clear understanding of the process and basis for reaching the root causes and recommendations.

The report is a direct reflection of the quality and professionalism of the incident investigation team. The entire team should review and approve the report before release. The company's legal and management review processes follow the investigation team approval. Management approval is done at the appropriate level for the actual or potential severity of the incident.

Recommendations are the mechanism by which improvements are made to lower the risk of an incident. The language of recommendations is unique among report content in that recommendations must be self-contained, self-explanatory statements that make sense when removed from the context of the incident investigation report and placed in corrective action tracking

systems. Recommendations must also create accountability by having specific team or individual assignment and target completion dates. Management is responsible for making the assignments and target dates, which flow into the investigation report.

14 IMPLEMENTING RECOMMENDATIONS

The ultimate goal of incident investigation is preventing recurrence of a specific incident scenario or related similar incidents. Considerable time and resources are expended in determining an incident's causal factors and associated root causes (incident findings) and identifying recommendations (preventive actions to remedy deficiencies or mitigate consequences). Despite this effort, *the potential for a similar occurrence at other facilities remains unchanged until the incident details are communicated, findings are evaluated across other sites, and remedial recommendations evaluated and implemented.* The value of the investigation is entirely dependent on the effectiveness of follow-up activities. This chapter focuses on implementation and communication of the team's conclusions.

The investigation team's charter is typically complete when the recommendations have been submitted in the final incident report; however, the *company's* responsibilities are far from over. Management needs to approve, or in some cases formulate recommendations. Other portions of the organization may be responsible for assessing the applicability of specific recommendations to remedy similar situations at their operations, while others may be assigned responsibility for evaluation, implementation and follow-up of findings identified by the investigation team.

Implementation of recommendations is a good and necessary business practice for a variety of reasons, most notably the desire to prevent repeat or similar events. In addition, recommendation implementation often leads to strengthened management systems that improve operations across the board (safety, productivity, quality, etc.) and positively impact employee morale. There has also been an increased emphasis within organizations to identify, investigate, publicize, and take action on near-miss occurrences.

This chapter addresses:

- Major activities related to implementing recommendations,
- Examples of repeat incidents where previous incident findings were not validated and/or followed-up adequately, and
- Practical suggestions for achieving successful implementation.

14.1 ACTIVITIES RELATED TO RECOMMENDATION IMPLEMENTATION

After presentation of the incident investigation report findings and recommendations to management, follow-up activities can fall into two distinct groups:

1. Implementing recommendations as accepted by management.
2. Verifying effectiveness (auditing) of implemented recommendations.

Failure of any of these activities may eventually result in a repeat incident. Follow-up is needed to track each recommendation until all incident findings have been resolved. The investigation should produce recommendations whose effectiveness is measurable. An organization should be able to track not only the completion of recommendations, but also, their effectiveness. Figure 14.1 presents an overview of the activities recommended in this chapter.

The implementation and follow-up phase follows the review and acceptance of the recommendations by management, and the assignment of implementation responsibilities. Each recommendation should have an individual assigned as personally responsible for monitoring the implementation through to completion or hand-off to another responsible individual. If the original recommendation needs to be changed, postponed, or rejected, this decision should be fully documented. The basis for the decision should be specified, along with any new information or new options that were considered. It may be appropriate to review the changes with the investigation team or otherwise seek review/approval via an established process for addressing such issues. The allocation of resources and timing of implementation will depend upon the priority placed on each action item.

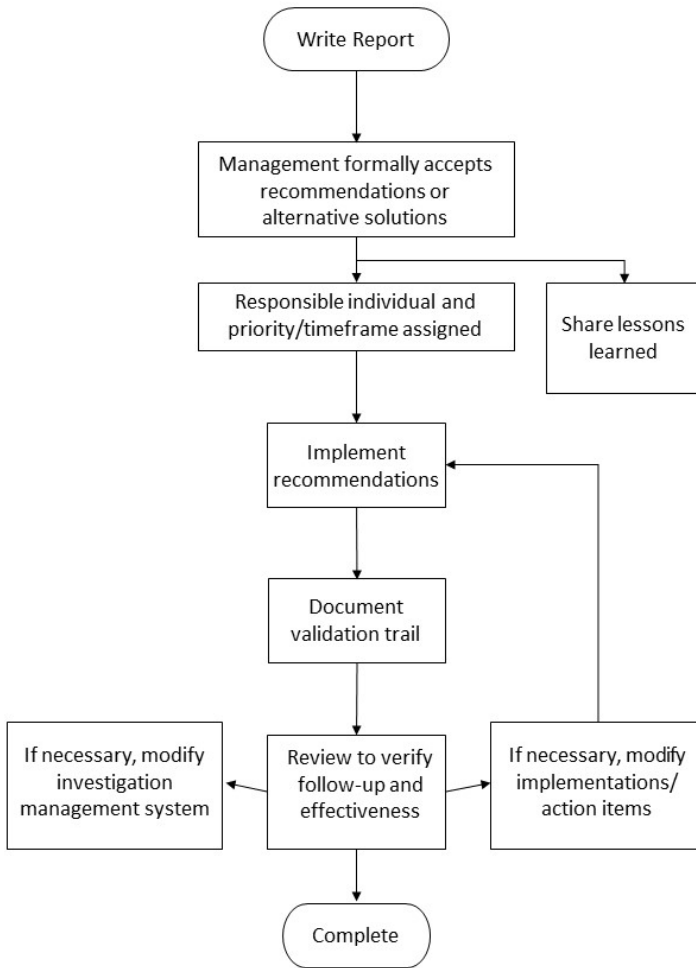


Figure 14.1 Flowchart for Implementation and Follow-up

Responsible managers should prioritize, monitor, and document progress of all actions through to completion to ensure that the corrective and preventive actions are achieving the intended results. Inevitably, some actions may result in changes to local management systems and equipment, and a rigorous Management of Change (MOC) procedure should be adopted to ensure that all potential consequences of implementing the

recommendations are understood and acceptable, and that all persons whose work assignments may be affected are aware of the changes.

Refer to Chapter 16 for more information on sharing and institutionalizing lessons learned.

Auditing is an integral step to verify that the actions have been implemented, validated to confirm intended results have been achieved, and documented to ensure lessons have been retained within the management system. If audits indicate that there are implementation gaps, remedial, alternative, or additional corrective actions may be needed.

14.2 VALIDATION OF EFFECTIVENESS – CASE STUDIES

Unfortunately, history includes examples of repeat incidents that might have been prevented or mitigated, had acceptable follow-up been completed following a previous incident investigation. This section highlights several previous events where weaknesses in the recommendation implementation process contributed to a subsequent event.

14.2.1 Nuclear Plant Incident

There were several root causes for the Three Mile Island Nuclear Power Plant incident that occurred in March 1979 (Ford, 1981). Inadequate follow-up to previous similar incidents contributed to the event. The actual initiating event for the 1979 incident was a loss of feed-water which caused the plant to trip the reactor and eventually lift a pilot-operated pressure relief valve. The coolant level lowered through loss of steam inventory, ultimately exposing the reactor core. Operators eventually turned off emergency cooling water, believing the entire plant was being flooded.

The cause of the stuck pressure relief valve was due to water contamination of the instrument air system. What was not well-publicized is that the instrument air contamination scenario had occurred twice before (in October 1977 and May 1978) in exactly the same manner. In fact, the pilot-operated relief valve had previously failed on 11 occasions, nine of them in the open position, allowing coolant to escape. More disturbing, however, the initial causal sequence of events had been duplicated 18 months earlier at another reactor site but that event was not publicized throughout the industry.

14.2.2 Aircraft Incident

The Concorde aircraft tragedy in July 1999 resulted from a fuel tank puncture caused directly by a tire failure or debris left on the runway from a previous flight (Weir, 2001). During the investigation, it was disclosed that there had been at least five previous incidents. In one of the previous incidents, a tire failed and punctured the fuel tanks, yet there was no ignition. Subsequent analysis of previous incidents suggested debris on the runway to be more likely the cause of the fuel tank rupture. Regardless, the incident investigation management systems in use at the time failed to adequately follow-up and apply lessons learned from previous investigations.

14.2.3 Petrochemical Plant Incident

At a facility in Pasadena, Texas, a serious fire and explosion occurred on a compressor section involving failure of a check valve (EPA, 1998). During the investigation by regulators, it was disclosed that another occurrence involving a failed check valve had recently taken place. The company was cited for failure to adequately apply lessons learned from previous incidents.

14.2.4 Challenger Space Shuttle Incident

The *Challenger* space shuttle disaster can also be viewed as an example of less than adequate incident investigation follow-up (Feyman, 1988). The *Challenger* space shuttle disaster was caused by the failure of an O-ring in the solid rocket booster. The presidential commission investigation report disclosed that O-ring failure had been previously identified as a serious problem for the shuttle program. In fact, concern over the potential consequences' severity resulted in a formal launch restraint being imposed six months before the January 1986 incident while follow-up actions had been initiated to resolve the problem.

Unfortunately, the actions taken did not prevent the 1986 incident. As pointed out by Vaughan's study, *The Challenger Launch Decision* (Vaughan, 1996), there is a process in organizations that can be defined as "normalization of deviance." Over time, deviations from specified practices are tolerated until, in some individual cases, the deviant practice becomes the norm. Investigators should be aware of "normalization of deviance" in all investigations.

14.2.5 Typical Plant Incidents

Repeat incidents with similar causes have often been a common occurrence. Implementing, across the organization and within the industry, effective recommendations that resolve these common causes can reduce the frequency and consequence of incidents. Typical examples of statements in incident reports have included the following potential indicators of common causes that might have been resolved through improved recommendation implementation and follow-up.:

- One of the causes of this incident was employee failure to follow an established procedure.
- Failure to depressurize the hose before disconnecting caused the exposure.
- Overfill and overflow of storage tank despite presence of high-level alarm.
- Leak caused by pump seal system failure.
- The premature failure of bearings was due to water contamination of lubrication oil.
- Leak caused by external corrosion underneath insulation covering.
- Chemical release caused by inadequate equipment isolation associated with lockout/tagout activities.
- Process relief valve lifted due to improper pressure testing practices (added nitrogen too fast).

A large number of these common events might be linked to less than adequate follow-up of findings and recommendations from previous incident investigations. The earlier investigation teams may have properly identified underlying root causes, submitted suggested preventive actions, and attempted to share results; yet the repeat occurrences continue due to incomplete implementation of recommendations or ineffective sharing of lessons learned between potentially affected parties.

14.3 PRACTICAL SUGGESTIONS FOR SUCCESSFUL RECOMMENDATION IMPLEMENTATION

Effective implementation is important to prevent incidents or mitigate consequences. A formal management system should be in place to promptly and thoroughly address each recommendation. Many regulatory agencies around the world require such a system (US OSHA, 1992). The system should ensure that each recommendation is tracked until completion or resolution

(e.g., recommendation no longer needed due to a change in process chemistry, alternative recommendation developed, etc.), should be in place. Chapter 4 addresses the overall management system needs. Specific suggestions for implementation and follow-up activities are included here in this chapter. Key considerations for effective recommendation implementation and follow-up include:

- Assignment of a responsible individual
- Action(s) to implement recommendations
- Challenges to resolving recommendations
- Changes to the management system
- Providing an audit trail
- Tracking action items
- Sharing lessons learned
- Follow-up audit

14.3.1 Assigning a Responsible Individual

An individual, rather than a department or division of the company, should be named as being responsible for each recommendation. The responsible individual should determine the most appropriate action(s) to address the recommendation. This individual should be responsible for the entire process of implementation, including monitoring the status, resolving any problems, verifying, validating, and documenting that the intended preventive action has been completed and is effective.

Formal hand-off should be planned and documented for shifting responsibilities to another person in the event of job assignment changes, retirements, etc.

14.3.2 Due Dates and Priorities to Implement Recommendations

Each recommendation should have a suggested target completion date reflecting both the urgency and the practicality of implementation. Complex recommendations requiring several steps or an extended time to complete should be assigned intermediate milestones to monitor progress of the actions. It may also be appropriate to consider additional temporary safety measures until the main actions have been completed. Alterations to recommendations and extensions to due dates should be reviewed, in light of the overall recommendation goal and subjected to an independent (i.e. not the Responsible Individual) approval process.

As an aid to priority determination, it is often helpful to risk rank each recommendation. Several CCPS publications provide guidance on the use of a variety of risk ranking techniques. (CCPS, 1989; CCPS, 1992; CCPS 2008). Additional information on hierarchies and layers of recommendations can be found in Chapter 12.

14.3.3 Challenges to Resolving Recommendations

A variety of challenges can influence effective resolution of recommendations sanctioned by management. In most cases, the investigation team conducts a preliminary examination of any possible adverse impacts of implementing the proposed recommendation. This is important because there have been instances when implementing a fix for one problem created a new problem that did not exist before, due to ineffective MOC procedures. MOC is a concept recognized by the CCPS as one of the fundamental elements necessary for successful process safety management (CCPS, 1989). The investigation team should conduct or arrange for another team to conduct a preliminary MOC examination before any recommendation is submitted to management. More often than not, these two management systems (approving / implementing action items and MOC) are handled as separate activities. An evaluation should be made to clearly understand the possible impact of all recommendations *before* implementing any action item. Additionally, a rigorous MOC system helps provide a thorough tracking system for action items.

As an example, one of the root causes of the *Challenger* disaster was inadequate MOC evaluation or communication of the findings for an earlier recommendation that attempted to prevent O-ring seal failures (Feyman, 1988; Winsor, 1989). The pressure testing procedure for the seal was changed in 1984 and actually resulted in an *increase* in the risk rather than the intended decrease in risk. A more thorough analysis of the proposed recommendation might have identified and corrected this problem before the disaster.

When recommendations reach management for approval, there is usually another examination of the costs, benefits, and potential consequences of implementing each recommendation. Cost-benefit analysis is not always easy or straightforward. Estimating cost is often straightforward; a more challenging task is to accurately determine the risk if the recommendation is rejected. Cost-benefit analysis is also used to compare different options that address the incident findings. These determinations require examining a set of scenarios, each with different

frequency and potential consequences. Accurate risk assessment is important to conducting a meaningful cost-benefit analysis. Layer of protection analysis (LOPA) (CCPS, 2001) is one tool that may be useful in this evaluation.

Another challenge to effective recommendation resolution occurs when the action intended by the investigation team is not clearly or completely stated. This avoidable mistake can lead to misunderstandings on the part of management decision-makers. A common example of obscure wording is ineffective use of the terms "consider" or "review." If the investigation team believes that a particular system defect exists and should be corrected, then the team should state this finding very clearly and recommend a specific measurable task (e.g. Task (1) "Study..", and Task (2) "Implement the findings of Task (1)..").

Any attempt to designate a recommendation as implemented and thus designated as "Closed" upon reaching an intermediate or temporary milestone should be discouraged. Typically such attempts stem from poorly worded recommendations and are based upon the promise of future actions. For example, "issue a project request for..." with a status of "Project Request Approved" is not verification that the recommendation has been "Completed". Similarly a recommendation to "consider adding ..." with a status of "consideration completed", provides no explicit documentation of the remedial corrective actions taken, if any.

In other cases where the investigation team does not believe the recommended action is mandatory, this distinction should also be clearly stated. An example would be the recommendation of a best practice activity, which could be rejected by management without major consequence. This is one of the reasons why it is useful for each recommendation statement to include comments on the consequences to be averted and the benefits associated with implementing the recommendation. Effectively written recommendations include phrases such as "in order to prevent x, implement y." It should be noted, however, that some companies have recommendation language protocols in place that may differ from this advice.

If a recommendation proposes a change in the process, the change should be managed through the MOC procedure and the associated actions should include a safety assessment which, depending on the change, may include a formal Process Hazard Analysis (PHA) study, such as a HAZOP or other methodology, before implementation. A systematic and formal Hazard Analysis approach identifies and evaluates hazards associated with the

proposed revisions. The study may uncover failure scenarios, adverse consequences, and obscure relationships that are not immediately apparent. The CCPS publication *Hazard Evaluation Procedures* (CCPS, 2008) is an excellent guide to the selection and proper application of PHA methodologies.

14.3.4 Tracking Action Items

Another challenge to effective recommendation implementation is adequate action item progress tracking, managing potential modifications, and evaluating completion effectiveness. Initial responsibilities and target dates may be properly assigned, and then in the course of normal business, competing priorities require reevaluation of realistic target completion dates. A high quality tracking system will aid in managing this common situation and prevent action items from becoming lost. A good system will automatically handle personnel changes, send reminders of assignment target dates, process status comments, identify potential delays, include up the line escalation reporting to management, etc. Some organizations require the personal participation of upper levels of management in tracking and documenting action items from process safety related incident investigations. Metrics reported to management might include trending the number of items coming due in 30 or 60 days, overdue items, and closed items. Management should also set the expectation that action item completion is a core responsibility of assigned employees.

Line management should establish a system to provide consistent information about incidents and compliance issues, together with associated follow-up actions. Progress should be reviewed regularly, and can be recorded in a report showing action status, estimated completion date, and whether an item is open or closed. When action items are completed, they can be moved to a closed punch-list for future audit trail purposes. This information will help management target interventions where they are needed to deliver timely and effective action item implementation performance improvement. Tracking the organization's performance data with respect to corrective and preventative actions can drive significant improvement in performance.

14.3.5 Follow-up Verification

A follow-up verification should be conducted after an appropriate period following the implementation. The objectives of this review are to verify that recommended actions remain in place and are working as intended. The

effectiveness verification process should start with determining that the investigation findings and recommendation justifications were clearly understood by the implementation team. The team should be assessing not only whether the actions completed, but also how effectively the action closure remedied the original findings.

A review also presents an opportunity to review the retention of the lessons learned and to identify any practices, knowledge, or awareness items that are being lost. The review should therefore consider whether the lessons learned were communicated appropriately throughout the company and to others in the industry.

The review may determine that a recommended action was ineffective. Engineers, designers, or the person responsible for implementation may find a reason why the original recommendation did not work or was not as effective as intended. If modifications have been made, the justification for these should be documented and communicated to the same extent as that of the original recommendation, and there should be evidence of approval in accordance with the applicable management system.

Although not essential, it may be helpful to include a member of the original incident investigation team on the audit team to help assure that the final implemented actions address the original issues in an acceptable manner.

15 CONTINUOUS IMPROVEMENT FOR THE INCIDENT INVESTIGATION SYSTEM

Regulations and guidance concerning the investigation of incidents varies between countries and it is important to determine the legislation that applies at the incident site. It should be noted, however, that in terms of process safety, regulations are a minimum requirement and may not be enough to prevent major accidents.

In the US onshore industry, the OSHA Process Safety Management (PSM) regulation 29CFR 1910.119 (m) (US OSHA, 1992) clearly defines the requirements of investigations conducted in “covered” facilities. The US EPA Risk Management Program (RMP) regulation in 40CFR Part 68.81 (US EPA, 2004) mirrors the US OSHA requirements. In the US offshore industry, the Safety and Environmental Management System (SEMS) rule made mandatory the API RP 75 requirements including those addressing investigation of incidents. During reviews of investigation system effectiveness, it may be helpful to confirm that the investigations address all necessary regulatory requirements.

Section 68.42 of the US EPA RMP standard (US EPA, 2004) requires certain specific information to be documented for each incident that is included in the five-year summary of incidents. Some of the required data includes:

- duration of the release,
- quantity of the release,
- notification of offsite responders, and
- changes to the process that resulted from the investigation.

Table 15.1 lists these requirements and provides a record of compliance for future analysis. Requiring completion of this record for each process incident investigated enhances the probability that all elements are covered. Auditing of incident reports against these requirements provides a forum for continuous improvement in meeting compliance requirements.

This table may also be incorporated into the PSM program assessment/audit protocol and used during periodic PSM program evaluations. (US OSHA, 1992). The PSM program also requires that incidents are incorporated into the site Process Hazards Assessments when they are

revalidated (5-year interval). This is an important means to institutionalize the lessons learned from the incident, as discussed in Chapter 16.

15.1 REGULATORY COMPLIANCE REVIEW

Table 15.1 Requirement Compliance Checklist (USA OSHA/EPA)

Requirement Statement	Compliance?	
	Yes	No
The Investigation Itself:		
1. An investigation must be performed for each incident in a covered process that did or could reasonably have resulted in a catastrophic release of: <ul style="list-style-type: none"> -a highly hazardous chemical per US OSHA PSM or, -a regulated substance per US EPA RMP. 		
2. The investigation should start as soon as is reasonably possible, but must start within 48 hours following the incident. (This requires documentation of date and time at which the investigation began.)		
3. The investigation team is to be composed of: <ul style="list-style-type: none"> -at least one person knowledgeable in the process involved, -a contract employee if the incident involved work of the contractor, -any other person with appropriate knowledge and experience that is required to thoroughly investigate and analyze the incident. 		
The Report and Findings:	Yes	No
1. A report is required at the conclusion of the investigation and the report must include: <ul style="list-style-type: none"> -date of the incident -date the investigation began -a description of the incident -the factors that contributed to the incident -recommendations resulting from the investigation 		
2. The report must be reviewed with all affected personnel whose jobs are relevant to the investigation findings, including contract employees where applicable.		
3. A system must be in place and utilized to promptly address the incident report findings and recommendations.		
4. The investigation report must be retained for five years.		

Table 15.1. Requirement Compliance Checklist (USA OSHA/EPA) (cont.)

Requirement Statement	Compliance?	
	Yes	No
Five-Year Accident History (Additional EPA Requirements)		
(1) Date, time, and approximate duration of the release.		
(2) Chemical(s) released.		
(3) Estimated quantity released in pounds and, for mixtures containing regulated toxic substances, percentage concentration by weight of the released regulated toxic substance in the liquid mixture.		
(4) Five- or six-digit NAICS code that most closely corresponds to the process.		
(5) The type of release event and its source.		
(6) Weather conditions, if known.		
(7) On-site impacts.		
(8) Known off-site impacts.		
(9) Initiating event and contributing factors if known.		
(10) Whether offsite responders were notified if known.		
(11) Operational or process changes that resulted from investigation of the release and that have been made by the time this information is submitted in accordance with §68.168.		
(12) Level of accuracy. Numerical estimates may be provided to two significant digits.		

In the UK onshore industry, the reporting of incidents falls under RIDDOR (Reporting of Injuries, Diseases and Dangerous Occurrence Regulations 2013). These regulations clearly define the types of incidents that should be reported and the records that must be kept, but does not cover the scope of the investigation. For major incidents involving processes that are covered by the COMAH (Control of Major Accident Hazards) regulations, regulation 26 (COMAH, 2015) provides instructions and high-level guidance on the investigation to be carried out by the competent authority and supported by the facility owner/ operator. The UK HSE (Health and Safety Executive) has also published a guide for investigating incidents and accidents, (HSE, HSG 245, 2004) which includes a series of tables that could be used as a measure of compliance with recommended practice.

In the EU, the Seveso III directive is the principal legislation dealing with the control of onshore major accident hazards involving dangerous substances. Other guidelines and standards include:

- Mexico - NOM standard
- Canada - PSM standard (non-regulatory), with individual occupational health and safety legislation for the fourteen jurisdictions
- Singapore - MOM standards
- China - SAWS guideline.

15.2 INVESTIGATION QUALITY ASSESSMENT

In order to ensure that the investigation process operates to the highest standard, it is necessary to periodically review the entire process and associated management system, the individual components, and the relevance and implementation of findings. Based on the review findings, it may be appropriate to update the investigation process, the training of individuals involved or the associated systems or procedures. For incident investigations, this can be done by listing the critical elements that should be addressed in an investigation and assessing actual performance against those criteria. Table 15.2 is an example audit sheet.

For smaller companies, a member of the process safety management team could be responsible for providing a systematic approach for continuous improvement of the incident investigation process. Alternatively, for larger facilities, an incident investigation subcommittee could be established. The subcommittee would report to the site process safety management committee and would have a charter to ensure that all incident investigation procedures exist and are updated, all incidents are reported and analyzed, and all recommendations are completed. The committee could also ensure adequate training is carried out for new members of the committee as well as for the site incident investigation team.

Table 15.2 Investigation Key Element Audit Checklist

Investigation Key Element Query	Yes	No
1. Are there written procedures or protocols for reporting and investigating process safety incidents?		
2. Has the investigation team leader been trained (qualified) to lead investigations and to use appropriate investigative tools?		
3. Does the investigation team leader have independence from the issue to be investigated to the point that there is no question as to that person's objectivity?		
4. Were the necessary skills available either on the investigation team or readily available to the team when needed?		
5. Have pertinent causes and discovery processes, including data gathered, been recorded and documented?		
6. Was evidence gathered and preserved properly, including a documented chain-of-custody?		
7. Were the proper investigative techniques applied correctly?		
8. Did the investigation go beyond the immediate or obvious causes and discover contributing causes?		
9. Did the investigation address all facets of all causes?		
10. Were the underlying root causes identified?		
11. Were the management system failure(s) identified?		
12. What other resources, techniques and/or tools could be used to make the next investigation better? Discuss below.		
13. Were audit/ review forms completed for each investigation?		
14. Were there any legal issues from this latest investigation that were related to incident investigation reports or documentation that should be resolved before the next major incident investigation?		
15. Is there a need to change any internal communication practices?		
16. Is there a need to change any team training or team procedures?		
17. Did the investigation team check whether any similar incidents have occurred at the facility in the past and if so, were these evaluated for relevance to the current incident?		
Discussion:		

15.3 CAUSAL CATEGORY ANALYSIS

Each company's management style and safety management systems have strengths and weaknesses. These strengths and weakness tend to influence the types and severity of incidents that might occur. An analysis of incident investigation findings, in terms of causal factors and root causes, may identify broad areas or management systems that contribute to a higher proportion of incidents.

Causes of incidents that repeat over time may also be indicative of a weakness in the investigation system (e.g., lessons are not being learned). The determination of these management system failures allows a broader, more effective approach to the reduction of common cause weaknesses and prevention activities than addressing individual causes might. Table 15.3 is an example of one way to accumulate this data for analysis by using causal categories.

Instructions: Review each classification statement to determine if it is TRUE or FALSE for the incident investigation finding in question. Any statement that is answered with FALSE presents an associated management system improvement opportunity.

Table 15.3 Example Categories for Incident Investigation Findings

Category	Circle	Defining Statements
Design	T / F	The current design used the correct specifications and was built such that it was adequate for the intended service. (This includes design logic, hardware, installation accuracy, arrangement, and ergonomic factors.)
Process Controls	T / F	The control system(s) for the equipment or activity in question performed in accordance with the design logic, programming, or other instructions. (This addresses the actual control operation or execution. It would not include control logic that is in the "design" category.)
Administrative Procedures	T / F T / F T / F T / F	<p>The administrative procedures were:</p> <ul style="list-style-type: none"> •available •adequate •accurate •approved and enforced <p>These are the procedures covering broad organizational needs such as management of change, design and installation expectations (including avoiding low piping that someone could hit their head on and providing logical labeling), procurement (including approving substitutions and vendor equivalents), implementation (including defining training requirements and administrative support systems), safety (including specifying appropriate protective gear), environmental compliance, housekeeping standards, and emergency response.</p>
Operation Procedures	T / F T / F T / F T / F	<p>The operational procedures were:</p> <ul style="list-style-type: none"> •available •adequate •accurate •approved and enforced
Maintenance Procedures	T / F T / F T / F T / F	<p>The maintenance procedures were:</p> <ul style="list-style-type: none"> •available •adequate •accurate •approved and enforced <p>(The focus of this category is the actual maintenance tools, techniques, and standards for work that go beyond the traditional scope of normal inspection and preventive maintenance activities.)</p>

Table 15.3. Example Categories for Incident Investigation Findings (cont.)

