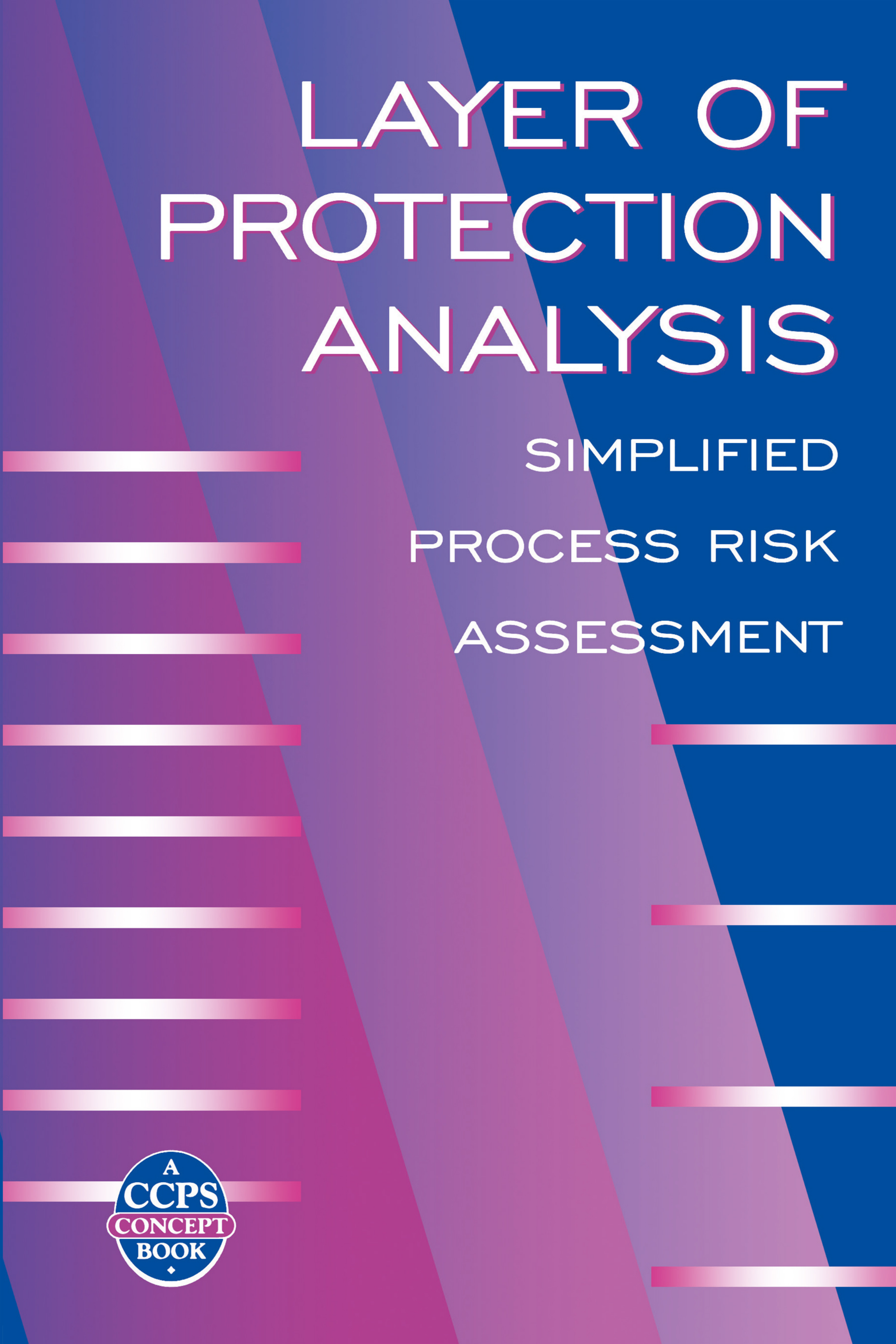

LAYER OF PROTECTION ANALYSIS

SIMPLIFIED PROCESS RISK ASSESSMENT

A CCPS CONCEPT BOOK

Layer of Protection Analysis

SIMPLIFIED PROCESS RISK ASSESSMENT

This is one of a series of publications available from the Center for Chemical Process Safety. A complete list of CCPS books is available online: www.aiche.org/ccps

