GUIDELINES FOR HAZARD EVALUATION PROCEDURES

Third Edition

Center for Chemical Process Safety
New York, New York

An AIChE Industry Technology Alliance

A JOHN WILEY & SONS, INC., PUBLICATION

This Page Intentionally Left Blank

GUIDELINES FOR HAZARD EVALUATION PROCEDURES

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

GUIDELINES FOR HAZARD EVALUATION PROCEDURES

Third Edition

Center for Chemical Process Safety
New York, New York

An AIChE Industry Technology Alliance

A JOHN WILEY & SONS, INC., PUBLICATION

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

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

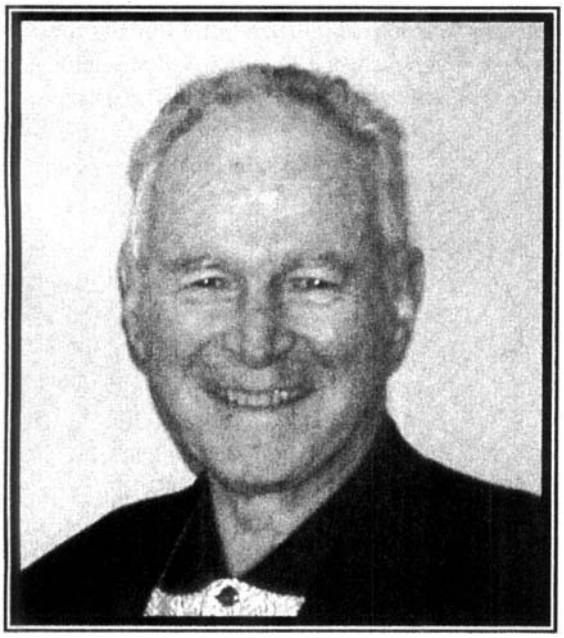
Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

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

ISBN 978-0-471-97815-2

Printed in the United States of America.

10 9 8 7 6 5 4



In Honor of Tom Carmody

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

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

This Page Intentionally Left Blank

Contents

Part II - Worked Examples and Appendices

This Page Intentionally Left Blank

Acknowledgments

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

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

Jonathan Babcock
Eli Lilly and Company

Kumar Bhimavarapu
FM Global

Christine E. Browning
Eastman Chemical Company

Paul Butler
Buckman Laboratories

Ken Harrington, HEP3 Subcommittee Chair
Chevron/Phillips

Wayne Jamison
Intel

Jim Johnston
Wyeth

Bob Lenahan
Bayer BMS

Donald Lorenzo
ABS Consulting

Narayanan Sankaran
UOP

John C. Stoney
BP

Angela Summers
SIS-TECH Solutions, LP

Tim Wagner
The Dow Chemical Company

Joe Wilson
Syngenta

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

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

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

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

List of Tables

Table

Table

List of Figures

Figure

Abbreviations and Acronyms

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

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

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

Glossary

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Failure: Cessation of equipment to operate as specified.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Mitigate: Reduce the impact of a loss event.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

This Page Intentionally Left Blank