Category	Circle	Defining Statements
Maintenance Procedures	T / F T / F T / F T / F	The maintenance procedures were: <ul style="list-style-type: none"> •available •adequate •accurate •approved and enforced (The focus of this category is the actual maintenance tools, techniques, and standards for work that go beyond the traditional scope of normal inspection and preventive maintenance activities.)
Training	T / F T / F	Training was: <ul style="list-style-type: none"> •available and timely •adequate and verified to be effective to achieve functional and compliance requirements
Inspection and Preventive Maintenance	T / F	Inspection and preventive maintenance were in accordance with applicable procedures, manufacturer's or experience-based recommendations and governing standards, and were adequate for the service conditions.
Equipment and Materials	T / F	The equipment, parts, and materials as initially procured were as specified, were not defective, and met or exceeded the applicable specifications.
Personnel Fitness	T / F	Personnel were "fit for duty." (Includes physical/mental/ emotional states and addresses preexisting physical conditions, substance abuse, and other related concerns.)
Human Actions	T / F	Personnel actions, activities, and decisions were in accordance with procedures, training, and expected workplace standards.
External	T / F	External items including weather and external third party actions/events were not creating out-of-design conditions.
Other	T / F	The incident has been satisfactorily classified in one or more of the above categories.

It is important to understand that the above approach is only used *after* the investigation has been concluded. It is not a technique to be used for the investigation itself; rather it is an aid to identify the broad categories into which the findings of investigations are falling.

An analysis of the data collected will provide management with information on root causes and causal factors that repeat, which could be indicative of an improvement opportunity for the incident investigation system or another management system.

15.4 REVIEW OF NEAR-MISS EVENTS

As discussed in Chapter 5 (Initial Notification, Classifying and Investigating Process Safety Incidents), the reporting and investigation of near-miss events is an essential part of the safety management process. While the scale of the investigation for a near-miss may be significantly lower than that for a larger event, the learning can be just as relevant. Further benefits of investigating near-misses include:

- More frequent investigations and learning.
- Greater involvement of staff with the investigation and learning process.
- Improvements in process safety culture.

Encouraging the reporting and investigation of near-misses can often lead, in the short term, to an apparent increase in the number of “incidents” albeit at a lower level of classification. This pattern is a useful indicator that the message about the importance of conducting investigations, whatever the scale of the incident was received by the workforce. In the longer term, the number of near-misses may start to decrease, although, more importantly, there should be a reduction in the number of the larger incidents.

A review of the causes and recommendations arising out of near-miss events should be conducted on a periodic basis to identify common factors that may be targets for improvement. This process could be included the Recommendations Review shown below in 15.5, or part of a separate process.

15.5 RECOMMENDATIONS REVIEW

To effectively address the findings of an investigation, appropriate recommendations should be drafted and acted upon within the agreed timescale. Recommendations should accurately translate the investigation findings into actions that are “SMART” (Specific, Measurable, Agreed/Attainable, and Realistic/ Relevant, with Timescales; see 12.2.2). They should clearly define what is to be done so that the implementer understands not only *what* to do, but *why*. A well-written recommendation will also identify the consequences that are being avoided or abated, and/or the likelihood of a reduction of consequences or occurrence. Periodic checks or audits of

recommendations arising from incident investigations provide managers with a better understanding of the location and nature of potential problems.

Table 15.4 is an example of a recommendation review checklist.

Table 15.4 Recommendations Review Checklist

Recommendations Review	Adequate?	
	Yes	No
1. Do the recommendations address the underlying or root causes?		
2. Is there a recommendation that addresses each root cause?		
3. If there are contributing or enabling causes identified, are there corresponding recommendations if warranted?		
4. Do the recommendations clearly identify what is to be done and why?		
5. Is each recommendation feasible?		
6. Will the recommendation(s) actually reduce the risk by lowering either the probability of occurrence or lessening the consequences?		
7. Is a system in place for tracking each recommendation, including: (a) Assignment of an individual responsible for completion of each recommendation? (b) Target-for-completion dates for each recommendation? (c) Periodic status checks and reports? (d) Documentation of final resolution of each recommendation?		
8. Is a formal documented system in place that assures each recommendation is evaluated through the management of change program before being implemented?		
9. Is there a system in place that assures communication of pertinent facts regarding the incident, the recommendations, and status to affected employees and contractors?		
10. Is a system in place that actively shares relevant process safety knowledge and lessons learned across the organization, including methods for making information available to relevant stakeholders, per Responsible Care® ? (ACC, 2012)		
11. Is there a system in place that provides metrics/ KPIs to staff (including senior management) on the progress of investigations and actions arising from the investigation? See section 15.6.		

15.6 INVESTIGATION FOLLOW-UP REVIEW

Table 15.5 offers prompts to evaluate the effectiveness of incident investigation follow-up. Not all options are appropriate for all investigation management systems or every investigation. The reader should determine which should be used and where.

Table 15.5 Example Follow-Up Checklist

Follow-Up Issues	Addressed?	
	Yes	No
1. Are the incident investigation follow-up expectations clearly stated in the incident investigation policy statement?		
2. Does the incident investigation management system include: <ul style="list-style-type: none"> -Strong encouragement for near-miss reporting and investigation? -Requirements for formal periodic status reports of recommendations? -Requirements for documentation of a formal plan for sharing lessons learned? -Provisions for providing appropriate report information to various levels as needed? -Provisions for modifications of original recommendations? 		
3. Are appropriate levels of upper management aware of and involved in monitoring the implementation or resolution of recommendations and resultant action plans?		
4. Have audit protocols been established that include examination of effective implementation of: <ul style="list-style-type: none"> -Investigation follow-up measures? -Recommendations? 		
5. Are incident investigation follow-up expectations included in training and competency systems?		
6. Are actions from investigations being completed within the specified timescale?		
7. Was the implementation of the recommendations effective?		
8. Has the investigation team leader provided the members of the investigation team and their supervisors structured feedback on their performance throughout the investigation?		

15.7 KEY PERFORMANCE INDICATORS

The safety management system should include a series of metrics or key performance indicators (KPIs) to provide management with regular reports on all aspects of process safety. Further details on metrics are provided by the CCPS publication: *Process Safety Leading and Lagging Metrics* (CCPS, 2012), API RP 754: *Process Safety Performance Indicators for the Refining and Petrochemical Industries* (API, 2017),¹ and the HSE (UK) guide HSG254: *Developing Process Safety Indicators* (HSE, 2006).

The process safety KPIs should include measures on the incident management system, including the progress on recommendations. For example, a software database could be used to provide statistics and trend graphs on measures such as:

- Number of ongoing investigations.
- Number of completed investigations
- Time to initiate investigations.
- Number of recommendations completed.
- Number of open recommendations.
- Percentage of recommendations completed within agreed timescale.
- Number of recommendations where timescale for implementation were revised.
- Categories of root causes and causal factors.
- Percentage of repeat incidents that had similar root causes or involved similar causal factors to those identified from previous investigations.
- Percentage of similar types of incidents or near-misses.
- Ratio of incidents to near-miss events.
- Number of communications on lessons learned that are shared with other parts of the organization.

A periodic review of the KPIs should be conducted, involving senior management personnel. Any adverse trends in the performance should be recorded along with the details of action required to address any potential issues.

15.8 SUMMARY

This chapter considers processes that can be used to ensure that there is a continuous improvement of the incident investigation system. Periodic audits of incident investigation reports, including near-miss reports, should be conducted to check that they properly address all root causes and that the recommendations are SMART. A review of causal categories should help to identify any areas where similar events are recurring and may be indicative of inadequate learning from previous incidents. The system that tracks the progress of recommendations and their effectiveness should be reviewed to ensure that they are being completed to the necessary timescale and will be successful in preventing future incidents. The identification of any gaps in the systems will help to drive continuous improvement, which also helps demonstrate to the workforce management's commitment to the investigation process.

16 LESSONS LEARNED

“Organisations do not learn from the past or, rather individuals learn but they leave the organisation, taking their knowledge with them, and the organisation as a whole forgets.”

—Lessons from Disaster, Trevor A Kletz, IChemE 1993

Incidents are costly in terms of injuries to personnel, repairs, environmental clean-up, business interruption, manpower, reputational damage and other factors. A well-conducted investigation generates lessons learned that can be applied to prevent the recurrence of a similar incident, or a different incident with similar root cause(s). The lessons could be applied at the incident site, other sites within the organization, other companies within the industry, or even different industries. Typically, the lessons learned address management system failures, which are often root causes of incidents.

If the lessons learned are properly communicated and incorporated into the organization’s Institutional Knowledge, facilities that are remote from the incident site can also benefit from the value of the incident learning without suffering the pain of a similar incident. Such properly incorporated institutional knowledge remains effective decades after the incident occurred. Lessons learned should also be retold at appropriate intervals, both to preserve organizational memory, and to maintain a sense of vulnerability amongst personnel. Building a culture of “telling the story” will improve process safety awareness and appreciation among staff and management.

This chapter focuses on how to identify and extract key learning(s), methods to share the learning and how to build the learning into the organization’s Institutional Knowledge.

16.1 VARIOUS SOURCES OF LEARNING FROM INCIDENTS

16.1.1 Internal Sources

After an incident has occurred at a facility, personnel on site may be aware of some details of the circumstances and consequences of the incident. They might have witnessed the event or discussed it with a colleague who was involved. However, they may not have access to accurate information and there may be much speculation about the causes of the incident. It is important that the causes and relevant lessons learned from the incident are properly communicated throughout the facility.

Facilities should also build up records/ archives of incidents, including near-misses, so that the lessons learned can be communicated periodically to staff as a “reminder” of the events and the associated lessons. Some of these incidents or near misses could be relatively minor, such as the failure of a protection system that did not lead to an incident. Nevertheless, the learning could still be extremely valuable and may prevent a more significant event from occurring at a future date. An additional benefit of collecting and trending information on minor events is that it helps in the identification of potential problems, such as issues with a certain type of equipment, which may justify further investigation.

16.1.2 External Sources

Staff may not be aware of incidents that occur at other facilities within their organization, or perhaps at an external company. Since the learning from some of these external incidents can be highly relevant to another facility, the organization should have a system of assessing the lessons learned from such events and communicating relevant details to the staff. One person should be assigned the responsibility of identifying those incidents, extracting relevant lessons learned, and ensuring that the details are communicated in an appropriate way to appropriate staff in the organization.

The sources of knowledge regarding these events include news media, professional institutes, investigation authorities and various texts, articles and conference papers. Many textbooks have also been written on significant events and there is great value in reminding personnel of the lessons learned from events that occurred long ago on similar processes or with similar equipment.

16.1.2.1 Newsletters

Sources of newsletters that are aimed at sharing learnings include the following:

- The Process Safety Beacon, produced by CCPS (CCPS, 2018-1)
- US Chemical Safety and Hazard Investigation Board (CSB) Safety Digest (CSB, 2018-1)
- Loss Prevention Bulletin, produced by the IChemE in the UK (IChemE, 2018-1)
- Safety Lore, produced by the IChemE Safety Centre in the UK (IChemE, 2018-2)
- Learning Sheet, produced by the European Process Safety Centre (EPSC, 2018)
- The ICI Safety Newsletters, mainly issued by Trevor Kletz (Kletz, 2018)

16.1.2.2 Incident Reports

More detailed incident reports can be found on the internet, including the following:

- Health and Safety Executive UK (HSE, 2018) - a series of reports on major incidents
- Chemical Safety Board (CSB, 2018-2) - reports and videos on major incidents

16.1.2.3 Incident Databases

A number of on-line databases are available, including:

- European Commission Major Accident Reporting System—a searchable database of incidents in the EU (eMARS, 2018)
- The Bureau for Analysis of Industrial Risks and Pollutions (BARPI, 2018)—Analysis, Research and Information on Accidents (ARIA) database—a searchable database of incidents and other reference material (BARPI 2018)
- CCPS Process Safety Incident Database (PSID) (CCPS, 2018-2)

Other sources of information may include insurers and other government agencies such as the National Transportation Safety Board (NTSB) for railcar events, OSHA, etc. Further references are provided in the References section.

16.1.3 Cross-Industry

Many organizations tend to recognize only those incidents that have occurred in similar operating environments or in similar processes within the same industry sector. For example, the chemical industry currently does not have a common platform to exchange incident information with the oil and gas sector, pulp and paper, or other industries. Given that the hazards, equipment, and processes used may be very similar in these industries, there is a significant need and opportunity to share lessons across geographical or industry boundaries.

Lessons learned from entirely different industries (such as the airline industry) may also be relevant to the chemical processing industry since there are common touchpoints (human factors, prestart checks, etc.). These opportunities should not be overlooked.

Material for learning from incidents can be obtained from a number of sources, as detailed in 16.1.2.

16.2 IDENTIFYING LEARNING OPPORTUNITIES

A well-written investigation report and associated recommendations should be structured in such a way that the lessons learned are clearly identifiable. However, this is not always the case and management must play a role in ensuring that the learning opportunities are identified and communicated to appropriate personnel and across organizational boundaries.

How this is organized will depend on the type and size of company or facility. Nevertheless, at least one member of staff, in a management and/or safety function, should be responsible for this activity; receiving incident reports from within the organization as well as seeking out information from external events from sources such as those listed in 16.1.2. This person or group should then extract the key learning that may be relevant to one or more of their facilities and prepare a communication aid to allow this learning to be disseminated to staff.

A series of questions that can be used to help identify key learning opportunities is provided below in Table 16.1.

Table 16.1 Questions for Identifying Learning Opportunities

1. What are the synergies or similarities between the reference case and your own operation?
2. Are there similar chemicals used at your facility?
3. Do you have similar processes or equipment at your facility?
4. How does your site layout and infrastructure compare to that of the reference case?
5. How does your operation or organization compare to that of the reference case?
6. Are there any trends or patterns in your own operations that reflect those in the reference case?
7. Could a similar incident occur at your facility? Why or why not?
8. What are the potential consequences of this type of incident occurring at your facility? What is the most probable outcome? Why?
9. Have the immediate causes of this incident ever contributed to a loss at your facility? What were the consequences?
10. How have incidents such as these typically been dealt with at your facility?
11. How would an investigation at your facility have likely dealt with this type of incident? Would it have drawn the same conclusions?
12. How do the PSM systems at your facility compare to those described in the case study?
13. Were there effective process safety initiatives or other positive factors that limited the consequences in the reference case? Does your facility or operation provide such benefits or opportunities?
14. How effectively would your PSM systems have prevented or limited such an incident at your facility?
15. Is there anything you could do to reduce the likelihood of a similar incident at your facility?
16. Is there anything described in the reference case that your facility should eliminate or avoid?
17. What direct learning can you apply to your own PSM systems or operation as a result of this incident?
18. Is there anything you should implement at your own facility as a result of what you learned from this case?
19. Is there anything from this incident that could influence future decisions and direction within your own organization?
20. Is there someone else who would benefit from having this information? If so, who are they and how can you get it to them?

16.3 SHARING AND INSTITUTIONALIZING LESSONS LEARNED

Once the learning opportunities have been identified, they should be shared across the organization with relevant personnel and at an appropriate frequency. However, there should be a balance in terms of the frequency of the communications, to avoid information overload. The content of the learning should be relevant and the level of complexity should be tailored to suit the audience. An engineer might want to read through a detailed report; whereas an operator or technician may learn more from a single page document. If in doubt, the advice is to keep it simple.

There are several methods by which the learnings can be shared/communicated throughout the organization. Some of these methods are transient, although the learnings can contribute to Institutional Knowledge if they are incorporated into training courses or otherwise saved, catalogued and re-used at suitable intervals. Other methods contribute to Institutional Knowledge either by providing a general understanding of how incidents occur or by expressly capturing relevant past lessons learned, for example, by being incorporated into company policies and procedures.

- a) **Safety Moments.** A “safety moment” is a brief discussion on a safety matter that could include a learning event, near-miss, safety initiative or any other safety-related topic. Some organizations start every meeting with a safety moment. In addition to sharing learning from events, this is an excellent way of demonstrating that safety is considered a top priority throughout the organization, up to the level of senior management and executive.
- b) **Safety newsletters/ bulletins.** These can be prepared internally by the organization, detailing lessons from incidents within and outside the organization. A bulletin can convey a key learning message on a single or two-sided sheet. Details of some external sources of newsletters are provided in 16.1.2, and example bulletins are included in 16.5.
- c) **Case studies.** More detailed papers and presentations on case histories, both inside and outside the organization can be prepared for sharing lessons learned. The material could be anonymized for sharing outside the organization; this can often lead to external companies reciprocating with lessons they have learned from incidents.

- d) **Safety meetings.** These should take place regularly throughout the organization. Some companies have a mandatory weekly safety meeting that is attended by all senior management, where safety performance is discussed and relevant incidents, particularly near-misses, are presented and reviewed. The information is then cascaded throughout the organization, to include Plant Management, Maintenance, Projects, Engineers, Technicians and Operators.
- e) **Toolbox talks.** In the workplace, "Toolbox talks" are typically led by Managers/ Supervisors and involve Technicians and Operators, where safety issues and learnings are discussed at a local level. When reviewing previous incident, the focus should be on "has/ could this happen here", "what do we have in place to prevent or mitigate such an incident?" and "is there anything we can do to reduce the risk of such an incident at our facility?" Sharing only the basic facts can be sufficient to start this conversation. Material from safety newsletters and case studies can be used, or information from the senior manager's safety meetings can be cascaded to staff. Videos, especially those produced by the CSB provide good material. A mechanism to provide feedback of process safety issues, which cannot be addressed at local level, to senior management is an important part of this process.
- f) **Archives of incidents.** A web-based, searchable database of previous incidents provides all staff with access to the accumulated learning within the organization. Analysis of causal factors and lessons learned from a database of incidents can help to establish process safety priorities and drive follow-up action and commitment. If an incident at a facility matches an industry pattern in terms of common failure mechanisms, process hazards, equipment details, or associated consequences, there might be an opportunity to target areas for improving process safety. The database could also be used prior to conducting an activity, e.g. project, turnaround, control of work, PHA/ HAZOP, to avoid making the same mistake again.
- g) **Hazard Identification and Risk Assessments (HIRAs).** Many sites incorporate incidents into their HIRAs. This ensures that an appropriate number and type of protection layers are provided to prevent recurrence of the incident and can also provide a useful historical reference. It is important to ensure that the historical

incident reference and associated lessons learned are retained when the HIRAs are redone.

- h) **Procedures.** Many sites include a “Consequences of Deviations” (COD) section in their operating procedures. If a previous incident has occurred from which lessons learned relate to operations described by the procedure, a brief description of those lessons with a linked reference could be listed in the COD section. The reference could be linked to an incident database that can provide more details as appropriate. Since operating procedures are a permanent record this is one of the most reliable means to institutionalize lessons learned from incidents.
- i) **Corporate standards and initiatives.** Lessons learned from a single event or from a review of trends from an incident database may lead to changes in corporate EHS, process safety and engineering standards and/or a revision of auditing specifications. This may include the development of corporate-wide initiatives.
- j) **Courses/ classes/ training programs.** All staff should undergo a period of refresher training, where process safety and learning from incidents should be a key element, thereby institutionalizing both the material and the learning process. Ideally, training days should be built into the shift patterns to ensure good attendance.

16.4 SENIOR MANAGEMENT – INCIDENT SHARING AND COMMITMENT

A high level of technical competence is required to oversee the operation of a manufacturing plant. Senior management must understand the full consequences of all decisions related to process safety. While some learn from direct experience, not all senior executives have had sufficient exposure in an operating environment to appreciate everything that can possibly go wrong and lead to major incidents. Major losses are rare, even in large corporations, and it is often necessary to look outside to gain sufficient knowledge of previous process safety incidents. It is therefore important that senior management, up to and including Board Level, are involved in discussions about process safety incidents. Their direct involvement in sharing key learnings from incidents, both recent and historic, helps to maintain a sense of vulnerability at the highest levels within the organization.

Learning from incidents also requires a willingness to change and adopt new and improved practices when appropriate. Management commitment is crucial to successful implementation in these cases.

In addition, senior management should be highly visible in their commitment to process safety, the process of learning from incidents and action they may be required to take. This commitment and visibility of senior management can be achieved by various means, including:

- Involvement in the regular communication processes on safety performance and goals, learning events and company safety initiatives;
- Being receptive and responsive to feedback from the plant floor;
- Recognizing and rewarding the reporting of near misses and associated lessons learned;
- Leading by example, including encouraging “stop work” principles; and
- MBWA (Management by Walking Around). Management (senior executives, technical authorities, supervisors) should regularly interact informally with staff, including discussing recent incidents, investigations and associated learning and progress of recommendations.
- Action taken at senior level in response to the specific findings & recommendations, often involving commitment from the business, either at a specific facility or cross-business.

16.5 EXAMPLES OF SHARING LESSONS LEARNED

Sharing lessons can come from a variety of sources and in a variety of formats, depending on the organization and the intended audience. Various examples are provided below.

16.5.1 Creating a Process Safety Alert from a Case Study

Case studies provide an opportunity to show the consequences of process safety decisions and the lessons learned. However, they are not usually presented in a format that is helpful for communicating key lessons learned to the shop floor. The case study in Appendix D involves an explosion of a catalyst storage tank. One of the findings was that a high level alarm had

been inhibited. The associated recommendation was to reinforce the management of change system. This is an issue that occurs across many industries and these details could be extracted from the case study, summarized on a single sheet as shown below in Figure 16.1 (Safety Alert) and used to communicate the common learning that applies.

SAFETY ALERT 1234 – MANAGEMENT OF CHANGE

What Happened?
An explosion occurred when a pipe failed in a polyethylene plant, releasing isopentane, which subsequently ignited. One person was killed, four were injured and there was extensive damage.

Why did it happen?
There were several factors that led to the incident, one of which was that the system pressure increased to well above normal. The investigation found that a batch vessel has overfilled, leading to the increase in pressure of the system. Further investigation into the reason for the overfilling identified that:

- a) The operating level of the batch vessel had been changed, sometime before the day of the incident, from 70% to 85%, although the high level alarm was still set at 80%.
- b) The high level alarm became a nuisance because it went off every batch, so the operators inhibited the alarm, preventing it from functioning.
- c) On the day of the incident, the vessel was overfilled, but nobody noticed the high level on the level gauge, and the inhibited alarm did not sound.

What are the Key Lessons?

- The bypassing of alarms must be carried out under the Management of Change (MOC) procedure.
- The process safety implications of a change to operating conditions should be considered and may involve the MOC procedure.

Had the safety and operability implications for the change of operating level been properly considered, the need to raise the setting of the high level alarm would have been identified.

How might this affect my work?

- Engineers and Supervisors: If there are any proposed changes to operating conditions, conduct a risk assessment/ PHA under the Management of Change procedure. Make sure that the implications are fully understood, documented and training is provided.
- Operators: If you notice a change in operating parameter, find out if this should be carried out under the Management of Change Procedure.
- Operators: If an alarm keeps coming up and becomes a nuisance, report it to your supervisor/ manager.
- Operators/ Supervisors: Do not bypass alarm systems unless this has been through the management of change procedure. Use of the short-term (24hr) bypass procedure may be used, provided the associated risk assessment is carried out and it is reported to management.

Figure 16.1 Example Safety Alert

16.5.2 Safety Newsletter

A safety newsletter should convey the learning as concisely as possible.

An example of a safety newsletter is the monthly issue of the CCPS Process Safety Beacon (CCPS website), which has been produced for a number of years. A copy of the April 2018 issue is provided in Figure 16.2.





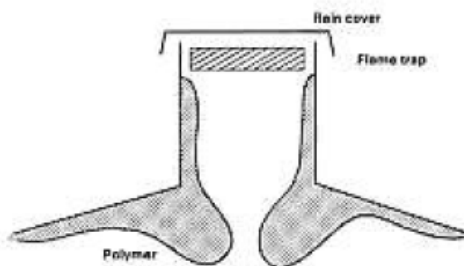
 <p>www.aiche.org/ccps</p>	<p>Process Safety Beacon</p> <p>http://www.aiche.org/CCPS/Publications/Beacon/index.aspx Messages for Manufacturing Personnel</p>	<p>This issue sponsored by ioMosaic</p> <p>www.iomosaic.com</p>
<p>Maintain a Sense of Vulnerability</p>		<p>April 2018</p>
<p>Maintaining a sense of vulnerability is an essential characteristic of a good process safety culture. What does “maintain a sense of vulnerability” mean? It means that everybody in your plant:</p> <ul style="list-style-type: none"> ➤ Has a high level of awareness of the hazards of your processes and materials. ➤ Is constantly vigilant for symptoms of weaknesses that might foreshadow more serious events. This includes reporting near miss events (March 2018 <i>Beacon</i>). ➤ Avoids complacency that might result from good past performance and a good safety record. <p>On April 15, 1912 (106 years ago this month) the ocean liner <i>Titanic</i> sank in less than 3 hours after hitting an iceberg in the north Atlantic Ocean, with the loss of over 1,500 lives. There are many examples of a failure to maintain a sense of vulnerability in the design and operation of the <i>Titanic</i>. For example:</p> <ul style="list-style-type: none"> ➤ The ship was perceived to be “unsinkable” resulting in poor critical safety decisions. For example, water tight bulkheads stopped two decks below the main deck. Lifeboats were considered “unnecessary” and the number of lifeboats was reduced from 64 to 16, so there were not enough for all passengers and crew. ➤ The captain was considered to be overconfident in his seamanship and the invincibility of his ship. ➤ The ship was traveling at high speed, although its course was through floating pack ice. Despite warnings about icebergs from other ships, at no time was any order to slow down given. 		
<div style="display: flex; justify-content: space-around;">    </div>		
<p>Do you know?</p> <p>Failure to maintain a sense of vulnerability has been a factor in process industry tragedies. For example, in December 1984 a toxic gas (methyl isocyanate – MIC) release in Bhopal, India caused thousands of fatalities. Following the tragedy, it was found that several critical safety systems had not been functioning for some time.</p> <ul style="list-style-type: none"> ➤ A vent gas scrubber and flare tower were out of service. ➤ A refrigeration system for the MIC storage tank had been left idle. ➤ Pipe blinds that would have prevented the water contamination that initiated the incident had not been installed. 	<p>What can you do?</p> <ul style="list-style-type: none"> ➤ Understand the hazards of your process and materials. Know what the worst-case incident is, and what safety systems and procedures are in place to prevent it. Understand how you can be sure that those systems and procedures are working properly, and inform management if you see weaknesses. ➤ Never think “it can’t happen here” or “it can’t happen to me.” It can! ➤ Encourage everyone at your plant to have a calm awareness that the worst-case scenario can happen, and it could happen right now! Know what you can do to prevent it, what to do if it happens, and always be ready to follow emergency response procedures. ➤ Understand the potential impact of the full range of events which could occur in your plant, not only the “worst case” event. 	
<p>“It does not do to leave a live dragon out of your calculations, if you live near him.” – J. R. R. Tolkien, <i>The Hobbit</i>, Chapter XII</p>		
<p><small>©AIChE 2018. All rights reserved. Reproduction for non-commercial, educational purposes is encouraged. However, reproduction for any commercial purpose without express written consent of AIChE is strictly prohibited. Contact us at ccps_beacon@aiiche.org or 646-495-1371.</small></p>		

Figure 16.2 CCPS Process Safety Beacon

Examples of old newsletters that still convey highly relevant learnings are shown in the ICI newsletter (Kletz, IChemE website), in Figure 16.3 and Figure 16.4.