Layer of Protection Analysis

SIMPLIFIED PROCESS RISK ASSESSMENT

CPS
CENTER FOR
CHEMICAL PROCESS SAFETY

An AIChE Industry
Technology Alliance

Center for Chemical Process Safety
of the
American Institute of Chemical Engineers
3 Park Avenue
New York, New York 10016-5991

American Institute of Chemical Engineers
3 Park Avenue
New York, New York 10016-5991

Library of Congress Cataloging-in-Publication Data
CIP Data applied for.

ISBN 0-8169-0811-7

It is sincerely hoped that the information presented in this volume will lead to an even more impressive safety record for the entire industry. However, the American Institute of Chemical Engineers, its consultants, CCPS Subcommittee members, their employers, and their employers' officers and directors disclaim making or giving any warranties or representations, express or implied, including with respect to fitness, intended purpose, use or merchantability, and/or correctness or accuracy of the content of the information presented in this document. As between (1) American Institute of Chemical Engineers, its consultants, CCPS Subcommittee members, their employers, and their employers' officers and directors 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

1
Introduction

2
Overview of LOPA

3
Estimating Consequences and Severity

4
Developing Scenarios

5
Identifying Initiating Event Frequency

6
Identifying Independent Protection Layers

7
Determining the Frequency of Scenarios

8
Using LOPA to Make Risk Decisions

9
Implementing LOPA

10
Using LOPA for Other Applications

11
Advanced LOPA Topics

Preface

For over 40 years the American Institute of Chemical Engineers (AIChE) has been involved with process safety and loss control in the chemical, petrochemical, hydrocarbon process and related industries and facilities. The AIChE publications are information resources for the chemical engineering and other professions on the causes of process incidents and the means of preventing their occurrences and mitigating their consequences.

The Center for Chemical Process Safety (CCPS), a Directorate of the AIChE, was established in 1985 to develop and disseminate information for use in promoting the safe operation of chemical processes and facilities and the prevention of chemical process incidents. With the support and direction of its advisory and management boards, CCPS established a multifaceted program to address the need for process safety technology and management systems to reduce potential exposures to the public, the environment, personnel and facilities. This program entails the development, publication and dissemination of *Guidelines* relating to specific areas of process safety; organizing, convening and conducting seminars, symposia, training programs, and meetings on process safety-related matters; and cooperating with other organizations and institutions, internationally and domestically to promote process safety. Within the past several years CCPS extended its publication program to include a "Concept Series" of books. These books are focused on more specific topics than the longer, more comprehensive *Guidelines* series and are intended to complement them. With the issuance of this book, CCPS has published 65 books.

CCPS activities are supported by the funding and technical expertise of over 80 corporations. Several government agencies and nonprofit and academic institutions participate in CCPS endeavors.

In 1989 CCPS published the landmark *Guidelines for the Technical Management of Chemical Process Safety*. This book presents a model for process safety management built on twelve distinct, essential, and interrelated elements. The foreword to that book states:

> For the first time all the essential elements and components of a model of a technical management program have been assembled in one document. We believe the *Guidelines* provide the umbrella under which all other CCPS Technical Guidelines will be promulgated.

This Concept Series book supports several of the twelve elements of process safety enunciated in the landmark *Guidelines for the Technical Management of Chemical Process Safety* including Process Risk Management, Incident Investigation, Process Knowledge and Documentation, and Enhancement of Process Safety Knowledge. The purpose of this book is to assist designers and operators of chemical facilities to use Layer of Protection Analysis (LOPA) to evaluate risk and to make rational decisions to manage risk with a simplified methodology.

Acknowledgments

The American Institute of Chemical Engineers and the Center for Chemical Process Safety express their gratitude to all the members of the Layer of Protection Analysis Subcommittee for their generous efforts and technical contributions in the preparation of this Concept Series book.

Layer of Protection Analysis: Simplified Process Risk Assessment was written by the Center for Chemical Process Safety Layer of Protection Analysis Subcommittee.