96/1 A NEW WAY TO SUCK IN A TANK

Previous Newsletters (78/8, 77/2, 47/5b, 42/1 and the supplement to 56) have described how tanks were sucked in or overpressured because the vents were choked. Another incident nearly occurred in the Division in a tank containing a hydrocarbon which is liable to polymerise and which is therefore always doped with an inhibitor. The hydrocarbon has a boiling point of 145° C and is stored at atmospheric temperature. When there is a fall in atmospheric temperature some vapour condenses on the roof of the tank; since the liquid formed in this way is not inhibited, it polymerises and a plug of polymer almost bridged across the bottom of the vent pipe as shown below.



The vent pipe is inspected regularly by removing the cover and flame trap and looking through the vent pipe to see that it is clear. The man doing this could not see the build-up of transparent polymer.

Now, as well as looking through the vent pipe, they push a wooden rod through it to make sure it is clear.

WARNING: If you do the same, make sure there is something on the end of the rod to prevent it falling into the tank.

The build-up of polymer was discovered when the plant manager, carrying out a personal inspection of the vents, noticed a thin coating of polymer on the inside of the vent pipe. He had the pipe removed for cleaning and the build-up was then discovered.

96/2 AN OLD WAY TO SUCK IN A TANK

A tank was fitted with a vent just big enough to cope with a pump-out rate of 30 m³/hr. The tank was connected to another pump which had a capacity of 65 m³/hr. Nobody checked that the vent size was still adequate and the tank was sucked in.

The operators were amazed that a 3 inch vent, fitted with a flame arrestor, was not big enough to prevent the tank being sucked in.

Figure 16.3 ICI Safety Newsletter No. 96/1 & 2

96/7 HUMAN ERROR DURING ALARM TESTING

Alarm testing is usually considered less risky than trip testing but errors can occur.

Two furnaces are each fitted with a temperature recorder controller and high temperature alarm.

The two recorders are side by side on the instrument panel in the control room with the recorder for A furnace on the left.

A
furnace
recorder

B
furnace
recorder

An instrument artificer was asked to test the alarm on A furnace. He put the controller on manual and then went behind the panel.

The next step is to take the cover off a junction box, disconnect one of the leads, apply a gradually increasing potential from a potentiometer and note the reading at which the alarm sounds.

Behind the panel the junction boxes for A and B are in line with the recorders and therefore B is on the left.

B

A

The only label was very small and close to the floor so it was hardly readable.

The artificer, who had done the job many times before, took the cover off B junction box and disconnected one of the leads. The effect was the same as if the thermocouple had burnt out. The recorder registered a high temperature, the controller closed the fuel gas valve and the furnace tripped.

The two junction boxes should have been labelled A and B in large letters. [Note added later: Or, better, the connections used for testing could be on the fronts of the instruments.]

Figure 16.4 ICI Safety Newsletter No. 96/7

Another “Learning Event Report” example is shown in Figure 16.5.

Learning experience from unplanned events


LER Event:	Metropolis Mineral Acids Plant: L1 – Acid Exposure
Date / Time:	May 1, 2018 / 2:15pm
CONTACTS:	John Q. Public
Presentation Link:	[insert link here]
Target Audience:	Production Leaders
Recommended Action:	Management system gap assessment

Event Course: Short Description:
A recently trained employee was completing a pressure test as part of the returning to operations activities for the acid pump. While disconnecting a nitrogen hose that the employee had attached to an incorrect location, acid was released and splashed on the employee’s upper legs. The employee immediately entered the safety shower and was subsequently evaluated by on-site emergency response personnel, who recommended further offsite evaluation. The employee was evaluated by an offsite medical facility and was released with prescription pain medicine.

Root Cause of each Protection Layer and its Management System:

- Appropriate PPE was not used when handling acid
 - Management System: Personal Protective Equipment Use
- Employee did not follow leak test procedure for returning pump to operation
 - Management System: Procedure Use Culture
- Inadequate training strategy in place to confirm application of knowledge
 - Management System: Effective Training of New Operators

Pump to Return to Service



Acid Exposure Point

Learning experience:

- Determine if a robust management system exists at your facility that demonstrates the application of knowledge of all Life Critical Standards prior to first certification of an operator. Implement a system if one is missing in your facility.
- Ensure the certification process includes an assessment of actual skill set before an employee starts training to ensure that any knowledge gaps are understood and addressed.
- Determine how your facility restricts or allows first-time infrequent task execution, even after certification, involving high process risks such as chemical exposure.
- Implement a formal procedure use metric (or other feedback mechanism) capable of ensuring ongoing effectiveness of the procedure use culture at the facility.

Figure 16.5 Learning Event Report Example

An example of a process safety bulletin is provided in Figure 16.6, which uses a bowtie diagram to visualize the barriers that failed and the associated causal factors.

Process Safety Bulletin

Incident

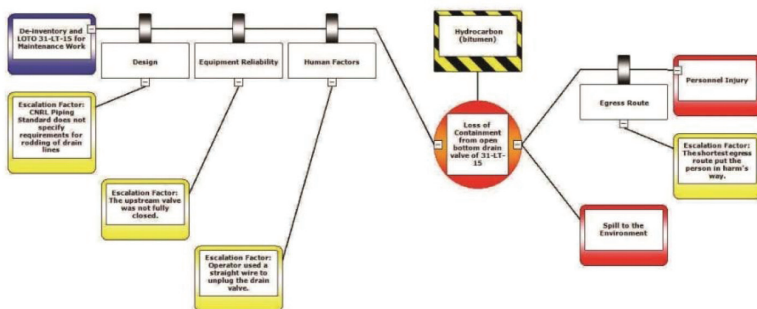
Approximately 3 m³ of hydrocarbon (bitumen) was released from a ½" drain valve on a level transmitter to the ground.

How Did it Happen

On Jun 23, 2015, at approximately 10:15 am, an Operator began isolating a level transmitter for maintenance work. He isolated the top leg of the transmitter. On the bottom leg, he isolated the bottom valve. When he opened the downstream drain valve to check for positive isolation and to drain the leg, he did not see any bitumen draining. He began to rod the drain valve to remove the solids pluggage. The pluggage broke free causing a flow of hot bitumen to be released. The Operator sustained burns as he attempted to close the drain valve and as he egressed from the platform. Approximately 3 cubic meters of hydrocarbon (bitumen) spilt onto the concrete pad.

Key Learnings

A number of causal factors were identified as key events that led to the incident. This is a bowtie diagram visualizing the causal factors which reduced the robustness of the barriers.



- Bitumen splashed out of the catch pail due to the proximity of the drain valve and the pail. When the operator went to close the drain valve handle, he could not avoid the bitumen splashing up from the catch pail.
- The upstream valve was not fully closed.
- Operator used a straight wire, instead of a rodding tool with a gland component, for unplugging the drain valve.
- Operator decided to evacuate the platform via the most direct route to ground level which was under the open drain valve

Figure 16.6 Process Safety Bulletin Example

16.5.3 Videos of Incidents

Videos with animations of incidents are available from the U.S. Chemical Safety Board site (CSB, Videos) at:

<https://www.csb.gov/videos/>

16.5.4 Detailed Incident Reports and Databases

Facilities often produce detailed incident reports that are available to the organization. In addition, reports on outside incidents are available from numerous sources including those detailed under 16.1.2.

Full and detailed incident reports will usually be of greater interest to engineers and process safety professionals. They may be too complex to efficiently provide key learning at a plant level, but could be used as material for a single page newsletter or “learning event”.

Sources of detailed incident reports are shown in 16.1.2.

16.6 SUMMARY

Learning lessons from incidents, and taking appropriate action to prevent a future incident from occurring, are arguably the most important outcomes of an incident investigation. If the lessons are not learned, are forgotten, or not acted upon, the same or a similar incident will occur again. There are opportunities to learn from incident investigations of all sizes, including smaller incidents, near misses and precursors. Learning from a broad range of incidents will help to reduce the frequency and severity of many types of incidents as opposed to simply preventing recurrence of an identical incident. The learning from incidents should take place at all levels of the organization to maintain a sense of vulnerability and to ensure this learning embeds in the organizational memory and becomes part of the corporate culture.

APPENDIX A.

PHOTOGRAPHY GUIDELINES FOR MAXIMUM RESULTS

The following guidelines provide a list to review before taking photographs.

1. Follow plant safety requirement when photographing. In addition, watch where you are walking and do not move when looking through a camera viewfinder to avoid tripping, falling, stepping in holes, and other accidents.
2. Flash units, motor drives, digital cameras, manual cameras with batteries, and other similar devices are not intrinsically safe and must be treated as potential ignition sources. In many cases, a gas test and hot work permit will be required before using these devices. An operator with a flammable gas detector may have to accompany the photographer. Infrared gas detectors may also be set off by flash units. When using a flash even with permission, it is a good practice to take the time to warn and alert all personnel who could see the flash (or a reflection of the flash). This will prevent startled response actions, and could prevent an injury (due to fall or other response). It is also a sign of courtesy and respect.
3. Before commencing investigation photography, check that the camera date and time settings are correct and that metadata created by the camera includes the time and date the photograph was taken.
4. Log and document every photograph shortly after it is taken. Trying to reconstruct or remember what the photograph is of and why it was taken after a period has elapsed is difficult.
5. Promptness is critical to minimize disturbing the data; however, in no case should emergency medical treatment or emergency response activities be delayed by any photographic activity.
6. Prioritize photography tasks. Give priority to areas where the scene may change. While the general rule is to photograph a scene from the outside in, time sensitive areas and items need to be documented quickly.

7. Digital cameras have become the norm in incident investigations. Digital images are acceptable in legal proceedings as long as it can be proven that the content of the image was not edited. On occasion when editing is needed to improve quality/clarity of a photo (e.g., to adjust exposure, crop an image, sharpen an image, etc.), an unedited version of the photo needs to be retained with the edited copy to prove that *content* in the image was not edited.
8. Digital media can be lost, overwritten, corrupted or deleted. As a result, digital images should be backed up and protected like other forms of electronic data.
9. Begin photographing a scene with overall views of the general area from multiple directions. This will help show perspective of distance and relative locations of items of interest.
10. Adjust camera settings as needed to achieve a good image. Flash, exposure, and focus mode are readily adjustable on higher quality digital cameras.
11. Know the scene protocol requirements for physically moving items while photographing. Movement of items can be considered spoliation of evidence.
12. Every object should include an item of measurable scale as a size reference in some shots. A scale may obscure part of an object, so photos with no scale are also needed. It is common to include a ruler/scale or some other object of known size in any close-up view (3 feet or less, 1 meter or less). Tape measures can also be used to show the size of objects and the distance between them. The orientation of the tape measure can also be used to show the orientation of the photograph.
13. When photographing a specific object, start with an overall photo that shows the location and position of the object in the scene. Then progressively zoom in for closer shots from the same orientation so the object of interest becomes apparent in closer views. A common mistake is taking close-up photos without any overall shots, making it difficult to determine where the object was located in relation to other objects or equipment.
14. Alert personnel in an area that you are taking photographs. Some personnel may object to being photographed in the scene. For example, when conducting multi-party protocols, some personnel attending to witness a protocol may not be investigators or experts, and may not want to appear in photos. When personnel are obstructing a photo, ask them to move before taking the photo. In some jurisdictions privacy laws prohibit photographs of individuals where they can be identified without

their permission.

15. Consider the location of the sun and the accompanying glare, reflections, and shadows generated during outside shots. It may be necessary to take photographs at different times of day to avoid glare and shadows. Sometimes a specially timed series of photographs may be needed to document the approximate lighting conditions at the time of the incident.
16. One disadvantage of an autofocus camera is that the camera does not always focus on the desired object. If the object of interest to the photographer is in the background but another object is in the foreground, the camera may select and focus on the closer object instead. A familiar example is the out-of-focus picture where the camera has focused on some background object in the gap between two people. Most autofocus cameras are now equipped with selectable focus features to overcome this limitation, including spot focus and manual focus.

A common avoidable mistake is to expect the camera to duplicate the ability of the human eye to focus in low light conditions such as dusk or heavy shade. The performance of cameras represents a compromise of several factors. These include lighting conditions, technical quality, and image resolution. The camera systems are designed to perform in a specific envelope. Operating near or beyond the edge of these specifications will produce correspondingly lower performance. When shooting in difficult conditions, try a variety of camera settings to find a combination that provides a good quality image. External lighting may be necessary. Side lighting is often helpful to make surface features on an object stand out, which may not be apparent with an on-board camera flash.

17. A fresh and complete spare set of batteries is a necessity rather than a luxury. If the camera is part of a seldom used supply kit, before traveling to the site, check that fresh primary and spare batteries are available and that a memory card is installed.
18. Some type of portable background is often desirable when shooting data in the field. A light colored pastel cloth will usually give better results than black or white.
19. When documenting a witness statement, the photograph should be taken from as close as possible to the actual viewpoint used by the witness.
20. Backlighting can cause major problems, especially when using an automatic or semiautomatic exposure control camera. Backlighting is the condition where the subject of interest (in the foreground) is in relative

darkness caused by a brighter background. The camera will sense the bright background and thus produce a photograph in which the desired object in the foreground appears to be in a shadow. Examples of this occur often when shooting in an upward direction, for instance, to capture some detail on an overhead pipe rack. Some cameras have an exposure feature that can be activated to help this situation. Spot focus can also correct backlighting by causing the camera to set exposure based on lighting on the object in the center spot in the viewfinder. "Fill flash" is another technique in which the flash is turned on to illuminate objects in the foreground. The combination of spot focus and fill flash is effective in many backlight situations.

21. A common mistake is to expect the camera to do the thinking for the investigator. Some investigators have used the approach of taking a general barrage of pictures in the hope that somewhere in the large pile will be a "gold nugget" with the key to the investigation. Each shot should have an intended purpose. Planned shots yield better results than random shots do.
22. A camera flash will create an instantaneous, temporary shadow that will appear in the photos. There are multiple techniques to eliminate an undesirable shadow. One approach is to turn the flash off and use a longer exposure. A tripod may be necessary for long exposure times. Special flash units that fit around the lens of some cameras are available to eliminate these shadows in macro photography. Off board flash units positioned to the side of an object and triggered by the camera can be very effective. In the field when off board flash units may not be convenient or available, a flashlight held to the side of an object may be adequate to turn a flash off and eliminate the shadow from the flash.
23. X-Rays (radiographs) are another form of photography. Digital X-ray recordings have become commonly available. Digital X-rays offer the advantage of rapid viewing of the image to determine if the X-ray captured the desired features/details of the object. The X-ray technician can adjust the irradiation time, photography equipment position and object orientation to improve the image if necessary.
24. Video cameras are valuable to record actions or motion. Video camera resolution and exposure/focuses features are not as good as still cameras, making still cameras the preferred choice for most investigation photography. Nonetheless, video cameras are preferred to document actions, such as testing that involved changing positions (e.g., opening/closing a valve), altering the scene (e.g., disconnecting an instrument from the scene), or performing a testing during a protocol (e.g., stroking a control valve to test functionality).
25. Video cameras typically include audio recording. It is common practice

when performing protocols to turn off or disable audio recording since participants at the protocol do not want their side conversations to be recorded. If audio will be recorded, it is expected that the photographer will alert everyone in attendance about the audio recording, and alert attendees whenever recording is about to be started.

APPENDIX B.

EXAMPLE PROTOCOL – CHECKING POSITION OF A CHAIN VALVE

This appendix contains an example protocol. Protocols are discussed in Chapters 8 and 9 with regard to evidence collection and evidence analysis, respectively. The example protocol below pertains to an in-situ check of the position of a chain valve to determine whether the valve is fully closed as it appears from external visual examination. The sections of the protocol are typical of protocols used in multi-party examinations, which include personnel not associated with the company or plant.

Protocol for Checking the Position of a Chain Valve

Background

An 8-inch manual valve is located in the Distillation Column overhead line. The manual valve is equipped with a chain drive for manual operation from ground level. The valve appears to be in the closed position and holding overhead line pressure.

Objective

The objective of this procedure is to check the position of the 8-inch chain valve on the Distillation Column overhead line. The position will be tested by two methods: by manually attempting to close the valve and by radiographing it.

Evidence

No items will be removed from the equipment as evidence at this time. If the valve is to be removed for further evaluation, a separate protocol will be prepared.

Safety Provisions

The site safety plan will be followed, including:

- PPE requirements – FRC, steel toes shoes, hard hat, safety glasses with side shields, leather gloves, hearing protection
- Gas detector for flammable atmosphere; for radiograph equipment and cameras
- The number of people who can be present on the platforms is limited by size of the platforms.
- Radiograph safety procedures provided by the contractor will be followed as approved by the radiation safety officer. All non-qualified personnel will be beyond the minimum safe distance specified by the subcontractor. The specific safety provisions are provided below.

Approach

The following steps are followed to check the valve position:

1. Place an alignment mark (Mark #1) on the chain wheel and adjacent housing to document as-found position.
2. Photograph the valve.
3. Measure the height of the valve stem and photograph with a measurement device beside the stem.
4. Radiograph the valve according to the following procedure:
 - An appropriate radiation source will be selected for all shots. The camera containing the radiation source is man-portable and requires no external power source. All film cassettes and support stands are also man-portable. The radiation safety protocol described in this protocol will be followed.
 - To maintain traceability, an alphanumeric identification system will be used to track which valve is being radiographed and the position of the source relative to the valve and exposure time. Lead lettering will

be used in each shot to place the identification on the exposed film. The identification nomenclature identifies the valve and the position of the source and exposure time.

- A flow direction indicator will also be placed in the field of view of each radiograph.
 - The valve identification and radiograph shot number will be logged. Before each radiograph, the relative position of the source on the valve will be documented with still and video photography.
 - The valve will have at least one radiographic shot to define the position of the valve. The radiographic team will determine the need for additional shots.
 - The radioactive source and the film cassettes will be supported on freestanding supports unless the orientation or position of the valve or film position for a valve poses a problem. If necessary, the film cassette will be secured to a nearby structure, pipes or the body of the valve being radiographed, with light rope, clamps or tape. Only the radiographic film will be in contact with the external body of the valve. The radioactive source will be away from the film and not in contact with the valve.
5. Manually attempt to close the valve using the chain. All personnel on the platform by the valve will stand at least 4 feet away from the valve. An operator positioned on the ground will attempt to close the valve by pulling on the chain while valve movement is witnessed by the interested parties and videotaped. No attempt will be made to open the valve. If the valve moves, slowly continue turning the valve in the closed direction until the valve can no longer be turned, documenting the number of turns relative to the alignment mark. Measure the stem height if the valve moved. Mark the chain wheel (Mark #2) relative to the alignment mark on the housing, and photograph the mark.
 6. Attempt to further close the valve with the valve wrench that is lying on the platform by the valve. All personnel on the platform by the valve will stand at least 4 feet away from the valve, to give an operator room. An operator positioned on the platform at valve level will attempt to further close the valve using the valve wrench following the site practice. If the valve moves, continue turning the valve in the closed direction until the valve can no longer be turned, documenting the number of turns relative to alignment Mark #2. Measure the final stem height if the valve moved.

Mark the chain wheel (Mark #3) relative to the alignment mark on the housing, and photograph the mark.

Restore System State

The valve will be left in the final position from Step 6.

Test Personnel and Observers

One third party forensic engineer will oversee the execution of the protocol. Interested parties will be given notice and the option to attend. Operations personnel will attempt to close the valve per the protocol. A radiograph contractor will perform the radiograph.

Documentation

Execution of the protocol will be videotaped, except when the radiation source is exposed. Still photographs will be taken to document as-found condition prior to making any changes. The radiograph images will be the radiograph documentation.

Radiation Safety Guideline

The radiation source will be chosen by the radiograph contractor as appropriate for the valve being radiographed. Because of the health hazard and potential exposure danger to radiographs, the site radiograph safety procedures will be followed.

APPENDIX C.

PROCESS SAFETY EVENTS LEVELING CRITERIA

The following table is an example of a logic tree approach to determine the incident classification level (“leveling”) described in Chapter 5. The table is used as guidance to determine whether or not a safety injury or fatality precursor or potential event should be investigated. It applies only to Process Safety processes and equipment that are determined to be high risk by local regulations and company policy.

Table C.1 Example of Process Safety Event Leveling Criteria

Process Safety Event Type	Definition	Level 3	Level 2 OR 2P*	Level 1	Level 0 (Trend Only)
Release	Release from primary containment of a Process Safety High Risk process hazardous material.	Release quantity > RQ in EPA 40 CFR 355.40 (or equivalent) OR RQ = 5000 lbs., if not listed.	Release quantity > RQ/10, but < RQ, OR 2P* - A lower level event that had the POTENTIAL to have been a 2 or 3 release event.	Release quantity > RQ/100 but < RQ/10	a. Release quantity < RQ/100, OR b. Activation of a safety device that didn't result in a spill/leak (real or false activation that was not related to a maintenance activity or testing of a safety device) – e.g. LSHH (Level Sensor High High), PSHH (Pressure Sensor High High), interlock, rupture disc activation, gas sensor activation, etc., OR Process Safe Operating Limit exceedance, even though it did not result in an undesired event.
Fire or Explosion	Fire or explosion within a Process Safety High Risk process.	Equipment damage was ≥ \$25,000	Equipment damage was ≥ \$5,000 but < \$25,000 OR 2P* - A lower level event that had the POTENTIAL to have been a level 2 or 3 fire/ explosion event.	Equipment damage was < \$5,000.	a. Abnormal heat was generated but no equipment damage, OR b. Asset Integrity Preventive Maintenance (PM) failure or instrument out of tolerance, or corrective task (i.e. equipment fails while in service), OR c. Operating procedure deviation that had the potential for a Process Safety event (e.g. material sent to Tank B instead of Tank A and had the potential for a Process Safety event), OR d. Deviation from a Process Safety and/or regulatory requirement with the potential for safety impact (e.g. Hazard Identification and Risk Analysis (HIRA) or Operational Readiness Review not done, etc.), OR e. Static sparking observed, OR Equipment with overdue PM tasks (i.e. outside of the PM window).
<p>Note: All level 0 and 1 events should be assessed for level 2 potential (2P), i.e., a lower level event that had the potential to have been a level 2 or 3 event.</p>					

APPENDIX D.

EXAMPLE CASE STUDY

The following case study describes the investigation work process for a hypothetical occurrence using a logic tree based multiple root-cause systems approach. An example incident investigation report follows the work process description. The example is intended for instructive purposes only; descriptions of process equipment and conditions are not intended to reflect actual operating conditions.

The Work Process

At the NDF Company in City, State, a major fire occurred in the catalyst preparation area on August 1. The fire originated at Kettle No. 3 at 11:10 A.M. An explosion of catalyst storage tank No. 2 followed at 11:20 A.M. Final extinguishment of the fire was accomplished by the local fire department and plant fire brigade at 12:10 P.M. One fatality and five personnel injuries resulted from this event.

When access was permitted by Incident Command, the catalyst preparation area was secured against unauthorized entry, and plant management assembled for a meeting to discuss immediate actions. They decided to call in a corporate risk analyst to lead the investigation team. With the corporate risk analyst's help, by teleconference, management selected the following incident investigation team:

- Corporate Safety and Risk Analyst, Team leader
- Process Engineering Supervisor
- Safety Supervisor (trained and expert in the multiple-cause systems-oriented incident investigation methodology)
- Catalyst Production Supervisor
- Outside Operator
- Polyethylene Process Unit No. 1 Foreman
- Maintenance Foreman
- Corporate Legal Representative

Representatives from OSHA, the local fire department, and the property insurance carrier's loss adjuster were also conducting parallel, independent investigations.

The selected team initially established a specific plan of investigation procedures for this occurrence. This strategy session listed priorities and necessary actions to ensure that all required information was obtained in a prompt manner. Needless delays in evidence collection were avoided by the use of this plan.

The investigation team visited the scene of this incident before the physical evidence could be disturbed. The maintenance foreman was given the duty of taking photographs of the damaged area. He was careful to obtain overall views of the scene and individual equipment and logged where each photo was taken. All team members were provided with a field investigative kit and appropriate safety protective gear. Important evidence was gathered, preserved, and identified using a written log and tagging system. A plot plan was posted and the location of each physical piece of evidence was noted on the plan along with the tag number.

On completion of this task, preparatory work was performed by the team members for preliminary witness interviews. The importance of focusing on confidentiality and fact finding, while avoiding assigning blame, was emphasized to team members prior to conducting interviews. Two team members, the safety supervisor and one other as available, were chosen to meet with the witnesses. A small conference room in the Administration Building was allocated for this project. The setting was arranged informally to allow the person involved to feel at ease. After considerable debate within the team, a conclusion was reached to not use a tape recorder during the witness interviews. The interview process was started early the evening of incident and was continued throughout the next two days. At the end of each day, the investigation team met to discuss the information obtained from the interviews and other activities.

The catalyst preparation area supervisor, on-duty control room operator for the catalyst operation, and maintenance superintendent were key sources of information. Their written records and logs were examined in detail. Other personnel who were interviewed included two outside operators, fire brigade members, and associated maintenance employees. During these conversations, special attention was paid to nonverbal signals. The interview process generated several unanswered questions about operational and maintenance procedures that required further study.

Second interviews, further evidence collection and examination, and thorough evaluations of operational and maintenance records were conducted to try to find explanations for the questions created by the preliminary witness interviews. Due to a high pressure alarm occurring at Kettle No. 3 in the catalyst preparation area prior to the fire, an analysis of the software and hardware for the control panel that oversees this process was deemed essential for this study.

In the incident investigation team's daily meetings, they began a timeline of the events preceding and during the incident, using flip charts and sticky notes for easy modification as new information became available.

The team conducted a series of fact finding and evidence analyzing meetings. During each of these meetings, specific action item assignments were made to gather further information needed to understand the events, systems functions, systems interrelationships, and failure modes.

After the team completed the preliminary sequence of events, they began to develop logic trees to describe the events. As the top event, they chose the last injuries in time, those to the four fire brigade members. They asked, "Why did these injuries occur?" Two events are required and are sufficient: the explosion at the storage tanks AND the presence of the fire brigade members. The team added these events to the tree and continued to ask "Why?" until system-level root causes were determined. (All logic trees are included in the investigation report.) To reduce the complexity of the trees, the team chose to treat the operator fatality, the contractor injury and the injuries to the fire brigade as separate trees.