Chair:
Arthur M. Dowell, III, P.E. *Rohm and Haas Company*

The primary authors were
William G. Bridges *ABS Consulting (includes former JBF Associates)*
Arthur M. Dowell, III, P.E. *Rohm and Haas Company*
Martin Gollin *Consultant, formerly of ARCO Chemical*
Warren A. Greenfield *International Specialty Products*
John M. Poulson *now retired from Union Carbide Corporation*
William Turetsky *International Specialty Products*

Providing support and valuable contributions throughout the project were
John T. Marshall *The Dow Chemical Company*
Stanley A. Urbanik *E. I. Du Pont de Nemours and Company*

Providing important guidance in the conceptual phases of the book were
Rodger M. Ewbank *Rhodia Inc.*
Robert J. Gardner *now retired from E. I. Du Pont de Nemours and Company*
Kumar Bhimavarapu *Factory Mutual Research*
John A. McIntosh *The Proctor & Gamble Company*

R. Peter Stickles *A. D. Little*
Arthur W. Woltman *Equilon Enterprises LLC, formerly Shell*

CCPS Staff Consultant
Robert E. Bollinger *Center for Chemical Process Safety*

Editor
Dr. Daniel A. Crowl *Michigan Technological University*

The Subcommittee acknowledges the support and contributions of their employer organizations in completing this book. Dr. Jack Weaver and Mr. Les Wittenberg of CCPS sponsored and supported this project and provided access to the resources of CCPS and its sponsoring organizations. The authors thank the following for their contributions in creation of figures and tables, setting up committee meetings and teleconferences and other administrative functions that were essential to the completion of this book: Ms. Jill Johnson and Mr. Paul M. Olsen, ABS Consulting; Ms. Sandy Baswell, Ms. Marge Killmeier, Ms. Angella Lewis and Ms. Jackie Rico't, Rohm and Haas Company.

Before publication, all CCPS books are subjected to a thorough peer review process. CCPS also gratefully acknowledges the thoughtful comments and suggestions of the peer reviewers. Their work enhanced the accuracy and clarity of the book.

Steve Arendt *ABS Consulting (includes former JBF Associates)*
Helmut Bezecny *Dow Deutschland Inc.*
Alfred W. Bickum *Goodyear Tire and Rubber Company*
Dennis Blowers, C.S.P. *Solvay Polymers, Inc.*
Michael P. Broadribb *BP Amoco Company*
David Campbell *Concord Associates*
Bill Carter *CCPS Staff Consultant*
Curtis Clements *E. I. Du Pont de Nemours and Company*
Kimberly F. Dejmek *Wilfred Baker Engineering*
Richard R. Dunn *E. I. Du Pont de Nemours and Company*
Jim Evans *Union Carbide Corporation*
Rodger M. Ewbank *Rhodia Inc.*
Dave Fontaine *Chevron Corporation*
Raymond A. Freeman *ABS Consulting*
Raymond W. French *Exxon Mobil Corporation*
Dallas L. Green *Rohm and Haas Company*
Dennis C. Hendershot *Rohm and Haas Company*
William H. Johnson *E. I. Du Pont de Nemours and Company*
Peter N. Lodal, P.E. *Eastman Chemical Company*
Donald M. Lorenzo *ABS Consulting (includes former JBF Associates)*

Vic Maggioli *Feltronics Corporation*
Rick Mann *Union Carbide Corporation*
Peter McGrath *Olin Corporation*
Norman McLeod *ATOFINA Chemicals, Inc.*
Steve Metzler *Primatech Inc.*
Dr. Hans Pasman *TNO*
Jack Philley, C.S.P. *Det Norske Veritas (DNV)*
Michael E. G. Schmidt, P.E. *Industrial Risk Insurers*
Art Schwartz *Bayer Corporation*
Adrian Sepeda *Occidental Chemical Corporation*
Bastiaan Schupp *Delft University of Technology*
Robert Stankovich *Eli Lilly and Company*
Peter Stickles *A. D. Little*
Dr. Angela E. Summers, P.E. *SIS-Tech Solutions, LLC*
Clark Thurston *Union Carbide Corporation*
Anthony Torres *Eastman Kodak*
Jan Windhorst *NOVA Chemicals*