Several times, the team created fact-hypothesis matrices where needed to determine which branch of the tree contributed to the incident. One of the fact/hypothesis matrices is shown in Chapter 9.

On completion of the investigative work, the team convened to discuss its findings. During the discussions, important recommendations for corrective actions were developed. Special attention was allotted toward determining the potential effects of these suggested alterations on the efficiency of the plant operations. After long deliberations, responsibilities and desired completion dates were designated for each recommendation.

The team presented its findings to the plant management and to the corporate safety department orally and handed out lists of the causes, the trees, the recommendations, and the criteria for restart. Management accepted the oral report and appointed the operations manager to be responsible for seeing that the action points were completed.

Over the next two weeks, the investigation team compiled and published a detailed report. The team leader appointed one member to edit the report; the editor used the criterion that the report would be understandable to a new operations or engineering person. It was assumed that the report audience would be experienced in polyethylene technology and NDF culture, and would include personnel from other plants remote from the location of the incident

The investigation team members were consulted frequently during the design and installation of the repairs for restart. Several team members participated in the recommended HIRA and the pre-startup safety reviews.

To reduce risk in the industry as a whole, NDF endeavored to share the lessons learned from the incident with others in the same or similar industries.

In October, the site manager gave an oral summary of the incident to the local manufacturers' association.

In December, the NDF representative on the co-producers' safety committee informally discussed the causes and corrective actions with the other co-producers.

In July of the following year, the safety supervisor presented an overview of the incident, causes, and corrective actions to a safety meeting sponsored by the regional chemical industry council.

In March, about 1-½ years after the incident, the process engineering supervisor gave a paper on the incident at a Loss Prevention Symposium of the American Institute of Chemical Engineers. The paper was published later in *Plant Operations Progress*.

Incident Investigation Report

Executive Summary

A major fire and explosion occurred August 1 at the NDF Company polyethylene manufacturing facility in City, State, resulting in one fatality, five personnel injuries, and extensive damage. The fire originated in the catalyst area when a vessel was overfilled and the exit piping ruptured releasing isopentane, a flammable material, and aluminum alkyl, a pyrophoric material.

The first fireball, at approximately 11:10 A.M., caused an operator fatality and a contractor injury. Emergency response was impaired because the fire water pumps were down. The fire spread to the catalyst storage tanks. A subsequent explosion of an adjacent catalyst storage tank resulted in the injury of four firefighters. Extinguishment of the fire was accomplished by the local fire department and plant fire brigade at 12:10 P.M.

The causal factors of the incident relate to several process safety management areas:

- mechanical integrity,
- contractors,
- emergency planning and response,
- process hazards analysis, and
- management of change.

Background

Twelve years prior to the incident, the NDF Company opened a facility in City, State to produce low density polyethylene. Manufacturing of the polyethylene is done in two 50-ton reactors that are encased individually within their own 8-story-high process unit. The main raw materials for the manufacturing operations include ethylene, hexane, and butene. The polymerization is completed in the presence of a catalyst. The base chemicals for the catalyst are aluminum alkyl and isopentane. The reactor and catalyst preparation areas are on a distributed control system (DCS). A simplified process flow diagram is included.

In the catalyst preparation area where the fire occurred, aluminum alkyl and isopentane are mixed in a batch blending operation in three 8000-gallon kettles. The flow rates of components are regulated by an operator at the control room. Temperature, pressure, and liquid level within the kettles are monitored by the control room operator. The formulated catalyst is stored in four 12,000-gallon vertical storage tanks within this process unit. Aluminum alkyl is a pyrophoric material and isopentane is extremely flammable. Each vessel was insulated and equipped with a relief valve sized for external fire.

The isopentane for the catalyst preparation unit is stored as a liquid in a 60-ton horizontal (bullet) storage tank. The aluminum alkyls and other required chemicals for this process are received in small truck trailers and kept beneath a metal canopy.

The catalyst preparation area is positioned between the two polyethylene production units that are located 60 feet apart. The aluminum alkyls storage canopy and isopentane horizontal storage tank are located at a remote area at an approximate distance of 250 feet away from the production and utility areas. The isopentane is transported to the catalyst preparation area through a 3-inch pipeline. A remote actuated isolation valve on this supply line that fails closed is located at the isopentane storage tank. This control valve and an associated isopentane feed pump are managed by the operator in the control room.

The catalyst preparation area is protected by an automatic water-spray sprinkler system that is actuated by associated heat detectors. Fixed fire water monitors surround this process area. The water for these fire protection systems is supplied through 8-inch underground water mains by three (two diesel and one electric) horizontal, centrifugal, 2500 gpm rated, 125 psi automatic fire pumps that take suction from a 750,000 gallon above-ground storage tank. The electric fire pump's power source is from an independent electrical feed. The water supply for this facility was designed to meet the highest water demand within the facility when one fire pump is out of service.

Sequence of Events and Description of the Incident

On August 1 at 10:30 A.M., a control room operator remotely started the feeds to Kettle No. 3 in the catalyst preparation area. The normal procedure was to fill the kettle to approximately 80%, but Kettle No. 3 was apparently completely filled this time. The level indicator showed a high level, but the alarm did not sound. (The alarm was later found to be bypassed.) A high-pressure alarm for this vessel was acknowledged at 11:03 A.M. by the control room operator. At 11:00 A.M., a severe thunderstorm had started and within 5 minutes caused a power outage throughout the immediate vicinity. The ambient temperature was about 83 °F and winds were from the northwest at about 3 mph.

With an available diesel emergency generator supplying power to critical pumps, the control room operators initiated shutdown procedures for the two reactor areas. An uninterruptible power supply (UPS) kept power to the DCS screens and instruments; however, the DCS system closed all catalyst preparation and reactor feed valves on loss of power as designed. Outside operators were sent to manually block in reactor feeds.

At 11:09 A.M., a high-LEL detector in the catalyst preparation area sounded on the DCS. The lead outside operator was contacted by radio communications to investigate the problem. He said he was just leaving the Reactor No. 1 area and would go right to the catalyst preparation area. The thunderstorm had passed overhead and the rain was diminishing. At about 11:10 A.M., a “whooshing” noise (now believed to be the fireball) was heard by many and the heat detector for the automatic water-spray sprinkler coverage in this area alarmed in the control room. The lead outside operator did not respond when called on the radio.

The plant fire brigade and the local volunteer fire department were notified by the supervisor of the catalyst preparation area by 11:12 A.M. On their arrival to the scene of the fire at 11:15 A.M., the plant fire brigade saw the lead outside operator down about 40 feet from the fire, in between the catalyst preparation area and reactor building No. 1. They also found a seriously burned unknown person about 120 feet from the fire, near the finishing building. (This person was eventually determined to be a service contractor who entered the premises at 10:30 A.M. to calibrate equipment in the instrument house for Reactor No. 1.)

The fire had engulfed most of the catalyst preparation area. The automatic deluge sprinkler coverage for this area had actuated, but water did not flow. The fire brigade tried to activate a fixed monitor, but again got no water flow. With the limited water supply from the plant fire engine available as a shield, the fire brigade members felt they could reach the lead outside operator. Meanwhile, the commander of the plant fire brigade

sent a team member to the fire pump house to investigate the lack of fire water.

Another explosion occurred at 11:20 A.M. as the fire spread to the formulated catalyst vertical storage tanks. Hot metal fragments from this blast severely injured four fire brigade members involved in the rescue attempt of the lead operator. They were about 60 feet away from the fire at the time of the explosion.

The local fire department arrived just after the explosion at 11:22 A.M. With the limited water supply on two of the fire trucks and the utilization of another fire truck to pump water directly from a nearby cooling water tower basin, the firemen were able to slow the fire spread.

The fire brigade member sent to the fire pump house found that the electric fire pump was inoperable due to the power outage. One diesel fire pump was known to be impaired due to mechanical problems and the other diesel fire pump had failed to start because its batteries were dead. Several maintenance personnel were sent immediately to repair this diesel fire pump. By 11:30 A.M., the Maintenance Department was able to transfer the set of batteries from the impaired diesel fire pump to the other diesel fire pump. On completion of this task, this diesel fire pump was started. The automatic deluge sprinkler protection was severely damaged by the fire/explosions and had to be valved into the off position. Three fixed monitors were turned onto full flow and directed at the fire. Also, the firemen and fire brigade used two hose streams off nearby fire hydrants for firefighting purposes. At 11:58 A.M., the fire was under control. Final fire extinguishment was accomplished by 12:10 P.M.

The lead operator died the next day due to lung damage attributed to inhaling the hot gasses. Five other people were seriously injured. The catalyst preparation area received extensive property damage. The production operations at this facility are estimated to be suspended for two months until this area including associated pipelines can be rebuilt.

Cause Analysis

The team developed logic trees to describe the events. To reduce the complexity of the trees, the team chose to treat the operator fatality, the contractor injury and the injuries to the fire brigade as a separate tree.

Since explosion at the catalyst storage tanks resulted from the spread of the fire from Kettle No. 3, the trees are interconnected. All the logic trees are attached and a key to the trees and subtrees is shown below. Note that some trees show an entry point with the same letter designation as the tree (e.g., entry point B in the B tree). The entry point shows where the user is routed into a tree from a different tree.

Tree	Tree Title
A	Operator Fatality in Kettle No. 3 Fire (Branch L is on Tree A)
B	Pool Fire at Kettle No. 3 (Branch C is on Tree B)
C	Kettle No. 3 Exit Piping Cracked
D	Kettle No. 3 System Pressure Reached 120 psig (Branch F is on Tree D)
E	Kettle No. 3 Exit Piping Failed at 120 psig (Below Design Pressure)
F	Power Failure Occurred
G	Contractor Injury in Kettle No. 3 Fire
H	Contractor Did Not Know He Should Leave the Area
I	Four Fire Brigade Members Injured By Metal Fragments
J	Fire Brigade Members ~60 feet from Fire When Explosion Occurred
K	Extended Pool Fire Under Catalyst Storage Tanks
L	Operator Near Kettle No. 3 During Flash

Some events were personnel or equipment doing what they were supposed to be doing at that time or have a very high likelihood of occurring; these events are depicted as a “house” symbol. For some events at the bottom of the tree, the team did not have enough information in their possession to answer the “Why?” question. Such events are shown as a diamond, indicating a team decision to stop the tree at that point. For many of the diamonds, the team recommended further study or investigation by other groups.

The incident investigation team concluded that the fire occurred due to failure of the Kettle No. 3 exit piping in the catalyst preparation area. The failure released isopentane, a flammable material, and aluminum alkyl, a pyrophoric material, from the vessel. Moist air and water in the curbed dike in the catalyst preparation area initiated an ignition of the contents. The atmospheric temperature was just above the flash point for isopentane, resulting in flashing vapor and some auto-refrigeration of the liquid. A jet fire occurred at the release point combined with a pool fire which spread throughout the dike and under the catalyst storage tanks. Because there was no fire water available, the fire could not be fought or the adjacent tanks cooled. The fire brigade was about 60 feet from the catalyst preparation area, attempting to rescue a victim, when an explosion occurred. Catalyst storage tank No. 2 had failed.

Even without water to fight the fire, the storage tank failed more quickly than would be expected for a tank with insulation in good repair and a relief valve sized for the fire case.

The causal factors of the incident relate to several risk-based process safety elements, as indicated below, plus engineering design practices:

- Asset Integrity & Reliability
- Contractors Managements
- Emergency Management
- Hazards Identification and Risk Analysis
- Management of Change
- Operating Procedures
- Safe Work Practices
- Conduct of Operations
- Process Safety Culture

Findings and Recommendations

Causal Factors:

i Piping Integrity

The carbon steel piping in the catalyst preparation area and the isopentane feed lines to the area was weakened by external corrosion. The lines were Schedule 40, carbon steel lines which are suitable for this service. However, the lines were 12 years old. Physical evidence indicates that the failure most likely occurred at an elbow in the Kettle No. 3 exit piping. Pressure data from the system indicates the failure occurred when the system pressure was 120 psig, which is below the pressure rating for the vessel. Inspections of remaining parts of the catalyst mix and isopentane feed lines revealed deterioration of insulation and missing parts of the external shield (designed to prevent water from getting into the insulation). Corrosion under insulation especially in a heat affected zone is consistent with a failure in the kettle exit piping. (*Asset Integrity & Reliability*)

ii Asset Integrity Management Program

The existing asset integrity management program did not appear to cover the catalyst preparation area. While records were found for inspections of the Reactor systems and the isopentane storage area, no inspection records were found for the catalyst preparation area. Interviews suggest these inspections were delayed by the budget crunch. (*Asset Integrity & Reliability*)

iii Fire Pumps Integrity

The No. 1 diesel fire water pump was inoperable because it had overheated during an outside agency annual performance test 1.5 months prior to the incident. The pump probably had problems prior to the test, but overheating may not have been detected in monthly maintenance tests because the 5-minute run time may not have been sufficient to find the overheating.

The No. 2 diesel fire water pump was down because its batteries were dead. The dead batteries were detected and recharged during a monthly check two months prior to the incident, but they were not replaced or rechecked after that.

Interviews suggest that the fire water pumps had not been repaired due to a mechanical department perception that, because of budgetary pressures the expensive repairs required delaying until the first of the year. It is interesting to note that although several people knew that one fire water pump was impaired, no one person in the department knew that both pumps were impaired. In interviews, several upper management representatives stated that fire water pump repairs would be critical and would be completed immediately, so there is a mismatch between the employee and management perspectives on the severity of the budget constraints. (*Asset Integrity & Reliability; Process Safety Culture*)

iv Catalyst Storage Tank Failure

The catalyst storage tank failed earlier than would have been expected had the fireproofing insulation been in good condition and the relief valve been adequate for the fire case. Witnesses indicate that several sections of the insulation had either fallen off or had been removed from the tank 2–3 months prior to the incident. The insulation had not been repaired. (*Asset Integrity & Reliability*)

v Relief Valve Sizing

A check of the catalyst storage tank relief valve sizing calculations indicates the valve was large enough for the fire case assuming the tank had fireproofing insulation, but it was undersized for an un-insulated vessel. The original relief valve design calculations could not be found. The relief valve may also have been compromised by improper maintenance or pluggage. The last relief valve preventative maintenance and pop test occurred five years prior to the incident. No records were found for years prior to this pop test. (*Mechanical integrity*)

Although the system failed below its design pressure, the overfilling of Kettle No. 3 caused a higher than normal pressure in the system. There were several causal factors for the Kettle No. 3 system being filled completely:

vi Operator Error

The control room operator did not stop filling Kettle No. 3 at the normal level of 85%. (*Human Factors: An operator error, but one that would be expected to occur over the normal life of a process*)

vii Safety Critical Equipment Inhibited

The Kettle No. 3 high-level alarm was bypassed, so it did not annunciate or log to the DCS alarm log. The operators bypassed the alarm because it

was set below the current normal batch level. The batch size had been changed from a 70% level to an 85% level but the alarm was still set for 80%; as a result, the batch level alarm was going off each time Kettle No. 3 was filled to the new normal batch level. (*Management of Change, Conduct of Operations*)

viii Absence of Redundant Protection

There was no redundant back-up protection (second level or monitoring of the pump) to shut down the pump in case it was blocked in. The hazard identification & risk analysis (HIRA) for the raw material storage, catalyst preparation, and catalyst storage areas was up for renewal this year. The prior HIRA was not as thorough as expected by today's standards. The corporation has now established criteria for HIRA leaders and has an approved list of resources. (*Hazard Identification & Risk Analysis, Engineering Design*)

Note: The isopentane feed valve is designed to fail closed on power failure, to prevent reverse flow from the kettles to the raw material storage tanks. This is the appropriate failure position for this valve.

Other Causal Factors:

Other causal factors were related to possible improvements in emergency planning and response, as follows:

ix Fire Brigade Procedures

No fire brigade member reported to the fire pump house when the fire alarm sounded. Interviews suggest personnel were confused about whose responsibility it was to go to the fire pump house. This may be a training or drill issue. (*Emergency Management*)

x Understanding of Fire Hazards

The fire brigade approached the catalyst preparation area to attempt rescue of a victim while firewater was unavailable. The small amount of water available on the fire engine was enough to protect the rescuers from the radiant heat from the fire, but was no protection against metal fragments. While the fire brigade did not recognize the potential hazards of this incident, further investigation is needed to determine if the emergency responders received insufficient training or if the emergency response plan is deficient in this area. (*Emergency Management*)

xi Personnel Headcount Procedures

The presence of the contractor (working in the instrument house) was not known to unit personnel. The contractor works in the area routinely, sometimes in the instrument house and sometimes in the rack. Because the instrument house is a general purpose area, a permit is not required

for the routine equipment calibration. The contractor did not check in with the control-room when he was going to work in the instrument house because a permit was not required. Interviews with the other contractors who performed similar work confirmed that this was the standard practice. None of the unit personnel had complained to the contractors about not checking in for the routine work in the instrument house in the 2 years the contractors had been doing this job. *(Emergency Management, Contractors Management, Safe Work Practices)*

xii Evacuation Procedures

There was no procedure to evacuate nonessential personnel from the area in the case of a high LEL alarm or a power failure. Because the contractors and some other workers in the area do not have radios to monitor unit communications, they would not know to leave the area unless the evacuation alarm was sounded. *(Emergency Management)*

xiii Gas Detector Reliability

The LEL detectors have frequent false high alarms which make unit personnel less responsive to the alarms going off. Further investigation is needed to determine the source of the LEL detector false high alarms. *(Asset Integrity & Reliability)*

xiv Operator Response

The procedure that states that the operator goes directly to the area of a high LEL alarm puts the operator in possible danger. If possible, risks to production personnel may be reduced with better data to decide on the appropriate alarm response. Further investigation is needed to determine if this is feasible. *(Emergency Management)*

Recommendations

The team looked at the structure of the trees and the bottom events on the trees to develop the following list of recommendations and timing. They also assigned each action to the appropriate individual in the plant. The due dates are shown in parentheses following the action.

1. Replace all corroded isopentane, catalyst mix, or fire damaged lines and equipment. For carbon steel lines without an inspection history, pull all insulation before inspection. *(Before startup)*
2. Review the rest of the asset integrity management program to ensure all critical equipment, piping, and pumps have acceptable integrity and an established inspection program with guidelines for repair. Include inspection and repair of fireproof insulation in the program. *(By March)*
3. Improve documentation of relief valve inspection and pop tests. Annual testing of relief valves is recommended until a valve has a history of good pop tests. Then the frequency can be slowly extended. *(Program)*

established by March)

4. Establish a weekly fire pump start and check program to be sure that this equipment works as intended. Revise the procedure to run the diesel pumps for a minimum of 30 minutes to detect overheating problems. Establish a preventive maintenance program to oversee all the maintenance on all the fire water pumps. Establish a high priority (Priority 1) maintenance task for repairs on the fire equipment. *(Before startup)*
5. Establish criteria for finding the cause of dead batteries on the diesel fire water pumps and for checking that recharged batteries retain the charge. Establish criteria for replacing impaired batteries. *(Before startup)*
6. Conduct a thorough Hazards Identification & Risk Analysis (HIRA) for the following areas: raw material storage, raw material feed systems, catalyst preparation, and catalyst storage. The HIRA leader must be on the approved corporate list. Ensure the following scenarios are considered:
 - Loss of utilities including electrical power, steam, cooling tower water, instrument air, and nitrogen.
 - Unit must be able to safely shut down on loss of any critical utility.
 - Deadheaded pumps, especially those pumps carrying liquids with a low flash point.
 - Leaks on flammable or toxic material systems. Give special consideration to whether the LEL detectors are correctly located and whether they offer complete coverage.
 - Response to high alarms on unit LFL detectors.
7. Review the emergency procedures for the allowable time to diagnose and act and the required response time for the system to recover after corrective action. Do a human reliability analysis on the actions, including the time for an operator to walk to the remote location. For critical actions (high consequence potential) with a required short time period for diagnosis and action, automatic interlocks should be installed. Consider a fault tree analysis to determine the reliability of the interlock designs. *(By November)*
8. Reinforce the management of change procedure with all personnel. Ensure that project leaders confirm that all parts of the change (such as alarm set point changes) are finished before the project is closed out. Ensure that Operations personnel follow the special procedure for disabling (silences alarms but they continue to log) or inhibiting alarms (prevents alarms from logging) and other safety critical equipment.
9. Establish a strong preventative maintenance program for the unit LEL detectors. Develop a good record keeping system for the testing program to aid in the diagnosis of problem detectors. *(Program established within 60 days after startup)*
10. Establish clear procedures for contractor and other non-operating

personnel entry and check-in to production units. No one should be out in the operating area without the unit personnel knowing they are there (includes maintenance workers, engineers, and other workers who routinely enter the area). (*Before startup*)

11. Establish criteria to pull the evacuation horn. Drill in evacuation once per quarter on each shift (one drill per quarter must be on days). Consider a public address system to communicate with visitors, maintenance workers, contractors and others who may not have radio communication. (*By November*)
12. Develop drills and talk-throughs for emergency procedures. Set priorities for emergency actions and have the personnel memorize and drill the most important actions. (*By November*)
13. Improve training and drill for the fire brigade members to ensure that someone reports to the fire pump house. (*Before startup*)
14. Improve the emergency response procedures, training, and drills, to help the fire brigade members respect the potential hazards of an incident and avoid unnecessary exposure, particularly when firefighting capabilities are below par. (*Plans complete by November*)

Attachments

- Simplified Process Flow Diagram
- Plot Plan
- Sequence of Events
- Logic Trees

Criteria for Restart

1. All recommendations required for restart (labeled *before startup* in the above list) must be completed. The rest of the above-listed recommendations should be completed by the indicated dates.
2. All changes introduced during repair and installation of the recommendations must go through a Hazards Identification & Risk Analysis (HIRA).
3. A walk-through safety, health, and environmental review must be completed after construction and before introduction of chemicals to ensure that repairs and additions have been made as intended.
4. Startup must be authorized by the signatures of the Operations Manager, Maintenance Manager, and Safety Supervisor (all three signatures are required).

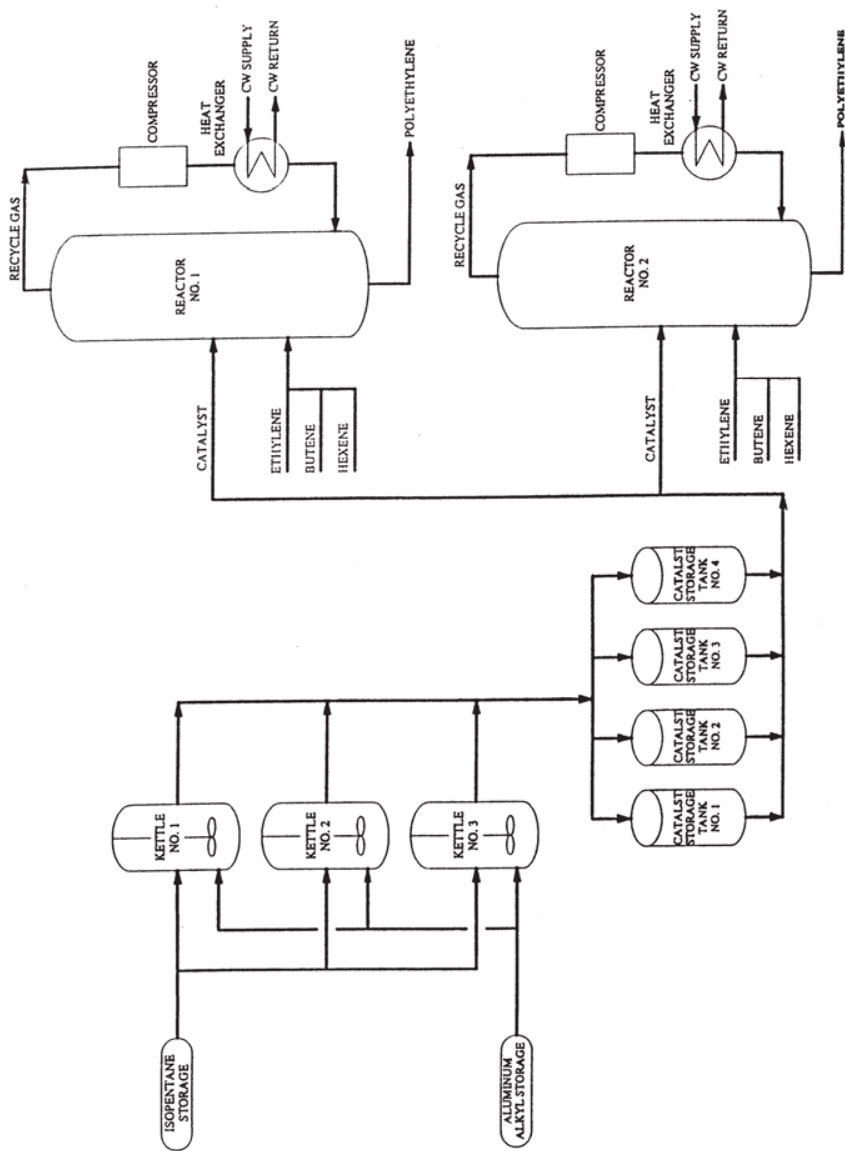
Additional Opportunities for Improvements

The following items were not related to the causes of the incident. Nonetheless, the investigation team felt that they represent additional opportunities in the future. These items do not impact restart.

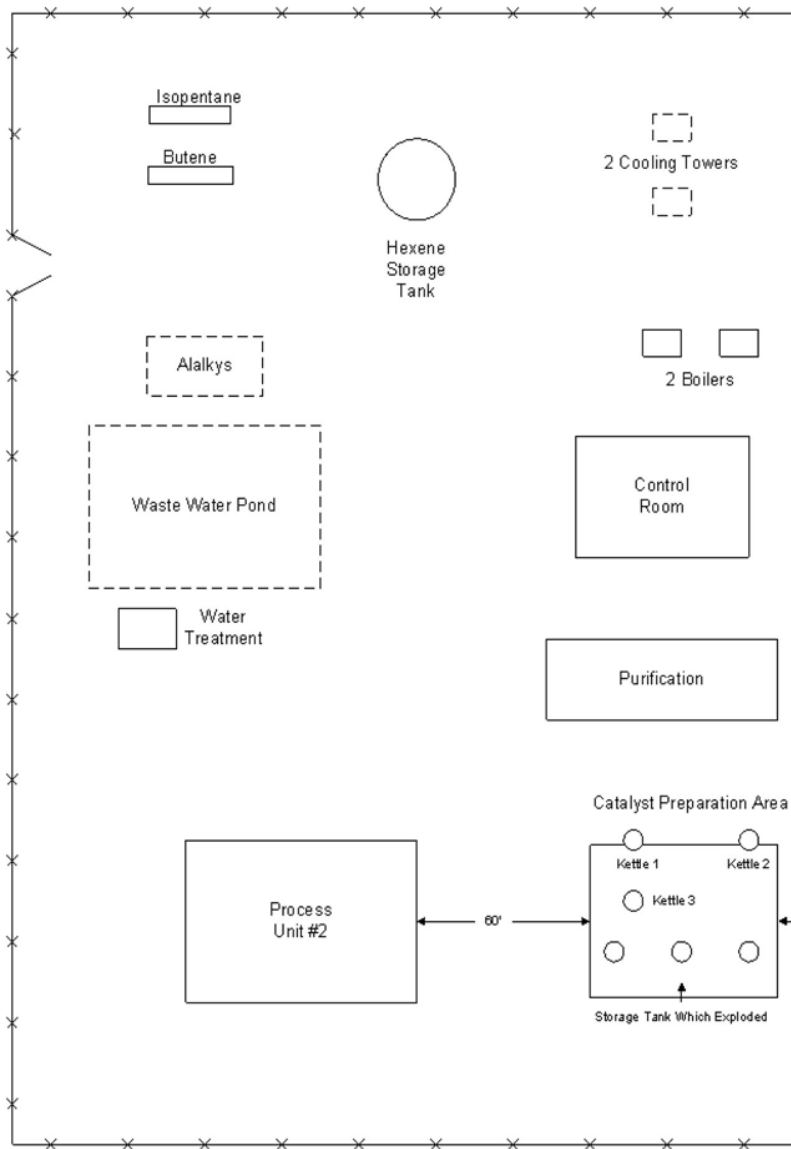
1. Review sloping of the catalyst mix kettle and catalyst storage tank dikes. Although the design intent was to slope the dikes to the sump, the dike collects liquid in some areas. Consider separating the dike for the catalyst mix kettle and catalyst storage tanks.
2. Clearly define a process for delaying maintenance and capital work in the event of budget constraints. Critical repair work should not be delayed. Environmental, Safety, and Health reviews should be conducted on delay of scheduled mechanical integrity program inspections.

Signatures

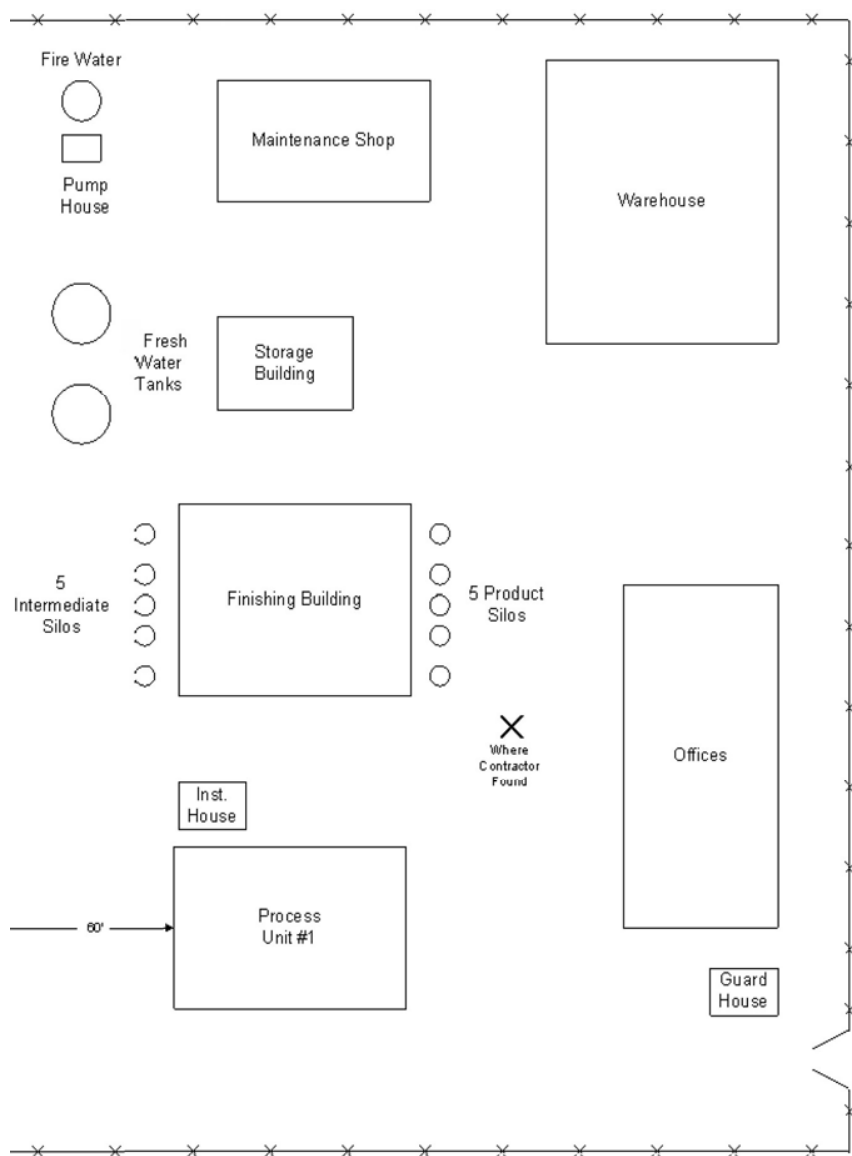
_____	_____
Team Leader	Date
_____	_____
Safety Supervisor	Date
_____	_____
Operations Manager	Date
_____	_____
Plant Manager	Date



Simplified Process Flow Diagram



Plot Plan (1 of 2)



Plot Plan (2 of 2)

Sequence of Events

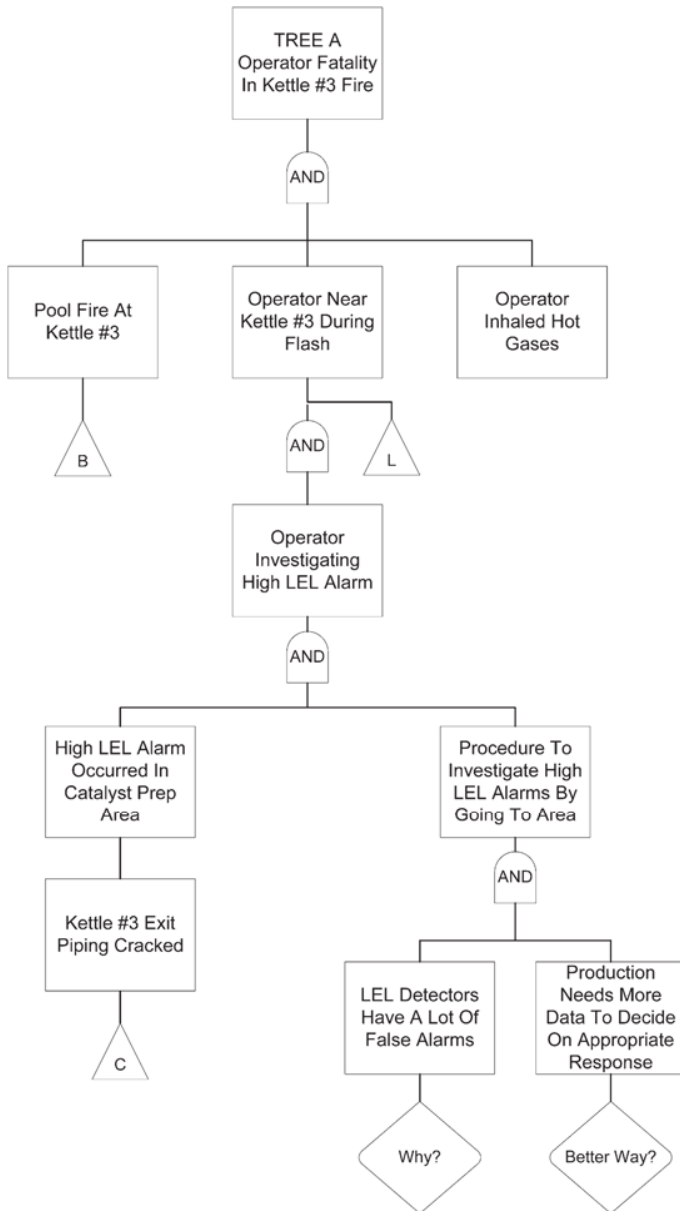
DATE	TIME	EVENT
-5 yrs		Last relief valve inspection and testing for Kettles and Catalyst Storage tanks. (<i>Maintenance records</i>)
-16 mo.		Corrosion control project proposed by maintenance superintendent.
-15 mo.		Last critical instrument check for No. 3 kettle (<i>Maintenance records</i>)
-1 mo.		No. 1 diesel fire pump taken out of service due to overheating during annual performance testing by outside agency. (<i>Maintenance records</i>) No. 2 diesel fire pump fails to start automatically due to weak batteries. (<i>Maintenance records</i>) Maintenance recharges No. 2 diesel fire pump batteries. (<i>Maintenance records</i>)
-1 mo.		Corrosion control work completed around Polyethylene Reactors. (<i>Maintenance records</i>)
-28 days		Last maintenance check of No. 2 diesel fire pump and the electric fire pumps. Test run of 5 minutes. (<i>Maintenance records</i>)
Aug 1	~ 10:30 A.M.	Service contractor enters area to calibrate equipment in the Polyethylene Reactor No. 1 instrument house. (<i>Interview</i>)
	10:30:33 A.M.	Control operator initiates filling of Kettle No. 3 (started remotely). (<i>DCS</i>)
	~11:00 A.M.	Severe thunderstorm starts. (<i>Interviews</i>) Ambient temperature 85°F, NW winds @ 3mph (<i>Plant weather station log</i>)
	11:00:47 A.M.	Kettle No. 3 reaches high 90% level (<i>DCS</i>) <i>Note:</i> High level alarm did not register in the DCS log. Later, the alarm is found to be inhibited.
	11:03:15 A.M.	Kettle No. 3 reaches 120 psig high pressure alarm (<i>DCS</i>).
	11:03:45 A.M.	Kettle No. 3 high pressure alarm acknowledged by control operator (<i>DCS</i>).
	11:05:03 A.M.	Plant-wide electrical power outage. Isopentane supply trips off: no power. (<i>DCS</i>) Main control valve for isopentane storage tank fails closed (as designed) on electrical failure. (<i>DCS</i>) 120 psig pressure trapped in Kettle No. 3 and related piping (<i>Concluded from data</i>). Outside operator goes to manually block in reactor feeds (<i>Part of emergency shutdown procedure</i>).

Sequence of Events (cont.)

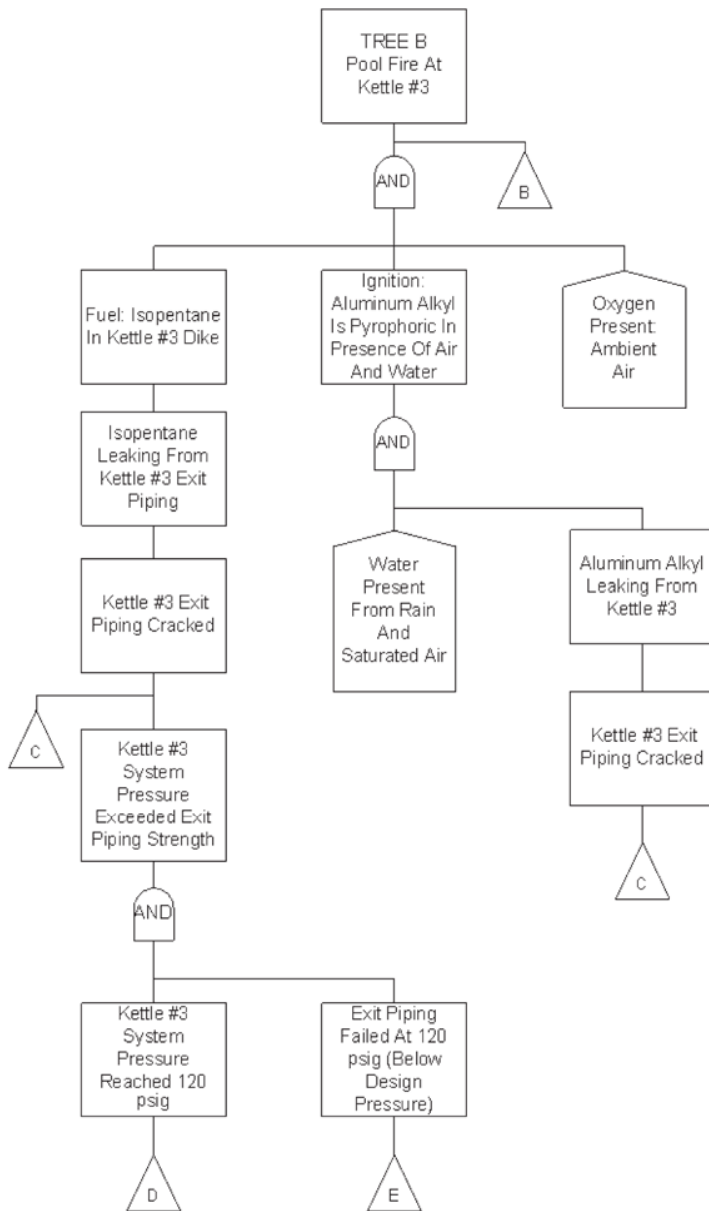
DATE	TIME	EVENT
Aug 1	~11:09 A.M.	Kettle No. 3 discharge piping cracks. Contents of kettle start dumping to the curb. Isopentane vapors spread as material flashes. <i>(Concluded from data).</i>
	11:09:30 A.M.	LEL detectors in Catalyst Prep area alarm. <i>(DCS)</i>
	After 11:09:30 A.M.	Control room operator requests by radio for the lead outside operator to visually inspect Kettle No. 3 due to high LEL alarm. Thunderstorm has passed and rain is diminishing.
	~11:10 A.M.	Whooshing” noise heard by many. <i>(Assumed to be fireball)</i> Contractor is just coming out of instrumentation house when he sees operator running towards catalyst prep area. Contactor sees fire flash throughout catalyst prep area. He remembers trying to get away from the heat.
	11:10:21 A.M.	Heat detector alarms for catalyst preparation area (Kettle No. 3 area) annunciate in control room. <i>(DCS)</i>
	After heat detector alarms	Control room operator tries to reach lead outside operator by radio, but there is no response.
	~11:11 A.M.	Catalyst preparation supervisor activates plant fire brigade using plant fire alarm and notifies plant dispatch by radio <i>(Plant dispatch log)</i>
	~11:12 A.M.	Catalyst preparation supervisor notifies local volunteer fire department by telephone. <i>(Local fire department log)</i>
	~11:15 A.M.	Plant fire brigade reaches the emergency location. They: <ul style="list-style-type: none"> • see fire engulfing catalyst prep area (automatic deluge sprinkler had actuated, but no water was available) • see the lead outside operator down about 40 feet from the catalyst prep area, • find the injured (unidentified at that time) service contractor about 120 feet away, Plant fire brigade then: <ul style="list-style-type: none"> • tries to activate a fixed monitor, but no water flows, • sends one brigade member to fire pump house to check pump status.
	~11:18 A.M.	Fire brigade member reaches pump house and finds: <ul style="list-style-type: none"> • electric fire pump inoperable due to power failure, • one diesel fire pump inoperable due to known mechanical problems, • second diesel would not start due to dead batteries; calls for maintenance help. Several maintenance employees dispatched to repair diesel fire pump No. 2.

Sequence of Events (cont.)

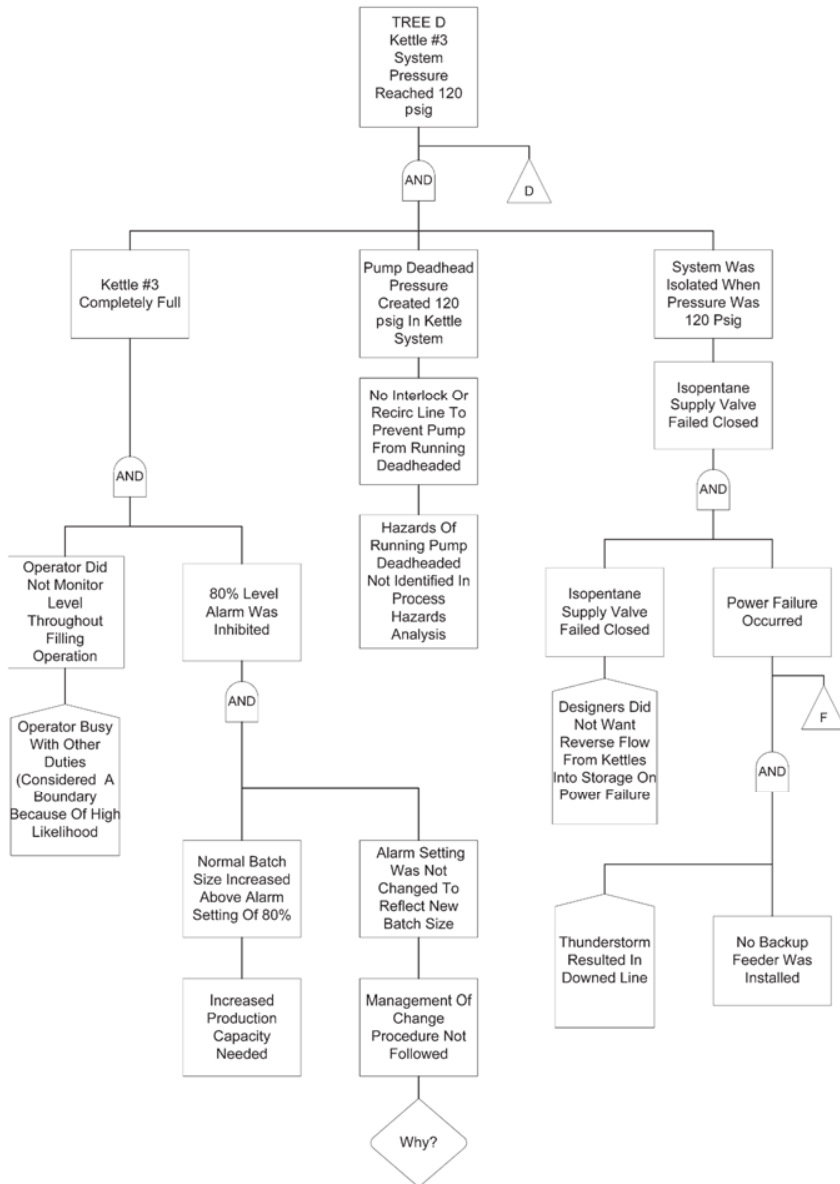
DATE	TIME	EVENT
Aug 1	~ 11:20 A.M.	Fire brigade uses limited water supply on engine to shield two members of team and attempts rescue of lead operator. Another explosion occurs and four fire brigade members are injured by metal fragments.
	~11:22 A.M.	Local fire department arrives.
	After 11:22 A.M.	Spread of fire is slowed using water from fire department trucks.
	~11:30 A.M.	Maintenance completes move of batteries from No. 1 diesel fire pump to No. 2 diesel fire pump. No. 2 diesel fire pump is started.
	After 11:30 A.M.	Automatic deluge sprinkler system found to be severely damaged by fire / explosions and is now valved into OFF position. Three fixed fire monitors directed on fire at full flow. Two hose streams from hydrants directed on fire also.
	~11:58 A.M.	Fire deemed under control.
	~12:10 A.M.	Final extinguishment of fire.
Aug 2		Lead operator dies from burn complications.
Aug 3		No. 1 diesel fire pump repaired.



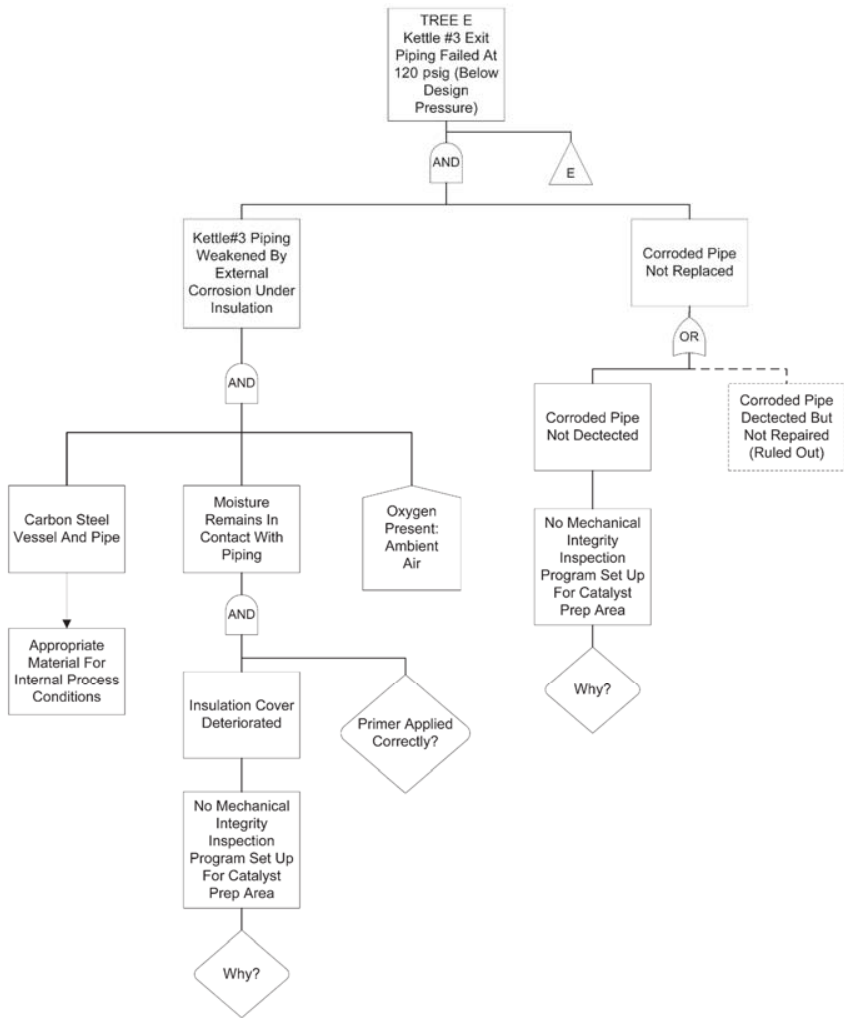
Logic Tree (1 of 9)



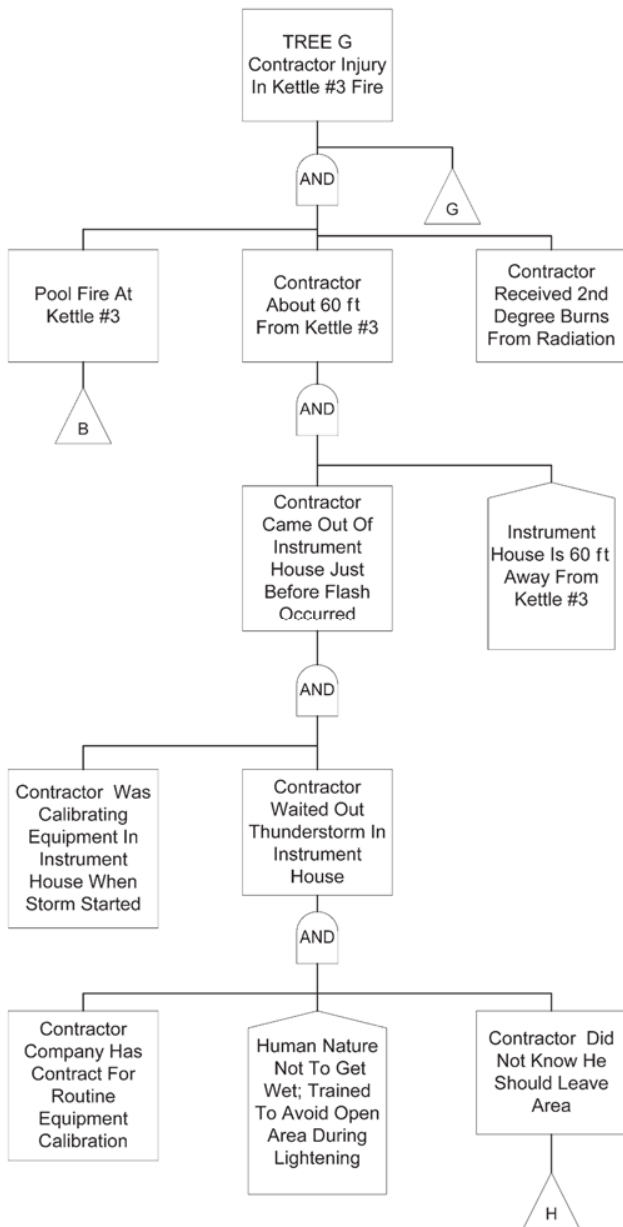
Logic Tree (2 of 9)



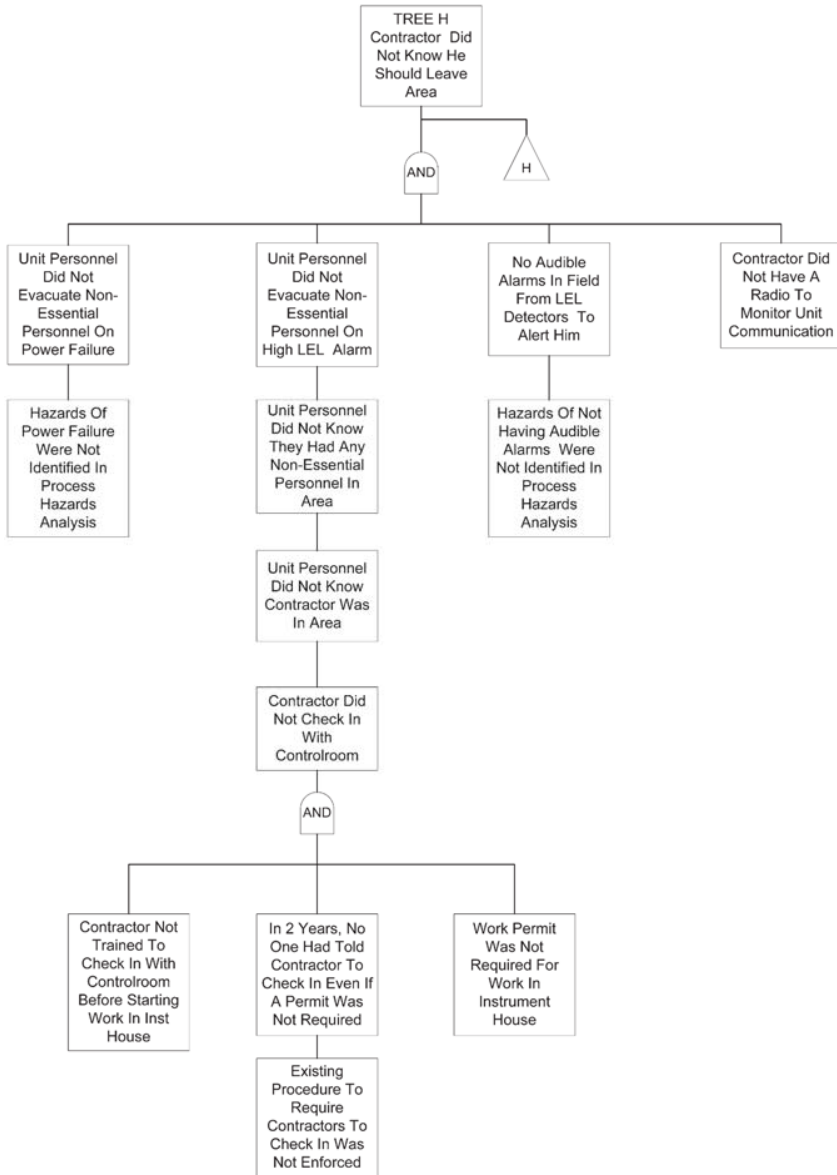
Logic Tree (3 of 9)



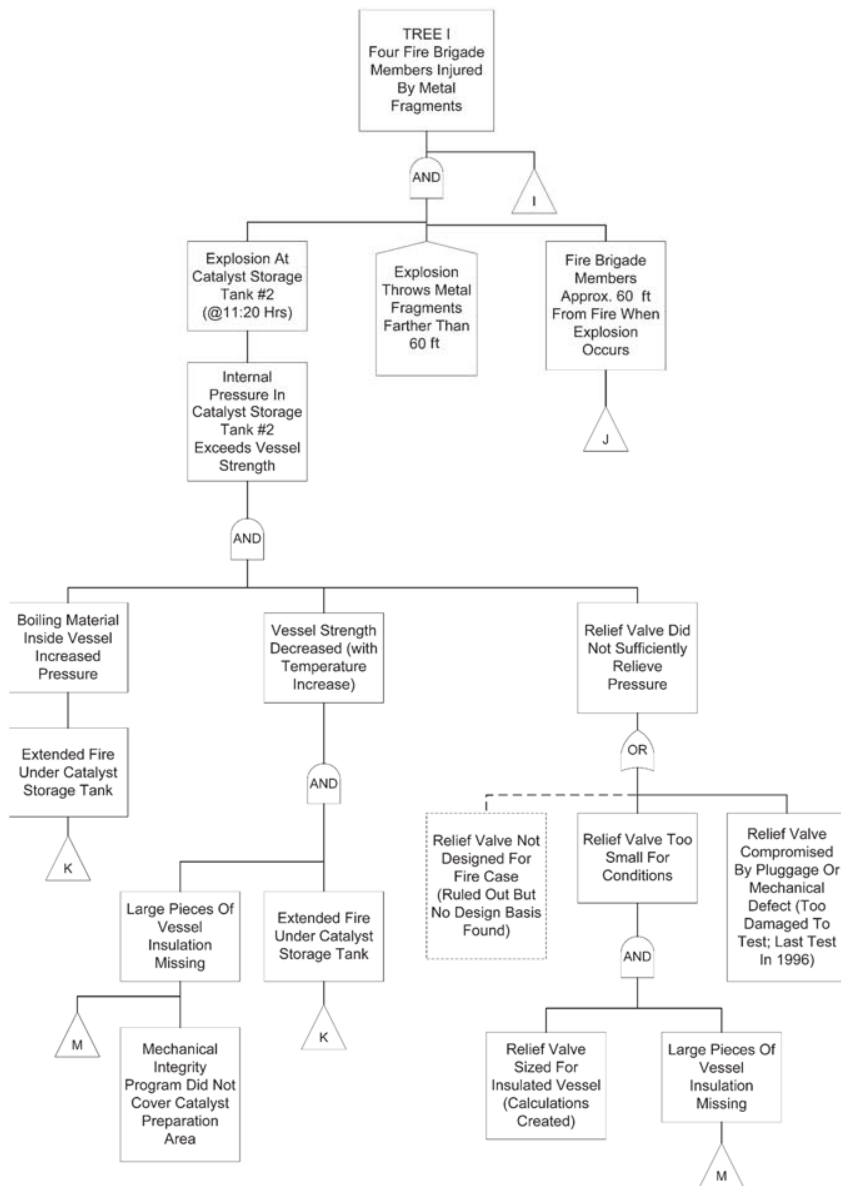
Logic Tree (4 of 9)



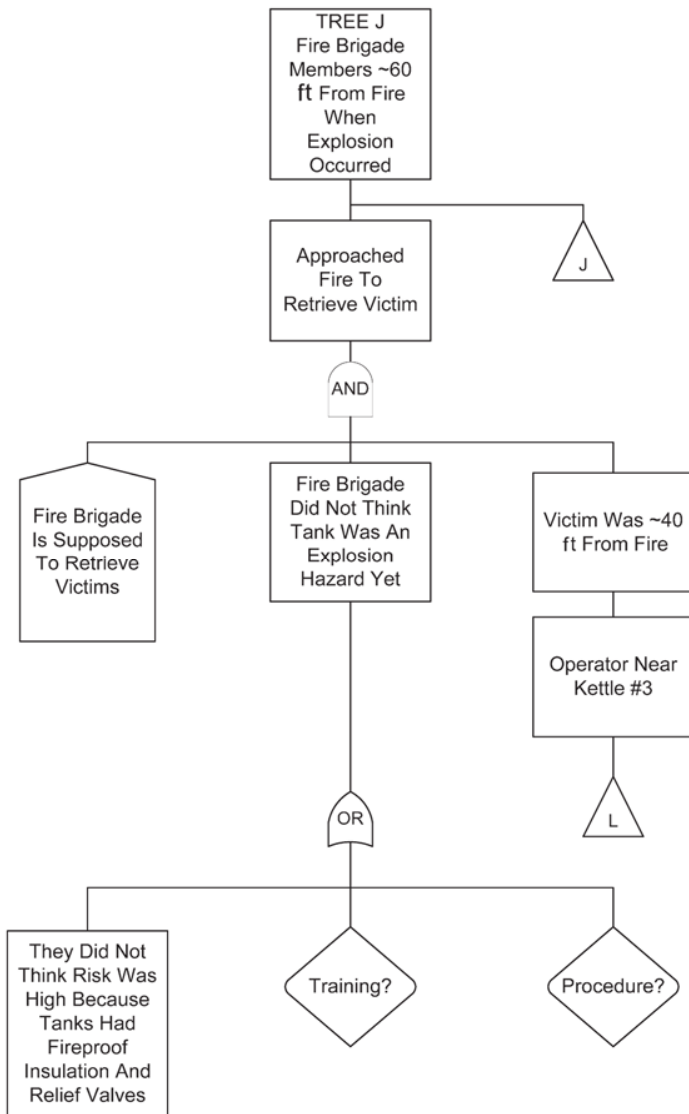
Logic Tree (5 of 9)



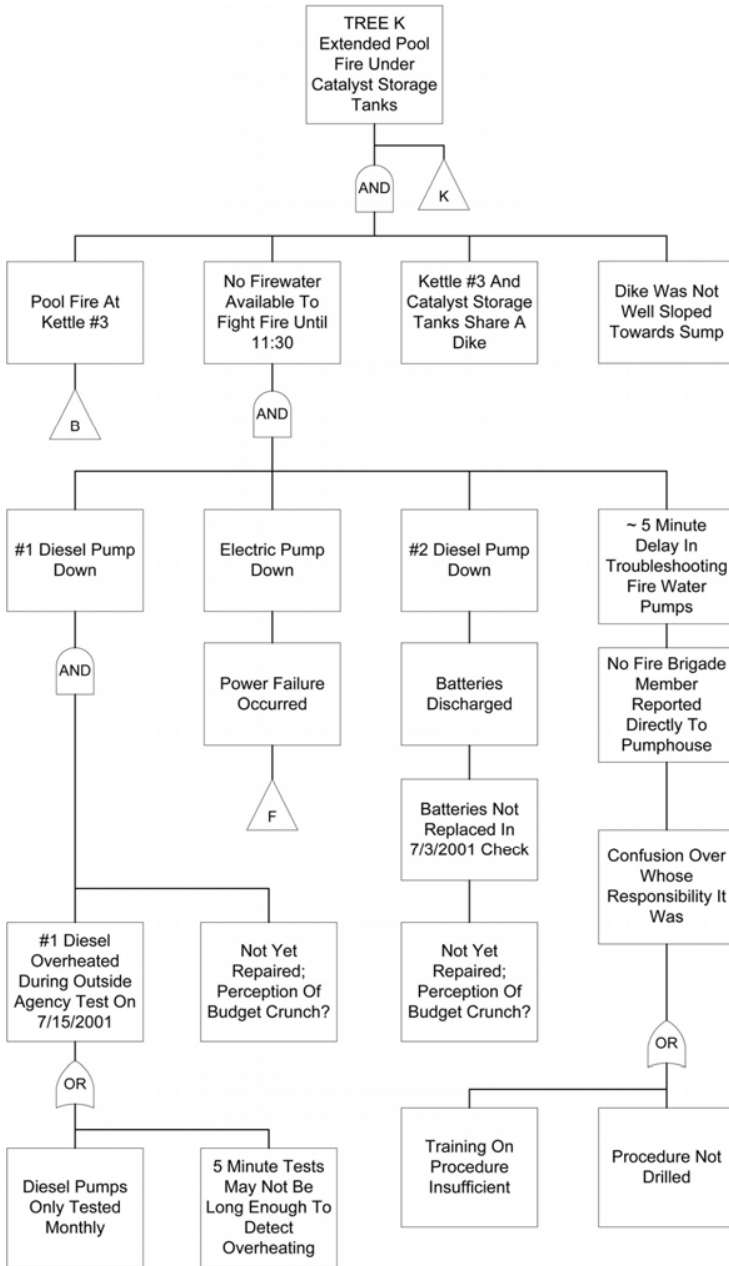
Logic Tree (6 of 9)



Logic Tree (7 of 9)



Logic Tree (8 of 9)



Logic Tree (9 of 9)

APPENDIX E.

QUICK CHECKLIST FOR INVESTIGATORS

The following checklist is intended to be used as a quick reminder of some key considerations for people on their way to an investigation. Incidents are unique and have unique requirements but the information included should be adequate reminders for most incidents.

Physical Items

Photographic Equipment

- Digital cameras, spare batteries, charger and cables
- Check the date and time on the cameras and that the metadata is properly recording the date and time.
- External flash and batteries
- Video camera, spare batteries, charger and cables
- Memory cards
- Tripod

Measurement Tools

- Tape measures
 - 50 feet
 - 25 ft
 - 10 feet (small, narrow)
 - Builders/engineers “Pocket Rod” – 6 ft
- 6-inch ruler
- Calipers – combination inside and outside
- Micrometer – 1 inch

Documentation Aids

- Dictaphone
- Notebooks
- Clipboard
- Pens and pencils
- Laptop or tablet computer

Evidence Marking Aids

- Paint pens
- Grease pens
- Permanent markers
- Tags with wire or plastic tie wrap connectors
- Orange flagging tape
- Evidence tags
- Disposable gloves

Evidence Collection Aids

- Self-closing plastic bags in a variety of sizes
- Tweezers
- Forceps
- Scrapers
- Sample bottles

Personal Protective Equipment

- Hard hat
- Safety goggles
- Steel-toed shoes
- Fire retardant coveralls
- Gloves – rugged for rough surfaces, climbing ladders, etc.
- Hearing protection
- Special PPE for chemical hazards as needed
 - Chemical resistant coveralls
 - Respirator with appropriate cartridges
 - Chemical resistant gloves
 - Chemical resistant boot covers or boots

Other

- Mobile phones
- Electric circuit tester
- Multi-purpose tool (pliers, knife, screwdriver, etc.)
- Compass
- Magnet
- Duct tape
- Mirror
- Small pocket mirror
- CCPS *Guidelines for Investigating Process Safety Incidents*
- Sticky notes
- Sticky flags
- Flashlights
- Magnifying glass

Action Reminders

- **Controlling the incident is first priority.** Until Incident Command has extinguished fires, evacuated injured personnel, completed a headcount, and contained spills/stopped releases, the control of the incident is first priority.
- **Secure the scene.** As soon as possible, protect the scene of the incident from disturbances. Work through operations, maintenance, and emergency response personnel to ensure the scene is not disturbed. Establish a system to limit and control entry into the area. Establish a system to log and document any changes made to the scene during emergency response and further changes that must be made for safety purposes.
- **Establish the incident investigation team.** A major investigation needs the best people available to represent each needed discipline. Frequently contractors/consultants will be needed for special expertise.
- **Establish systems for legal considerations.** Confer with corporate counsel to establish systems to protect company proprietary and privileged information. Determine whether the investigation team will be the primary contact with government agencies. Establish systems for collecting and securing documents and other data.
- **Time sensitive evidence is a high priority.** Gathering evidence that might deteriorate with time should be high priority.
 - Many electronic systems record data from operating units and then delete that data after a specified period of time, often 24 hours or less. Systems connected to historian recording systems

may have recent data at more frequent intervals for a limited time period then start to average over a longer period.

- Some evidence such as burn char patterns, surface fractures, or volatile chemicals spills can degrade as a result of weather conditions (rain, wind, or sunlight)
- **Ensure that the investigation meets regulatory requirements.** For example, OSHA has specific requirements for the incident investigation teams. OSHA 1910.119 (m) (3) states: *An incident investigation team shall be established and consist of at least one person knowledgeable in the process involved, including a contract employee if the incident involved work of the contractor, and other persons with appropriate knowledge and experience to thoroughly investigate and analyze the incident.* Requirements in other jurisdictions may differ.
- **Establish roles and expectations for the investigation team.** Roles and expectations need to be defined early so that there are no misunderstandings.
 - What expectations do local management and corporate management have for the investigation team for timing, interim reports, final reports, and defining requirements for startup of units or equipment?
 - What resources are available and just as important, what resources are not available?
- **Interviews need to be done promptly.** Memories fade with time and are influenced by discussions with other witnesses.
 - Interviewing techniques are important.
 - Plan the interview. Do not do it haphazardly.
 - Interview one person at a time and in a private comfortable setting. Use only one or two interviewers.
 - Set the interviewee at ease. One method is by asking questions about activities prior to the incident.
 - Be sensitive to the interviewee's emotional state.
 - Do not express opinions.
 - Do not lead the interviewee. Ask questions that allow the interviewee to describe the incident in their own words. Questions should be neutral, unbiased, and non-leading.
 - Do not interrupt the interviewee.
 - Use a plot plan to better understand
 - « the location of interviewee
 - « the location of people and activities the interviewee saw
 - « movement of the interviewee

- Ask what the interviewee saw, heard, felt, and smelled before, during, and after the incident.
- Ask about timing/sequence of events to help develop the timeline.
- At the end of the interview, if the interviewee has anything to add that was not already covered
- **Gather information about the process early.** The investigation team will need information about the process, equipment, operations, maintenance, and changes. Gathering the information can sometimes be done while waiting to gain access to the unit for physical inspection and data gathering.
 - Plot plans
 - Process description
 - P&ID's
 - Information about the chemicals in the area
 - Process data that is accessible outside of the scene
 - Maintenance data
 - PHAs
 - MOCs
 - Prior incident investigation reports
- **Follow established safety policies.** Incident investigation team members should lead by example by strictly following site safety policies.
- **Initial work is focused on "what" happened.** Determination of root causes is important to prevent recurrence of the incident, but the initial focus of the investigation team is to define "what" happened.
- **Photograph the scene.** Photograph overall views and specific items.
 - Decide if still photography is adequate or if video photography is also needed.
 - Photographs should be taken to document as-found location, orientation, and condition of items deemed to be evidence.
 - Logging all photographs with information such as item, location, orientation, and date may be helpful.
- **Establish a timeline.** The investigation of almost every significant incident will require the development of a timeline to depict the sequence of events before, during, and after the incident.
- **Establish an evidence collection, preservation and storage system.** Assign personnel and equip them to collect evidence. Make available a secure evidence storage location(s)/facilities with restricted access to physical evidence that is removed from the scene. Appoint an evidence custodian. Log all evidence. Establish a system to control access to

the evidence.

- **Secure all documents collected and used in the investigation.**
Secure the investigation room and any other room that is used to store the investigation documents. Determine the method by which evidence will be physically gathered.
 - Incidents with significant debris may require the establishment of a grid system to define the exact location of specific pieces.
 - Establish a method for documenting as found positions, such as valves, switches, and debris.
 - If evidence items were exposed to chemicals, determine if the evidence will have to be decontaminated for evidence storage. If so, establish an evidence decontamination procedure.
- **Develop a list of potential hypothesis and remain open minded.** On complex incidents, it is sometimes helpful to develop a list of potential hypothesis. Do not fall into the trap of only pursuing the initial obvious hypothesis. It is important to prove that the actual hypothesis did happen but it is also important to prove that other potential hypotheses did not happen.

APPENDIX F.

EVIDENCE PRESERVATION CHECKLIST

– PRIOR TO ARRIVAL OF THE

INVESTIGATION TEAM

Preservation of evidence at the incident scene is a critical requirement for a successful investigation. It may not be possible for an investigation team to be promptly on site. There may be interested parties at the site, including emergency services, regulatory authorities etc., whose priorities and instructions may not be aligned with each other and the facility. Nevertheless, effective actions can be taken by site staff to help prepare for the investigation and to preserve evidence before the arrival of the investigation team, including those detailed on the checklist below, subject to safety and legal requirements.

It would also be helpful if the site were to establish the personal protective equipment (PPE) requirements, before the arrival of the investigation team.

EVIDENCE PRESERVATION CHECKLIST
<ul style="list-style-type: none"> • Consult legal and medical department on determining requirements for collecting blood and other biological samples, as appropriate.
<ul style="list-style-type: none"> • Record environmental factors at the time of incident, including wind strength & direction, temperature, light, precipitation, humidity, etc.
<ul style="list-style-type: none"> • Determine through risk assessment of the site where evidence preservation activities can take place and where entry is disallowed.
<ul style="list-style-type: none"> • Establish security presence at incident scene and establish an "exclusion zone" (e.g., a team of responsible people before barriers can be installed).
<ul style="list-style-type: none"> • Install tape/ barriers to prevent unauthorized access to the incident scene.
<ul style="list-style-type: none"> • Limit and log all personnel movements in and out of the exclusion zone
<ul style="list-style-type: none"> • Instruct all personnel to not touch any item, equipment or debris, unless it needs to be moved or adjusted for reasons of health, safety or environmental protection. Photograph where possible before moving items.
<ul style="list-style-type: none"> • Record changes made to equipment during or post incident response, e.g., changes to valve positions, electrical switches, etc. Changes may be made by emergency response teams, process teams etc. as a means to reduce a potential hazard, but all adjustments must be recorded.
<ul style="list-style-type: none"> • Have all personnel (operations and emergency response) separately and simultaneously prepare a written statement of their observations and actions.
<ul style="list-style-type: none"> • Prevent removal of evidence from scene, except that needed for emergency response and management of hazards.
<ul style="list-style-type: none"> • If debris is present off-site and must be recovered to prevent loss of evidence, record locations and orientations, photograph, preserve and secure.
<ul style="list-style-type: none"> • Conduct extensive photographic / video / drone survey of site.
<ul style="list-style-type: none"> • Check and maintain power supplies to computer systems to help preserve electronic data. • DO NOT attempt to <u>restore</u> electrical power supplies to electronic systems without expert advice.
<ul style="list-style-type: none"> • Initiate recovery of time sensitive data including process data, water/ chemical damaged paper records, chemical samples from breached equipment, etc. Contact OEMs for computer system for advice on preservation of raw data before it is overwritten or averaged/trended onto a historian.
<ul style="list-style-type: none"> • Secure copies of any recordings from security cameras and any photographs of the scene prior to and after the incident.
<ul style="list-style-type: none"> • Request copies of any recordings or photographs of the incident from personal electronic devices. Do not forget to include emergency responders in this request.
<ul style="list-style-type: none"> • Ensure paper records are kept in or moved to a dry location. Create photographic copies of all paper records for electronic storage.
<ul style="list-style-type: none"> • Take action to prevent any paper-type chart recorders from being overwritten. See 8.2.3
<ul style="list-style-type: none"> • Take samples of liquids as equipment is being drained and label clearly.
<ul style="list-style-type: none"> • Document locations of items that need to be moved. Surveyors may be useful for some circumstances.
<ul style="list-style-type: none"> • Document the "as-found" configuration of process equipment and piping. Compare to P&IDs and note any differences.

APPENDIX G.

GUIDANCE ON CLASSIFYING POTENTIAL SEVERITY OF A LOSS OF PRIMARY CONTAINMENT

Extract from

*Process Safety Leading and Lagging Metrics ...You
Don't Improve What You Don't Measure,
CCPS, 2011*

**Addressing Potential Chemical Impact of Tier 1
Process Safety Incidents**

(Note: This publication was superseded in 2018 and should only be used for the purposes of estimating potential severity of incidents.)

Process Safety Incident (PSI) (Tier 1 PSE per API RP - 754)

For the purposes of the common industry-wide process safety lagging metrics, an incident is reported as a process safety incident if it meets all four of the following criteria:

- (1) Process involvement
- (2) Above minimum reporting threshold
- (3) Location
- (4) Acute release

Process Involvement

An incident satisfies the chemical or chemical process involvement criteria if the following is true:

A process must have been directly involved in the damage caused. For this purpose, the term "process" is used broadly to include the equipment and technology needed for chemical, petrochemical and refining production, including reactors, tanks, piping, boilers, cooling towers, refrigeration systems, etc. An incident with no direct chemical or process involvement, e.g., an office building fire, even if the office building is on a plant site, is not reportable.

An employee injury that occurs at a process location, but in which the process plays no direct part, is not reportable as a PSI (though it could be an OSHA or other agency reportable injury). The intent of this criterion is to identify those incidents that are related to process safety, as distinguished from personnel safety incidents that are not process-related. For example, a fall from a ladder resulting in a lost workday injury is not reportable simply because it occurred at a process unit. However, if the fall resulted from a chemical release, then the incident is reportable.

Reporting Thresholds

An unplanned or uncontrolled release of any material, including non-toxic and non-flammable materials (e.g., steam, hot condensate, nitrogen, compressed CO₂ or compressed air), from a process that results in one or more of the consequences listed below:

Note: Steam, hot condensate, and compressed or liquefied air are only included in this definition if their release results in one of the consequences other than a threshold quantity release. However, other nontoxic, nonflammable gases with defined UNDG Division 2.2 thresholds (such as nitrogen, argon, compressed CO₂) are included in all consequences including, threshold releases.

1. An employee or contractor day(s) away from work injury and/or fatality, or hospital admission and/or fatality of a third party (non-employees/contractor)
 2. An officially declared community evacuation or community shelter-in-place;
 3. Fires or explosions resulting in greater than or equal to \$25,000 of direct cost to the company, or;
 4. An acute release of flammable, combustible, or toxic chemicals greater than the chemical release threshold quantities described on Table G.1. Note that Table G.1 has an additional threshold quantity level column which is recommended for indoor releases
- Releases include pressure relief device (PRD) discharges, whether directly or via a downstream destructive device that results in liquid carryover, discharge to a potentially unsafe location, on-site shelter-in-place, or public protective measures (e.g., road closure)

Table G.1 Process Safety Incident Threshold Values

Threshold Release Category	Material Hazard Classification ^{a, c, d}	Threshold Quantity	Recommended Threshold Quantity for indoor ^b releases (Optional)
1	TIH Zone A Materials	5 kg (11 lb)	2.5 kg (5.5 lb)
2	TIH Zone B Materials	25 kg (55 lb)	12.5 kg (27.5 lb)
3	TIH Zone C Materials	100 kg (220 lb)	50 kg (110 lb)
4	TIH Zone D Materials	200 kg (440 lb)	100 kg (220 lb)
5	Flammable Gases or Liquids with Initial Boiling Point ≤35 °C (95 °F) and Flash Point < 23 °C (73 °F) or Other Packing Group I Materials excluding strong acids/bases	500 kg (1100 lb)	250 kg (550 lb)
6	Liquids with Initial Boiling Point > 35 °C (95 °F) and Flash Point < 23 °C (73°F) or Other Packing Group II Materials excluding moderate acids/bases	1000 kg (2200 lb) or 7 bbl	500 kg (1100 lb) or 3.5 bbl
7	Liquids with Flash Point ≥23 °C (73 °F) and ≤60 °C (140 °F) or Liquids with Flash Point > 60 °C (140 °F) released at a temperature at or above Flash Point or strong acids/bases or Other Packing Group III Materials or Division 2.2 Nonflammable, Nontoxic Gases (excluding Steam, hot condensate, and compressed or liquefied air)	2000 kg (4400 lb) or 14 bbl	1000 kg (2200 lb) or 7 bbl

It is recognized that threshold quantities given in kg and lb or in lb and bbl are not exactly equivalent. Companies should select one of the pair and use it consistently for all recordkeeping activities.

a Many materials exhibit more than one hazard. Correct placement in Hazard Zone or Packing Group shall follow the rules of DOT 49 CFR 173.2a [14] or UN Recommendations on the Transportation of Dangerous Goods, Section 2 [10]. See Annex B.

b A structure composed of four complete (floor to ceiling) walls, floor, and roof.

c For solutions not listed on the UNDG, the anhydrous component shall determine the TIH zone or Packing Group classification. The threshold quantity of the solution shall be back calculated based on the threshold quantity of the dry component weight.

d For mixtures where the UNDG classification is unknown, the fraction of threshold quantity release for each component may be calculated. If the sum of the fractions is equal to or greater than 100%, the mixture exceeds the threshold quantity. Where there are clear and independent toxic and flammable consequences associated with the mixture, the toxic and flammable hazards are calculated independently. See Annex A, Examples 29, 30 and 31.

For a full list of materials cross-referenced to the UN Dangerous Goods definitions, see chemical list or spreadsheet tools posted on the web site www.ccpsonline.org

Location

An incident satisfies the location criteria if:

The incident occurs in production, distribution, storage, utilities or pilot plants of a facility reporting metrics under these definitions. This includes tank farms, ancillary support areas (e.g., boiler houses and waste water treatment plants), and distribution piping under control of the site.

All reportable incidents occurring at a location will be reported by the company that is responsible for operating that location. This applies to incidents that may occur in contractor work areas as well as other incidents.

At tolling operations and multi-party sites, the company that operates the unit where the incident initiated should record the incident and count it in their PSI metric.

For further clarification, look at the exclusions described in Section 6 (Applicability).

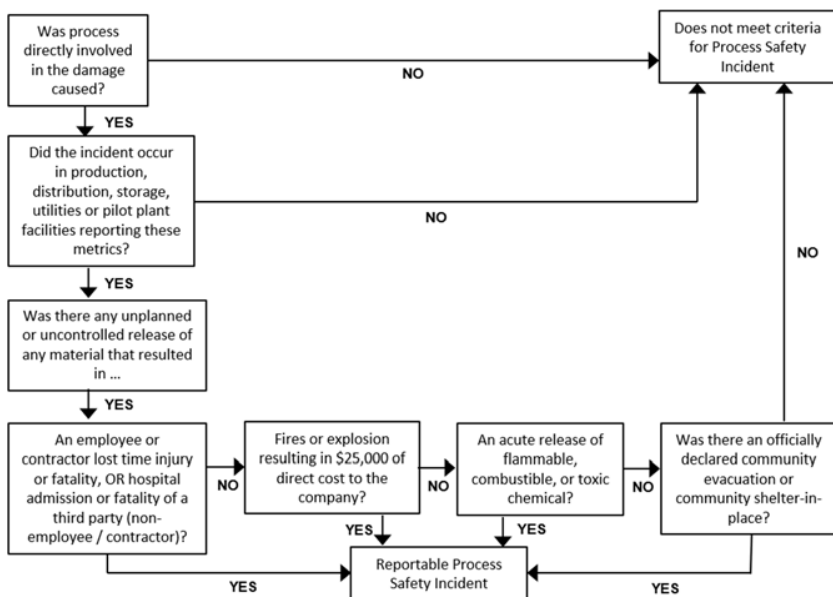
Acute Release

A "1-hour" rule applies for the purpose of the reporting under this metric, i.e. the release of material reaches or exceeds the reporting threshold in any 1-hour period. If a release does not exceed the TQ level during any 1-hour period, it would not be treated as a PSI. Typically, acute releases occur in 1-hour or less; however, there may be some releases that would be difficult to prove if the threshold amount release occurred in 1-hour. (Example: A large inventory of flammable liquid is spilled from a tank or into a dike overnight due to a drain valve being left upon prior to a transfer operation. It may not be discovered for several hours, so it is difficult to know the exact time when the threshold quantity was exceeded.) If the duration of the release cannot be determined, the duration should be assumed to be 1 hour.

Flowchart

The criteria for reporting incidents as a PSI described above are illustrated in the attached flowchart (Figure G.1).

Figure G.1 Determining if an Incident Meets Definition of a Reportable Process Safety Incident (PSI) under the Definitions of the CCPS Industry Lagging Metric



Process Safety Incident Severity

A severity level will be assigned for each consequence category for each process safety incident utilizing the criteria shown in Table G.2.

Table G.2 Process Safety Incidents & Severity Categories

Severity Level (Note 4)	Safety/Human Health (Note 5)	Fire or Explosion (including overpressure)	Potential Chemical Impact (Note 3)	Community/Environment Impact (Note 5)
NA	Does not meet or exceed Level 4 threshold	Does not meet or exceed Level 4 threshold	Does not meet or exceed Level 4 threshold	Does not meet or exceed Level 4 threshold
4 (1 point used in severity rate calculations for each of the attributes which apply to the incident)	Injury requiring treatment beyond first aid to employee or contractors (or equivalent, Note 1) associated with a process safety incident (In USA, incidents meeting the definitions of an OSHA recordable injury)	Resulting in \$25,000 to \$100,000 of direct cost	Chemical released within secondary containment or contained within the unit - see Note 2A	Short-term remediation to address acute environmental impact. No long term cost or company oversight Examples would include spill cleanup, soil and vegetation removal
3 (3 points used in severity rate calculations for each of the attributes which apply to the incident)		Resulting in \$100,000 to 1MM of direct cost	Chemical release outside of containment but retained on company property OR Flammable release without potential for vapor cloud explosives -see Note 2B	Minor off-site impact with precautionary shelter-in-place OR Environmental remediation required with cost less than \$1MM. No other regulatory oversight required. OR Local media coverage

Table G.2 Process Safety Incidents & Severity Categories (cont.)

Severity Level (Note 4)	Safety/Human Health (Note 5)	Fire or Explosion (including overpressure)	Potential Chemical Impact (Note 3)	Community/Environment Impact (Note 5)
NA	Does not meet or exceed Level 4 threshold	Does not meet or exceed Level 4 threshold	Does not meet or exceed Level 4 threshold	Does not meet or exceed Level 4 threshold
2 (9 points used in severity rate calculations for each of the attributes which apply to the incident)		Resulting in \$1MM to \$10MM of direct cost	Chemical release with potential for injury off- site or flammable release resulting in a vapor cloud entering a building or potential explosion site (congested/confined area) with potential for damage or casualties if ignited - see Note 2C	Shelter-in-place or community evacuation OR Environmental remediation required and cost in between \$1MM - \$2.5MM. State government investigation and oversight of process. OR Regional media coverage or brief national media coverage.
1 (27 points used in severity rate calculations for each of the attributes which apply to the incident)	Off-site fatality or multiple on-site fatalities associated with a process safety event.	Resulting in direct cost > \$10MM	Chemical release with potential for significant on-site or off-site injuries or fatalities – see Note 2D	National media coverage over multiple days OR Environmental remediation required and cost in excess of \$2.5MM. Federal government investigation and oversight of process. OR other significant community impact.

NOTE 1: For personnel located or working in process manufacturing facilities.

NOTE 2: It is the intent that the “Potential Chemical Impact” definitions shown in Table 2 to provide sufficient definition such that plant owners or users of this metric can select from the appropriate qualitative severity descriptors without a need for dispersion modeling or calculations. The user should use the same type of observation and judgment typically used to determine the appropriate emergency response actions to take when a chemical release occurs.

However, CCPS does not want to preclude the use of a “sharper pencil” (e.g. dispersion modeling) if a company so chooses. In those cases, the following notes are being provided, as examples, to clarify the type of hazard intended with the four qualitative categories:

A: AEGL-2/ERPG-2 concentrations (as available) or 50% of Lower Flammability Limits (LFL) does not extend beyond process boundary (operating unit) at grade or platform levels, or small flammable release not entering a potential explosion site (congested/confined area) due to the limited amount of material released or location of release (e.g., flare stack discharge where pilot failed to ignite discharged vapors).

B: AEGL-2/ERPG-2 concentrations (as available) extend beyond unit boundary but do not extend beyond property boundary. Flammable vapors greater than 50% of LFL at grade may extend beyond unit boundaries but did not entering a potential explosion site (congested/confined area); therefore, very little chance of resulting in a VCE.

C: AEGL-2/ERPG-2 concentrations (as available) exceeded off-site OR flammable release resulting in a vapor cloud entering a building or potential explosion site (congested/confined area) with potential for VCE resulting in fewer than 5 casualties (i.e., people or occupied buildings within the immediate vicinity) if ignited.

D: AEGL-3/ERPG-3 concentrations (as available) exceeded off-site over the defined 10/30/60 minute time frame OR flammable release resulting in a vapor cloud entering a building or potential explosion site (congested/confined area) with potential for VCE resulting in greater than 5 casualties (i.e., people or occupied buildings within the immediate vicinity) if ignited.

NOTE 3: The Potential Chemical Impact table reflects the recommended criteria. However, some companies may object to making a relative ranking estimate on the potential impact using the terms described. In those situations, it would be acceptable for those companies to substitute the following criteria corporate wide: Severity Level 4: 1X to 3X the TQ for that chemical, Level 3: 3X to 9X, Level 2: 9X to 20X, and Level 1: 20X or greater the TQ for that chemical. However, if a company elects to use this alternative approach they should be consistent and use this approach for all releases. They should not select between the two methods on a case-by-case basis simply to get the lowest severity score.

NOTE 4: The category labels can be modified by individual companies or industry associations to align with the severity order of other metrics. It is important is to use the same severity point assignments shown.

NOTE 5: The severity index calculations include a category for “Community/Environmental” impact and a first aid (i.e., OSHA “recordable injury”) level of Safety/Human Health impact which are not included in the PSI threshold criteria. However, the purpose of including both of these values is to achieve greater differentiation of severity points for incidents that result in any form or injury, community, or environmental impacts.

GLOSSARY

Accident—An unplanned event or sequence of events that results in an undesirable consequence.

Accidental Chemical Release—An unintended, sudden release of chemical(s) from manufacturing, processing, handling, or on-site storage facilities to the air, water, or land.

Action Tracking—A method of logging progress when implementing a task or set of tasks.

Ad Hoc Investigation—An incident investigation fashioned from the immediately available information and concerns. Typically, the ad hoc investigation is performed whenever there are no prior investigation procedures. A synonym to ad hoc is *unsystematic*.

Amelioration—Improvement of conditions immediately after an accident; treatment of injuries and conditions that endanger people and property.

Anomaly—An unusual, abnormal, or irregular set of circumstances that, left unrecognized or uncorrected, may result in an incident.

Assumed Risk—A risk that has been identified, analyzed, and accepted at the appropriate management level. Unanalyzed or unknown risks fall under oversight and omissions by default.

Audit Trail—The proof that systematic documentation of activities was performed in a way that allows an auditor to confirm compliance with required or desired organizational behavior.

Catastrophic—A loss with major consequences and unacceptable lasting effects, usually involving significant harm to humans, substantial damage to the environment, and/or loss of community trust with possible loss of franchise to operate.

Catastrophic incident—An incident involving a major uncontrolled emission, fire or explosion that causes significant damage, injuries and/or fatalities onsite and has an outcome effect zone that extends into the surrounding community.

Causal Factor—A major unplanned, unintended contributor to an incident (a negative event or undesirable condition), that if eliminated would have either prevented the occurrence of the incident, or reduced its severity or frequency. (Also known as a critical causal factor or contributing cause.)

Cause—An event, situation, condition that results, or could result, directly or indirectly in an accident or incident.

Chemical Process Quantitative Risk Assessment (CPQRA or QRA)—The quantitative evaluation of expected risk from potential incident scenarios. It examines both consequences and frequencies, and how they combine into an overall measure of risk. The CPQRA process is always preceded by a qualitative systematic identification of process hazards. The CPQRA results may be used to make decisions, particularly when mitigation of risk is considered.

Common Cause or Common Mode Failure—Failure, which is the result of one or more events, causing coincident failures in multiple systems or on two or more separate channels in a multiple channel system, leading to system failure. The source of the common cause failure may be either internal or external to the systems affected. Common cause failure can involve the initiating event and one or more safeguards, or the interaction of several safeguards.

Consequence—The undesirable result of a loss event, usually measured in health and safety effects, environmental impacts, loss of property, and business interruption costs.

Consequence Analysis—The analysis of the expected effects of incident outcome cases, independent of frequency or probability.

Deductive Approach—Reasoning from the general to the specific. By postulating that a system or process has failed in a certain way, an attempt is made to determine what modes of system, component, operator, or organizational behavior contributed to the failure.

Enabling Event—An event that makes another event possible. Sometimes used for enabling condition. The term enabling condition is preferred, since enabling conditions are not generally events but rather conditional states.

Episodic Event—An unplanned event of limited duration.

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

Evidence—Data on which the investigation team will rely for subsequent analysis, testing, reconstruction, corroboration, and conclusions.

Evidence gathering—The collection of data on which the investigation team will rely for subsequent analysis, testing, reconstruction, corroboration, and conclusions.

Failure—An unacceptable difference between expected and observed performance.

Failure Mode and Effects Analysis (FMEA)—A hazard identification technique in which all known failure modes of components or features of a system are considered in turn and undesired outcomes are noted.

Falsifiability—A concept where a specific effort is made to disprove a speculated hypothesis, in addition to the efforts made to prove the hypothesis.

Fault Tree—A logic model that graphically portrays the combinations of failures that can lead to a specific main failure or incident of interest.

Fault Tree Analysis—A method used to analyze graphically the failure logic of a given event, to identify various failure scenarios (called cut-sets), and to support the probabilistic estimation of the frequency of the event.

Forensic Engineering—The art and science of professional practice of those qualified to serve as engineering experts in matters before the courts of law or in arbitration proceedings.

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

Hazard—An inherent chemical or physical characteristic that has the potential for causing damage to people, property, or the environment.

Hazard and Operability Study (HAZOP)—A systematic qualitative technique to identify process hazards and potential operating problems using a series of guide words to study process deviations. A HAZOP is used to question every part of a process to discover what deviations from the intention of the design can occur and what their causes and consequences may be. This is done systematically by applying suitable guide words. This is a systematic detailed review technique, for both batch and continuous plants, which can be applied to new or existing processes to identify hazards.

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 and Risk Analysis (HIRA) — A collective term that encompasses all activities involved in identifying hazards and evaluating risk at facilities, throughout their life cycle, to make certain that risks to employees, the public, or the environment are consistently controlled within the organization's risk tolerance.

High Potential Incident—An event that, under different circumstances, might easily have resulted in a catastrophic loss.

Historic Incident Data—Data collected and recorded from past incidents.

Human Error—Intended or unintended human action or inaction that produces an inappropriate result. Includes actions by designers, operators, engineers, or managers that may contribute to or result in accidents.

Human Factors—A discipline concerned with designing machines, operations, and work environments so that they match human capabilities, limitations, and needs. Includes any technical work (engineering, procedure writing, worker training, worker selection, etc.) related to the human factor in operator-machine systems.

Human Reliability Analysis—A method used to evaluate whether system-required human-actions, tasks, or jobs will be completed successfully within a required time period. Also used to determine the probability that no extraneous human actions detrimental to the system will be performed.

Hypothesis—A supposition or proposed explanation made on the basis of limited evidence as a starting point for further investigation.

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 unusual, unplanned, or unexpected occurrence that either resulted in, or had the potential to result in a process upset with potential process condition excursions beyond operating limits, release of energy or materials, challenges to a protective barrier, or loss of stakeholder confidence in a company's reputation.

Incident Investigation—A systematic approach for determining the causes of an incident and developing recommendations that address the causes

to help prevent or mitigate future incidents. See also Root cause analysis and Apparent cause analysis.

Incident Investigation Management System—A written document that defines the roles, responsibilities, protocols, and specific activities to be carried out by personnel performing an incident investigation.

Incident Investigation Team—A group of qualified people who examine an incident in a manner that is timely, objective, systematic, and technically sound to determine that factual information pertaining to the event is documented, probable cause(s) are ascertained, and complete technical understanding of such an event is achieved.

Inductive Approach—Reasoning from individual cases to a general conclusion by postulating that a system element has failed in a certain way. An attempt is then made to find out what happens to the whole system or process.

Initiating Event—The minimum combination of failures or errors necessary to start the propagation of an incident sequence. It can be comprised of a single initiating cause, multiple causes, or initiating causes in the presence of enabling conditions. (The term initiating event is the usual term employed in Layer of Protection Analysis to denote an initiating cause or, where appropriate, an aggregation of initiating causes with the same immediate effect, such as "BPCS failure resulting in high reactant flow".

Injury—Physical harm or damage to a person resulting from traumatic contact between the body and an outside agency or exposure to environmental factors.

Job Safety Analysis (JSA)—A procedure that systematically identifies: (1) job steps, (2) specific hazards associated with each job step, and (3) safe job procedures associated with each step to minimize accident potential. Also called job hazard analysis.

Kaizen—A quality system using lessons learned.

Latent Failure—Failure in a component because of a hidden flaw.

Layer of Protection Analysis (LOPA)—An approach that analyzes one incident scenario (cause-consequence pair) at a time, using predefined values for the initiating event frequency, independent protection layer failure probabilities, and consequence severity, in order to compare a scenario risk estimate to risk criteria 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.

Lessons Learned—Applying knowledge gained from past incidents in current practices.

Likelihood—A measure of the expected probability or frequency of occurrence of an event. This may be expressed as an event frequency (e.g., events per year), a probability of occurrence during a time interval (e.g., annual probability) or a conditional probability (e.g., probability of occurrence, given that a precursor event has occurred).

Limited impact incidents—Incidents deemed to be controllable with local resources and which have no lasting effects.

Lockout/Tagout—A safe work practice in which energy sources are positively blocked away from a segment of a process with a locking mechanism and visibly tagged as such to help ensure worker safety during maintenance and some operations tasks.

Management of Change (MOC)—A management system to identify, review, and approve all modifications to equipment, procedures, raw materials, and processing conditions, other than replacement in kind, prior to implementation to help ensure that changes to processes are properly analyzed (for example, for potential adverse impacts), documented, and communicated to employees affected.

Management System—A formally established set of activities designed to produce specific results in a consistent manner on a sustainable basis.

Medical Treatment—As defined by OSHA, treatment (other than first aid) administered by a physician or by registered professional personnel under the standing orders of a physician.

Methodology—The use of a combination of two or more incident investigation tools to analyze the evidence and determine the root causes of the incident.

Minor incidents—Incidents with minor actual or potential consequences, including minor injuries and minor damage.

Mitigation—Lessening the risk of an accident event sequence by acting on the source in a preventive way by reducing the likelihood of occurrence of the event, or in a protective way by reducing the magnitude of the event and/or the exposure of local persons or property.

Morphological Approach—A structured analysis of an incident directed by insights from historic case studies but not as rigorous as a formal hazard analysis.

Near Miss—An incident in which an adverse consequence could potentially have resulted if circumstances (weather conditions, process safeguard response, adherence to procedure, etc.) had been slightly different.

Occupational Incident—An incident involving injury to workers.

Operational Interruption—An event in which production rates or product quality is seriously impacted.

Organizational Error—A latent management system problem that can result in human error.

OSHA Recordable Cases—Work-related deaths, injuries, and illnesses (other than minor injuries requiring only first aid treatment) which involve medical treatment, loss of consciousness, restriction of work or motion, or transfer to another job.

OSHA Reportable Event—An incident that causes any fatality or the hospitalization of five employees or more requires a notification report to the nearest OSHA office.

PF_D—Probability of failure on demand. The probability that a system will fail to perform a specified function on demand.

Prevention—The process of eliminating or preventing the hazards or risks associated with a particular activity. Prevention is sometimes used to describe actions taken in advance to reduce the likelihood of an undesired event.

Probability—The expression for the likelihood of occurrence of an event or an event sequence during an interval of time, or the likelihood of the success or failure of an event on test or on demand. Probability is expressed as a dimensionless number ranging from 0 to 1.

Process Control System—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.

Process Hazard Analysis—Also known as a Hazard Risk and Identification Analysis (CCPS 2014). An organized effort to identify and evaluate hazards associated with processes and operations to enable their control. This review normally involves the use of qualitative techniques

to identify and assess the significance of hazards. Conclusions and appropriate recommendations are developed. Occasionally, quantitative methods are used to help prioritize risk reduction.

Process Safety—A disciplined framework for managing the integrity of operating systems and processes handling hazardous substances by applying good design principles, engineering, and operating practices. It deals with the prevention and control of incidents that have the potential to release hazardous materials or energy. Such incidents can cause toxic effects, fire, or explosion and could ultimately result in serious injuries, property damage, lost production, and environmental impact.

Process Safety Management—A management system that is focused on prevention of, preparedness for, mitigation of, response to, and restoration from catastrophic releases of chemicals or energy from a process associated with a facility.

Process-Related Incident—An incident with impact, or potential impact, on process, equipment, people, and the environment. The incident could be internal or external to the process. An occupational incident can result from a process-related incident.

Protection Layer—A device, system, or action that is capable of preventing a scenario from proceeding to the undesired consequence without being adversely affected by the initiating event or the action of any other protection layer associated with the scenario.

Proximate Cause—The causal factor that directly produces the effect without the intervention of any other cause. The cause nearest to the effect in time and space.

Risk—A measure of human injury, environmental damage, or economic loss in terms of both the incident likelihood and the magnitude of the loss or injury. A simplified version of this relationship expresses risk as the product of the likelihood and the consequences (i.e., $\text{Risk} = \text{Consequence} \times \text{Likelihood}$) of an incident.

Risk Analysis—The estimation of scenario, process, facility and/or organizational risk by identifying potential incident scenarios, then evaluating and combining the expected frequency and impact of each scenario having a consequence of concern, then summing the scenario risks if necessary to obtain the total risk estimate for the level at which the risk analysis is being performed.

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, while avoiding business interruptions. Includes decisions to use suitable engineering and administrative controls for reducing risk.

Risk Ranking—A decision making aid that ranks items, such as scenarios or proposed recommendations, in order of their potential associated risk exposure.

Root Cause—A fundamental, underlying, system-related reason why an incident occurred that identifies a correctable failure(s) in management systems. There is typically more than one root cause for every process safety incident

Safeguard—Any device, system, or action that either interrupts the chain of events following an initiating event or that mitigates the consequences. A safeguard can be an engineered system or an administrative control. Not all safeguards meet the requirements of an IPL.

Safety—The expectation that a system does not, under defined conditions, lead to a state in which human life, economics or environment are endangered.

Safety Critical Actions—Specific steps humans take that provide layers of protection to lower the risk category of a specific scenario or scenarios from “unacceptable” to “acceptable” as defined by organizational risk tolerance criteria. Sometimes called *administrative control*. Such steps that further reduce the risk below “acceptable” might not be designated as safety critical actions.

Safety Critical Equipment—Engineering controls that provide layers of protection to lower the risk category of a specific scenario or scenarios from “unacceptable” to “acceptable” as defined by organizational risk tolerance criteria. Engineering controls that further reduce the risk below “acceptable” might not be designated as safety critical equipment.

Scenario—A detailed description of 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.

Scientific Method—Principles and procedures for the systematic pursuit of knowledge involving the recognition and formulation of a problem, the collection of data through observation and experiment, and the formulation and testing of hypotheses

Sensor—Field measurement system (instrumentation) capable of detecting the condition of a process (for example, pressure transmitters; level transmitters, and toxic gas detectors).

Serious Injury—The classification for an occupational injury which includes: (a) all disabling work injuries and (b) non-disabling work injuries as follows: (1) eye injuries requiring treatment by a physician, (2) fractures, (3) injuries requiring hospitalization, (4) loss of consciousness, (5) injuries requiring treatment by a doctor and (6) injuries requiring restriction of motion or work, or assignment to another job.

Significant incidents—Incidents that have, or would have in the case of near-misses, consequences requiring considerable resources to mitigate and usually involve human injuries and/or major interruptions to operations.

Software—Programs, procedures, rules, and associated documentation required for the operating and/or maintenance of a digital system. Computer programs, routines, programming Languages and systems. The collection of related utility, assembly, and other programs that are desirable for properly presenting a given machine to a user. Including; detailed procedures to be followed, whether expressed as programs for a computer or as procedures for an operator or other person, documents, including hardware manuals and drawings, computer program listing, and diagrams, etc., and items such as those listed above, as contrasted with hardware.

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.

Taxonomy—The practice and science (study) of classification of things or concepts, including the principles that underlie such classification.

Technique—A way of carrying out a particular task.

Tool—A device or means used at a discrete stage of the incident investigation to facilitate understanding of event chronology, causal factors, or root causes.

Underlying Causes—Actual root causes.

Validation—The action of checking or proving the validity or accuracy of something.

Verification—The activity of demonstrating by analysis or test, that, for the specific inputs, the deliverables meet, in all respects, the objectives and requirements set forth by the functional specification.

Witness—A person who has facts related, directly or indirectly, to the incident.

REFERENCES

Note: These references and associated internet websites (if applicable) were current at the time they were accessed during this guideline's preparation (2017-2018).

1. ABS Consulting (1999). *Root Cause Analysis Handbook: A guide to effective Incident Investigation*. Knoxville, TN: ABS Group Inc.
2. ABS Consulting (2000). *Introduction to Reliability Management: An Overview*. Knoxville, TN: ABS Group Inc.
3. ABS Consulting (2001). *Incident Investigation/Root Cause Analysis Training: Results Trending and Assessment*. Knoxville, TN: ABS Consulting.
4. ACC (1990). American Chemistry Council. *Responsible Care® , A Resource Guide for the Process Safety Code of Management Practices*. Washington, DC.
5. ACC (2014). *Performance Metrics Guidance Document*, American Chemistry Council, Washington D.C.
6. American Chemistry Council (ACC), *Responsible Care® Process Safety Code of Management Practices*, 2012.
7. Adams, Kathy B. (1999). *Accident Investigation Reports: What Are Your Lawyers Afraid Of?* Presentation for American Society of Safety Engineers Conference. Baltimore, Maryland. June 14.
8. ACC (1990). American Chemistry Council. *Responsible Care® , A Resource Guide for the Process Safety Code of Management Practices*. Washington, DC: 1990.
9. ACC (2000). American Chemical Council. *Responsible Care® , Process Safety Code*. Arlington, Virginia.
10. AIChE/GCPS (2018). Forest, J., "Don't Walk the Line – Dance it!," American Institute of Chemical Engineers 2018 Spring Meeting and 14th Global Congress on Process Safety, April 22-25, 2018.
11. Amyotte, P. et al, "CSB Investigation Reports and the Hierarchy of Controls: Round 2," Presentation Paper at 14th Global Congress on Process Safety, 2018.
12. Anderson, S. E., and Skloss, R. W. (1991). "More Bang for the Buck: Getting the Most from an Accident Investigation." Paper, *Loss Prevention Symposium*. New York: AIChE.
13. American Petroleum Institute (API). Recommended Practice API 9100, Model Environmental, Health & Safety (EHS) Management System and Guidance Document.
14. API (2014). *Pressure Equipment Integrity Incident Investigation*, Recommended

- Practice 585 (API RP 585), 1st edition, American Petroleum Institute, Washington D.C.
15. API (2016a). *Process Safety Performance Indicators for the Refining & Petrochemical Industries, Part 2: Tier 1 and 2 Process Safety Events*, Recommended Practice 754, 2nd edition, American Petroleum Institute, Washington D.C.
 16. API (2016b). *Guide to Reporting Process Safety Events*, Version 3.0, American Petroleum Institute, Washington D.C., 2016.
 17. API RP 754, *Process Safety Performance Indicators for the Refining and Petrochemical Industries*, 2017.
 18. Arendt, J. S. (1991). "A Chemical Plant Accident Investigation Using Fault Tree Analysis." *Proceedings of 17th Annual Loss Prevention Symposium*. Paper 11a, New York: AIChE.
 19. ASCE, *Design of Blast-Resistant Buildings in Petrochemical Facilities, Second Edition*, ISBN 9780784410882, 2010.
 20. ASCE, *Structural Design for Physical Security*, ISBN 9780784404577, 1999.
 21. ASSE (1988). American Society of Safety Engineers, *Dictionary of Terms Used in the Safety Profession*, 3rd ed, Des Plaines, IA.
 22. Baker, W.E. et al. *Explosion Hazard and Evaluation*. New York: Elsevier Scientific, 1983.
 23. BARPI, Research and Information on Accidents (ARIA) database, The Bureau for Analysis of Industrial Risks and Pollutions (BARPI), an Analysis — a searchable database of incidents and other reference material—(accessed August 2018): <https://www.aria.developpement-durable.gouv.fr/?lang=en>
 24. Benner, L. Jr. (1975). "Accident Investigations: Multilinear Events Sequencing Methods." *Journal of Safety Research*, 7(2):67–73.
 25. Benner, L., Jr. (2000). *10 MES Investigation Guides*. Oakton, VA: Starline Software Ltd.
 26. Bird, F. E., Jr., and Germain, G. L. (1985). *Practical Loss Control Leadership*. Loganville, GA: International Loss Control Institute (ILCI).
 27. Boissieras, J. (1983). *Causal Tree, Description of the Method*. Princeton, NJ: Rhone-Poulenc.
 28. BP (formerly BP Amoco) (1999). *Incident Investigation. Root Cause Analysis Training. Comprehensive List of Causes*. London.
 29. Bridges, W. G. (2000). "Get Near Misses Reported," *Proceedings of the International Conference and Workshop on Process Industry Incidents, Orlando, FL*. New York: Center for Chemical Process Safety (CCPS), AIChE, October.
 30. Browning, R. L. (1975). "Analyze Losses by Diagram." *Hydrocarbon Processing*, **54**:253–257.
 31. Buys, R. J. (1977). *Standardization Guide for Construction and Use of MORT-Type Analytical Trees*. Idaho Falls, ID: System Safety Development Center. Idaho

- National Engineering Laboratory. (ERDA 76-45/8)
32. Buys, R. J., and Clark, J. L. (1978). *"Events and Causal Factors Charting."* Revision 1, Idaho Falls, ID: System Safety Development Center, Idaho National Engineering Laboratory. (DOE 76-45/14 SSDC-14)
 33. CAA, UK (2014). *Flight-crew human factors handbook*, CAP 737, Civil Aviation Authority, UK.
 34. Carper, K. (1989). *Forensic Engineering*. New York: Elsevier.
 35. Center for Chemical Process Safety (1989). *Guidelines for Technical Management of Chemical Process Safety*, (CCPS), New York: American Institute of Chemical Engineers.
 36. Center for Chemical Process Safety (1992). Center for Chemical Process Safety. *Guidelines for Hazard Evaluation Procedures, Second Edition with Worked Examples*. New York: American Institute of Chemical Engineers (AIChE).
 37. Center for Chemical Process Safety (2000). *Guidelines for Chemical Process Quantitative Risk Analysis, 2nd Edition*, New York, NY, 2000.
 38. Center for Chemical Process Safety (2001). *Layer of Protection Analysis, Simplified Process Risk Assessment*. New York: American Institute of Chemical Engineers, 2001.
 39. Center for Chemical Process Safety (2008), *Guidelines for Hazard Evaluation Procedures, 3rd Edition with Worked Examples*. New York, NY, 2008.
 40. Center for Chemical Process Safety (2008). Guidelines for Hazard Evaluation Procedures, 3rd edition, AIChE, New York, 2008
 41. Center for Chemical Process Safety (2007). *Human Factors Methods for Improving Performance in the Process Industries* (NY: AIChE Center for Chemical Process Safety).
 42. Center for Chemical Process Safety (2007a). *Guidelines for Risk Based Process Safety*. Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, 2007.
 43. Center for Chemical Process Safety (2007b). *Inherently Safer Chemical Processes, A Life Cycle Approach*, 2nd edition, (CCPS), American Institute of Chemical Engineers (AIChE), New York, 2007.
 44. Center for Chemical Process Safety (2010). Guidelines for Vapor Cloud Explosion, Pressure Vessel Burst, BLEVE and Flash Fire Hazards, 2nd Edition, ISBN 978-0-470-25147-8, Wiley, 2010.
 45. Center for Chemical Process Safety (2011). *Conduct of Operations and Operational Discipline for Improving Process Safety in Industry* (NY: AIChE Center for Chemical Process Safety), 2011.
 46. Center for Chemical Process Safety (2011), *Process Safety Leading and Lagging Metrics*, January 2011.
 47. Center for Chemical Process Safety (2012). *Guidelines for Evaluating Process Plant Buildings for External Explosions and Fires*, (CCPS), ISBN 978-0-470-64367-9, Wiley, 2012.

48. Center for Chemical Process Safety (2011). *Process Safety Leading and Lagging Metrics, ... You don't improve what you don't measure*, (CCPS), American Institute of Chemical Engineers (AIChE), New York, NY, 2011.
49. Center for Chemical Process Safety website, (CCPS), viewed August 2018, <https://www.aiche.org/ccps/resources/tools/process-safety-metrics>
50. Center for Chemical Process Safety (2018). *Bow Ties in Risk Management: A Concept Book for Process Safety*, Center for Chemical Process Safety, ISBN 1119490391, 9781119490395, Wiley, 2018.
51. Center for Chemical Process Safety (2018). *"Process Safety Metrics; Guide for Selecting Leading and Lagging Indicators"*, CCPS, 2018.
52. Center for Chemical Process Safety website, (accessed August, 2018): <https://www.aiche.org/ccps/resources/glossary/process-safety-glossary/human-factors>
53. Center for Chemical Process Safety, The Process Safety Beacon, produced by CCPS, <http://www.sache.org/beacon/products.asp>, accessed August 2018.
54. Center for Chemical Process Safety, Process Safety Incident Database (PSID), produced by CCPS, accessed August 2018. <https://www.aiche.org/ccps/resources/psid-process-safety-incident-database>
55. CEFIC (2016). *CEFIC Guidance for Reporting on the ICCA Globally Harmonised Process Safety Metric*, European Chemical Industry Council, Brussels, Belgium.
56. COMAH (2015). *The Control of Major Accident Hazards Regulations (COMAH)*, 2015.
57. CSB, Reports and videos on major incidents, U.S. Chemical Safety Board, accessed August 2018. <https://www.csb.gov/investigations/completed-investigations/>
58. CSB, Safety Digest, US Chemical Safety and Hazard Investigation Board, <https://www.csb.gov/news/>, accessed August 2018-1
59. CSB, Videos, <https://www.csb.gov/videos/>, accessed August 2018-2
60. DoE (1985). Department of Energy, *Accident/Incident Investigation Manual*. 2nd ed., Idaho Falls, ID: System Safety Development Center. Idaho National Engineering Laboratory. (DOE/SSDC 76-45/27)
61. Dew, J. R. (1991). "In Search of the Root Cause." *Quality Progress*. **23**(3): 97–102.
62. Dowell, A. M. (1990). *Guidelines for Systems Oriented Multiple Cause Incident Investigations*. Deer Park, TX: Rohm and Haas Texas Inc. Risk Analysis Department.
63. Driessen, G.J., 1970: "Cause Tree Analysis, Measuring How Accidents Happen and the Probabilities of Their Cause". Presented to American Psychological Association, September, 1970, Miami, FL
64. EI (2016). *Learning from Incidents, Accidents and Events*, Energy Institute, London, August 2016.
65. eMARS, A searchable database of incidents in the EU. European Commission

- Major Accident Reporting System, accessed August 2018.
<https://emars.jrc.ec.europa.eu/en/emars/accident/search>
66. <https://ec.europa.eu/jrc/en/scientific-tool/major-accident-reporting-system>
 67. Englund, S. M. (1991). "Design and Operate Plants for Inherent Safety" *Chemical Engineering Progress*, Part 1, March 1991; Part 2 May 1991.
 68. EPA, "EPA/OSHA Joint Chemical Accident Investigation Report, Shell Chemical Company, Deer Park, Texas," US EPA document # 550-R-98-005, 1998
 69. EPSC, "Learning sheet," produced by the European Process Safety Centre, <http://epsc.be/Learning+Sheets.html>, accessed August 2018.
 70. Evans, Ralph A., "Engineering Design Handbook Design for Reliability", US Army Materiel Command. AMCP-706-196. January 1976.
 71. Ferry, T.S. (1988). *Modern Accident Investigation, and Analysis* 2nd ed. New York: John Wiley & Sons.
 72. Feyman, R. P. *What Do You Care What Other People Think?* New York: Norton, 1988.
 73. Foord, A. G. (2004). "Applying the Latest Standard for Functional Safety – IEC 61511," IChemE Hazards XVIII, Paper 23.
 74. Ford, D. F. *Three Mile Island, Thirty Minutes to Meltdown*. New York: Penguin Books, 1981.
 75. Forest, J. (2018). "Don't Walk the Line – Dance it!," American Institute of Chemical Engineers 2018 Spring Meeting and 14th Global Congress on Process Safety, April 22-25, 2018.
 76. Gano, D, (2008). "Apollo Root Cause Analysis," 3rd Edition, ISBN-13: 978-1883677114, Apollonian Publications.
 77. Gibson, J.J. (1961). *Contribution of experimental psychology to formulation of problem of safety, Behavioural Approaches to Accident Research*, Association for the Aid of Crippled Children.
 78. Haddon, W. (1980). *The Basic Strategies for Reducing Damage from Hazards of All Kinds*, Hazard Prevention, Sept/Oct, 1980.
 79. Hendrick, K. and Benner, L., Jr. (1987). "Investigating Accidents with S-T-E-P." New York: Marcel Dekker.
 80. Heinrich, H.W. (1936). *Industrial Accident Prevention*. New York: McGraw-Hill.
 81. HSE, UK (1999). *Reducing Error and Influencing Behaviour*, Health and Safety Executive, Report No. HSG48, ISBN 0 7176 2452 8, HSE Book, Sudbury, UK.
 82. HSE (2001). *Root Causes Analysis: Literature Review*, Contract Research Report 325/2001, Health and Safety Executive, Bootle, UK.
 83. HSE (2004). *Investigating accidents and incidents, A workbook for employers, unions, safety representatives and safety professionals*, HSG245, UK Health & Safety Executive, Bootle, UK.
 84. HSE (UK), HSG254, Developing Process Safety Indicators, 2006.
 85. Health and Safety Executive (HSE), Guide 65: Managing for Health and Safety,

- 2013.
86. HSE, A series of reports on major incidents, Health and Safety Executive UK, <http://www.hse.gov.uk/comah/investigation-reports.htm>, accessed August 2018
 87. HSG245 (2004). "Investigating incidents and accidents." (Accessed August 2018): <http://www.hse.gov.uk/pubns/books/hsg245.htm>
 88. HM Government (2013). *Reporting of Injuries, Diseases and Dangerous Occurrences Regulations*, UK.
 89. ICCA (2016). *Guidance for Reporting on the ICCA Globally Harmonized Process Safety Metric*, The Responsible Care® Leadership Group, International Council of Chemical Associations, Brussels, Belgium.
 90. IChemE, "Loss Prevention Bulletin," produced by the IChemE in the UK, <http://www.icheme.org/lpb>, accessed August 2018-1.
 91. IChemE, "Safety Lore," produced by the IChemE Safety Centre in the UK, <http://www.ichemesafetycentre.org/resources/safety-lore.aspx>, accessed August 2018-2.
 92. IChemE, "Why do we keep repeating major accidents," Loss Prevention Bulletin 259, February 2018.
 93. ILCI (1990). *SCAT—Systematic Cause Analysis Technique*. International Loss Control Institute, Loganville, GA: Det Norske Veritas.
 94. International Organization for Standardization (ISO), ISO 9000 series, *Quality Management Systems*
 95. International Organization for Standardization (ISO), ISO 14000, *Environmental Management System*
 96. IOGP, UK (2005). *Human Factors* (London, UK: International Association of Oil and Gas Producers, IOGP Report 368, <https://www.iogp.org/bookstore/product/human-factors-a-means-of-improving-hse-performance>).
 97. IOGP (2011). *Process Safety – Recommended Practice on Key Performance Indicators*, IOGP Report 456, International Association of Oil & Gas Producers, London, UK.
 98. Johnson, W. G. (1980). *MORT, Safety Assurances Systems*. New York: Marcel Dekker.
 99. Kepner, C. H., and Tregoe, B. B. (1976). *The Rational Manager*, 2nd ed. Princeton, NJ: Kepner-Tregoe, Inc.
 100. Kidama, K., & Hurmea, M., (2013). *Analysis of equipment failures as contributors to chemical process accidents*, Process Safety and Environmental Protection, 91, (2013), 61–78.
 101. Kletz, T. A. "Make Plants Inherently Safe" *Hydrocarbon Processing Magazine*. Houston, TX: Gulf Publishing Company, September 1985.
 102. Kletz, T. A. (1988). *Learning from Accidents in Industry*, Boston-London:

- Butterworths Publishers.
103. Kletz, "The ICI Safety Newsletters," mainly issued by Trevor Kletz, <http://www.icheme.org/communities/special-interest/groups/safety%20and%20loss%20prevention/resources/ici%20newsletters.aspx>, accessed August 2018.
 104. Kuhlman, R. *Professional Accident Investigation*. Loganville, GA: Institute Press, International Loss Control Institute., 1977.
 105. Laborde, G. Z. (1984). *Influencing with Integrity Management Skills for Communications and Negotiation*. Palo Alto, CA: Syntony Publishing Co. Pp. 92–106.
 106. Lees, F. P. *Loss Prevention in the Process Industries*. Vol. 1. London: Butterworths, 1980.
 107. Leplat, J. (1978). "Accident Analyses and Work Analyses." *Journal of Occupational Accidents*. 1: 331–340, 1978.
 108. Livingston, A.D., Jackson, G., Priestley, K., (2001). "Root cause analysis: Literature review," HSE Contract Research Report 325, Her Majesty's Stationery Office, St. Clements House, 2-16 Colegate, Norwich NR3 1BQ, UK.
 109. Mannan, S., *Lees' Loss Prevention in the Process Industries, 4th Edition*, Butterworth-Heinemann, 2012.
 110. Merrifield, R. "Report on the Peterborough Explosion, Blast Damage and Injuries," HSE, H M Explosives Directorate, 24th Explosive Safety Seminar, 1990
 111. Mosleh, A. et al. (1988). *Procedures for Treating Common Cause Failures in Safety and Reliability Studies*. Palo Alto, CA: Electric Power Research Institute. 1988. (EPRI NP-5613)
 112. Nelms, Robert, C. (1996). *The Go Book*. C. Robert Nelms publisher, ISBN 978-1886118201.
 113. NFPA (2017). "Guide for Fire and Explosion Investigations," National Fire Protection Association, NFPA 921, Quincy, MA.
 114. Norman, D. A. (1988). *The Design of Everyday Things*. London: MIT Papers. (Also published under the title *The Psychology of Everyday Things*.)
 115. Kuhlman, R. (1977). *Professional Accident Investigation*. Loganville, GA: Institute Press, International Loss Control Institute.
 116. Okes, D., *Root Cause Analysis*, American Society for Quality, Milwaukee, WI, 2009.
 117. Paradies, M. (1991). "Root Cause Analysis and Human Factors." *Human Factors Bulletin*. 34(8): 1–5.
 118. Paradies, M., and Unger, L, (2016). "Using TapRoot[®] Root Cause Analysis for Major Investigations," © Copyright 2016 by System Improvements, Inc.
 119. Peterson, D. (1984). *Human-Error Reduction and Safety Management*. Goshen, NY: Aloray Inc. Professional & Academic Publisher.
 120. Pieterse, C.M., "Mexico City LPG Terminal Disaster," TNO Report, 1985.

121. Rasmussen (1983). *Skills, Rules, and Knowledge; Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models*, Jens Rasmussen (IEEE Transactions on Systems, Man, and Cybernetics, Vol.smc-1 3, May 1983).
122. Reason, J. (1990). *Human Error*. New York: Cambridge University Press.
123. Reason, James (1990). "The Contribution of Latent Human Failures to the Breakdown of Complex Systems". *Philosophical Transactions of the Royal Society of London. Series B, Biological Sciences*, **327** (1241): 475–484. (1990-04-12)
124. Recht, I.L. (1965-66). "System Safety Analysis - A Modern Approach to Safety Problems," *National Safety News*, December, February, April, June, 1965-66.
125. Rogers, N.P., et al., "Space Shuttle Challenger Accident," Presidential Commission report, Washington, DC, June 6, 1986
126. Rothblum, A., et al (2002). "Human Factors in Incident Investigation and Analysis." 2nd International Workshop on Human Factors in Offshore Operations
127. RSSB, "Accident investigation guidance part 3," Rail Safety and Standards Board, UK, 2014
128. Stephens, M. M. *Minimizing Damage to Refineries*. Washington DC: U.S. Department of Interior, Office of Oil and Gas, 1970.
129. Toft, B, Turner, BA, (1987). "The Schematic Report Analysis Diagram: a simple aid to learning from large scale failures," *International CIS Journal*, v1n2, pp 12-23.
130. Trost, W. A., and Nertney, R. J. (1985). "Barrier Analysis." Idaho Falls, ID: System Safety Development Center. Idaho National Engineering Laboratory. (DOE/SSDC 76-45/29)
131. US Department of Energy (1985). *Accident/Incident Investigation Manual*, Second Edition. Idaho Falls, ID: System Safety Development Center, Idaho National Engineering Laboratory 1985. (DOE/SSDC 76-45/27)
132. US EPA. Accidental Release Prevention Requirements: Risk Management Programs. *Clean Air Act Section 112(r)(7). 40 CFR Part 68*, Washington, DC: Environmental Protection Agency, 2004.
133. US OSHA. "Process Safety Management of Highly Hazardous Chemicals" *29 CFR 1910.119*. Washington, DC: Occupational Safety and Health Administration, 1992.
134. US OSHA (2002) 29 CFR 1904, *Recording and Reporting Occupational Injuries and Illnesses*. Effective January 1, 2002; US OSHA website for recordkeeping revisions (accessed August 2018): <http://www.osha.gov/recordkeeping/index.html>
135. Vaughan, D. *The Challenger Launch Decision*. Chicago: University of Chicago Press, 1996.
136. Vesely, W.E. et al. (1981). "Fault Tree Handbook." Washington, DC: US Government Printing Office. (NUREG-0492)
137. Waldram, L, (1988). *Systematic Accident Cause Analysis (SACA)*.

138. Weaver, DA. (1973). "TOR Analysis: A Diagnostic Training Tool," ASSE Journal, June, pp 24-29.
139. Weir, A. "Concorde Crash Raises Questions without Answers." *Journal of System Safety*, System Safety Society. Second Quarter 2001
140. Winsor, D. A. (1989). "*Challenger*: A Case of Failure to Communicate," *Chemtech Magazine*, American Chemical Society, September.

References (Appendices)

1. API, "Pressure Equipment Integrity Incident Investigation," API Recommended Practice 585, First Edition, April 2014
2. Baker, Q. A., Pierorazio, A. J., Ketchum, D.E., "Investigation of Explosion Accidents," Center for Chemical Process Safety International Conference and Workshop on Process Industry Incidents, October 2000, Orlando Florida. New York: AIChE, 2000
3. Berrin, E. *Investigative Photography*. Report 83-1. Society of Fire Protection Engineers. Boston, MA: Society of Fire Protection Engineers, 1982.
4. Center for Chemical Process Safety (CCPS), 1989, *Guidelines for Technical Management of Chemical Process Safety*. New York: American Institute of Chemical Engineers. Appendix C
5. NFPA, Guide for Investigating Fires and Explosions, National Fire Protection Associate, ISBN 978-1 45591602-3, Quincy, Massachusetts, 2016

INDEX

A

accident, 3
 defined, 416
Acoustic Emission inspection, 186
AND-gate, logic trees, 41, 221–23
anomaly, 156
assumed risk, 33
attorney–client privilege, 59–62
audio recording, 120, 360
audit trail, 298, 320

B

barrier analysis, 36, 194, 195, 197, 198
Bhopal, India
 (toxic gas release), 1
blame-free policy, 70, 267
brainstorming, 27, 29, 30, 38, 44

C

case studies, 206, 317, 345, 348
catastrophic events, 1
causal category analysis, 331
causal factors, 333, 337, 346, 354
Causal Tree, 41
causation, 7, 13, 17–22
 event tree, 16
 event vs. root cause, 22
 human factors, 21
 key causation concepts, 18
 latent failures, 16
 loss of containment. *See* management system failure, 20
 multiple causation, 22
 Swiss Cheese model, 16

 three-phase model, 16

 cause, 1–4
Challenger space shuttle disaster, 71
change analysis, 36, 194, 244
checklists, 37, 44, 46
classification systems, 81, 94
commendation, 289
common cause, 319, 331
 failure, 229
communications. *See* Human Factors, Notifications
communications, legal issues, 49–55
completeness test, 244, 255
Concorde aircraft tragedy, 318
confidentiality, 60, 98, 124, 369
Consequence analysis, 151
consequences, 1, 6, 13, 14, 16, 29
continuous improvement, 73, 74, 100, 326
controlling risk, 23
cost-benefit analysis, 321
credibility, 77

D

data management systems, 74
deductive approach, 212, 216, 219
developer role, 53
dimensional measurement, 186
disciplinary action, 77, 118, 164, 289
 blame-free policy, 70
documentation
 requirements, 59

E

electronic evidence. *See* evidence identification

employee interviews. *See* *Witness management*

environmental protection
agencies, 55

Environmental protection, 54

errors
human factors, 13, 193, 244

event tree, 41, 187
model, 14

Events & Causal Factor Charting (E&CF), 33

evidence
defined, 137

evidence analysis, 178

evidence collection, 137, *See* *Witness management*

evidence gathering, 137, 142, 156

evidence identification, 76, 137

executive summary
report document, 298, 300

external notification, 58

external notifications, 52

F

fact/hypothesis matrix, 188

falsifiability, 181
defined, 418

fault tree analysis. *See also* *Logic trees*

Fault Tree Analysis (FTA), 42, 194

filtering concept, 117

findings, 134, 275, 295, 297, 298, 300

first notification, 80

Flixborough
UK explosion incident, 206

flowcharts, 274

follow-up
activities, 315
implementing recommendations, 314
management of, 306
recommendations, 280

forensic engineering
defined, 418

fractography, 186

fragile data source, 186

G

glass pieces, 154

H

hazard analysis, 322

Hazard and Operability (HAZOP)
checklist, 37, 232, 256

Hazard Barrier Target Analysis (HBTA), 197

Hazard Identification and Risk Analysis (HIRA), 54, 346, 378

HAZMAT teams, 140

HAZOP, 219, 232, 322
defined, 418

high potential incident
defined, 419

historic incident data, 13, 17
defined, 419

human error. *See* *human factors*

human factors, 261–75
errors, 14, 18, 21

human reliability analysis, 119, 258, 274

hypothesis testing, 190, 193, 202

I

incident
defined, 419

incident causation. *See* *Causation*

incident classification, 81

incident investigation, 11
best practices, 13

incident investigation management
system, 47–50
legal considerations, 60
recommendations, 71

incident investigation methodology, 46, 103

incident investigation team, 107, 112, 117, 120
inductive approach, 257
 defined, 420
inherent safety, 278, 294
 concepts, 284
 recommendations, 294
initiating event, 317
 defined, 420
Initiating event, 328
integration
 with management system, 54
intensification
 inherent safety, 284
interim report, 295, 296, 309
internal notifications, 52, 91
interviews, 29, 57, 59, *See Witness management*
investigation environment, 139
iterative loop
 logic trees, 217

J

Job Safety Analysis (JSA), 288

K

Kaizen
 defined, 420

L

latent failures, 17
layers of protection, 193, 194, 197
leadership, 47, 275
 incident investigation team, 268
leading indicators, 1
learning. *See Lessons Learned*
legal considerations, 55, 60
lessons learned, 47, 57, 324, 340
limited impact incidents
 defined, 421
lockout/tagout, 115, 142, 196, 319

logic trees, 37, 39, 86, *See Fault tree analysis*
 development, 215
 diagram, 219
 root cause determination, 214
Logic trees, 241
LOPA
 defined, 420

M

magnetic particle inspection, 165
maintenance error. *See Human factors*
Management of Change (MOC), 70, 280, 316, 321
Management Oversight and Risk Tree (MORT), 33, 198
management responsibilities, 72
management system, 20, 23, 33, 47, 74, 204, *See Incident investigation management system*
medical treatment, 52, 96, 357
memory
 witness interviews, 119
microscopic examination, 186
minor incident, 208
 defined, 421
mitigation, 20, 173, 261, 286
Multilinear Event Sequencing (MES), 31
multiple cause, 69, 174, 198, 203, 206, 212
multiple layers of protection, 285, *See Layers of protection*
Multiple-Cause, Systems-Oriented Incident Investigation (MCSOII), 44

N

near-miss, 24, 220, 247
 defined, 422
near-miss events, 334
noncontributory factors, 306

notification, 49, 52
 nuclear power plant incident, 317

O

occupational incidents, 33
 operational interruption, 3
 defined, 422
 operator error, 15, *See also Human Factors*
 organization's responsibilities
 incident investigation, 47–50
 OR-gate, 222, 223, 246
 logic trees, 219

P

paper evidence, 149, 151
 photography, 157, 158, 164–66
 guidelines, 357
 physical evidence, 2, 57, 110, 147–49
 planning, 73, 75
 position evidence, 153–56
 predefined trees, 33, 37, 38, 212
 preplanning, 2, 54, 60, 73
 prevention, 63, 192, 287, 331
 strategies, 19
 preventive action, 314, 316, 319
 priority determination, 321
 process control system, 152, 169, 187
 defined, 422
 Process control system, 113
 Process Hazard Analysis (PHA), 322,
 See also HIRA
 Process Safety Management (PSM),
 75, 326
 process-related incident, 14
 defined, 423
 protection layer, 294, *See Layers of protection*
 protective gear
 evidence gathering equipment, 163

Q

quality assurance, 194, 217, 245, 255,
 257
 report, 307
 quantitative risk assessment
 defined, 417
 questioning, witness interviews. *See*
 Witness management

R

rapport, witness, 118, 121, 129
 recommendations
 developing, 70
 implementation, 72
 review, 334
 regulatory compliance review, 327
 report
 final, 295
 reporting system, 52, 80
 Risk Analysis. *See HIRA*
 risk management, 46
 defined, 424
 Risk Management Program (RMP),
 326
 risk ranking, 321
 defined, 424
 root cause, 4, 13, 18, 20, 21, 22, 26,
 29, 33, 37, 69
 defined, 424
 determining, 203
 investigation, 212
 root cause analysis, 203

S

safeguard, 19, 197, 289
 defined, 424
 Scanning Electron Microscope (SEM),
 186
 scenario, 203, 218, 232
 determination, 244
 scientific method, 31, 34, 35, 178,
 180, 202

- defined, 425
- sequence diagram, 29, 31, 34, 36, 168, 174, 175, 176, 187, 193, 195, 198, 199, 212, 257
- Sequentially Timed Events Plot (STEP), 31, 33, 199
- sharing
 - institutionalizing lessons learned, 345–47
 - lessons learned, 345
- significant incident
 - defined, 425
- simulations, 119, 171, 179, 187, 191, 192
- site visit, 77, 138
 - evidence gathering techniques, 157
- statistics, 337
- stopping guidelines
 - logic trees, 232
- structured approach, 203–6, 278
- substitution
 - inherent safety, 284
- supervision, 18, 21, 74, 261, 273
- systems theory, 219

T

- tape recording. *See* Audio recording
- team. *See* Incident investigation team
- technology
 - electronics, 187
 - photographic, 166
- testimony. *See* Interviews, Witness management
- Three Mile Island
 - nuclear power plant incident, 317
- timelines, 31, 34, 36
 - constructing, 168
- tools

- and methodologies, 26–43
- incident investigation equipment, 162
- top event, 33, 42, 203, 216, 219
 - choosing, 220
- training, 49, 51, 67
 - leaders, 69
 - program requirements, 65
 - team members, 68
- trend analysis, 39, 86, 92, 247, 257

U

- ultrasonic testing, 186
- underlying causes, 204, 208, 212, 259, 271, 272, 285, *See* Root cause human factors, 273

V

- validation
 - defined, 426
 - hypothesis, 190
 - of effectiveness, 317
 - scientific, 2
- verification
 - defined, 426
 - follow-up, 323
- video, 35, 154, 157, 158, 167
 - and photography, 164
 - camera, 163
 - recorder, 133
- visual examination, 185, 362

W

- Why tree, 40, 219
- witness management, 110, 118
- witnesses. *See* Witness management