Acronyms and Abbreviations

AIChE	American Institute of Chemical Engineers
ALARP	As Low as Reasonably Practicable
ANSI	American National Standards Institute
API	American Petroleum Institute
ASME	American Society of Mechanical Engineers
BI	Business Interruption
BLEVE	Boiling Liquid Expanding Vapor Explosion
B.P.	Boiling Point
BPCS	Basic Process Control System
C	Consequence factor, related to magnitude of severity
CCF	Common Cause Failure
CCPS	Center for Chemical Process Safety, American Institute of Chemical Engineers
CEI	Dow Chemical Exposure Index
CPQRA	Chemical Process Quantitative Risk Assessment
CW	Cooling Water
D	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, American Institute of Chemical Engineers
DOT	Department of Transportation

EBV	Emergency Block Valve
ERPG	Emergency Response Planning Guideline
EuReData	European Reliability Data (series of conferences)
F	Failure Rate (hr^{-1} or year^{-1})
f	Frequency (hr^{-1} or year^{-1})
F&EI	Dow Fire and Explosion Index
F/N	Fatality Frequency versus Cumulative Number
FCE	Final Control Element
FMEA	Failure Modes and Effect Analysis
FTA	Fault Tree Analysis
HAZOP	Hazard and Operability Study
HE	Hazard Evaluation
HRA	Human Reliability Analysis
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IPL	Independent Protection Layer
ISA	The Instrumentation, Systems, and Automation Society (formerly, Instrument Society of America)
LAH	Level Alarm – High
LI	Level Indicator
LIC	Level Indicator – Control
LFL	Lower Flammability Limit
LNG	Liquefied Natural Gas
LOPA	Layer of Protection Analysis
LOTO	Lock-Out Tag-Out
LT	Level Transmitter
MAWP	Maximum Allowable Working Pressure
MOC	Management of Change
N_2	Nitrogen
OSBL	Outside Battery Limits
OREDA	The Offshore Reliability Data project
OSHA	Occupational Safety and Health Administration (U.S.)
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

PFD	Probability of Failure on Demand
PHA	Process Hazard Analysis
PI	Pressure Indicator
PL	Protection Layer
PM	Preventive Maintenance
PSM	Process Safety Management
PSV	Pressure Safety Valve (Relief Valve)
R	Risk
RV	Relief Valve
SCE	Safety Critical Equipment
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
T	Test Interval for the Component or System (hours or years)
VCE	Vapor Cloud Explosion
VLE	Vapor Liquid Equilibrium
XV	Remote Activated/Controlled Valve

1

Introduction

Layer of protection analysis (LOPA) is a semiquantitative tool for analyzing and assessing risk. This book

- describes the LOPA process,
- discusses the strengths and limitations of LOPA,
- describes the requirements for implementing LOPA in an organization, and
- provides worked examples that show how several different companies have applied LOPA.

This chapter

- identifies the audience for this book,
- provides the history of LOPA,
- shows the use of LOPA in the process life cycle,
- discusses the linkage to other publications, and
- provides an annotated outline for the book.

1.1. Audience

This book is intended for:

- Executives who are considering expanding their corporate strategy for managing risk by adding LOPA to their existing risk analysis process. For the executive audience, the following chapters are recommended. Chapter 2 summarizes the LOPA method and its benefits. Chapter 9 discusses the questions that an organization must answer when deciding whether to use LOPA and the required steps to implement the process effectively. Chapter 10 describes other processes (such as management of change, identification of safety critical equipment, etc.) which can be enhanced by LOPA. The appendices contain summary forms and worked examples that demonstrate the LOPA product.

- Safety specialists who are familiar with existing methods (such as HAZOP, fault tree analysis, event tree analysis, etc.) or who may already have some experience with LOPA (analysts, participants, reviewers, auditors, etc.). For this audience, Chapters 3 through 8 discuss the steps of the LOPA process in detail, with several continuing examples used to demonstrate the method. The appendices contain additional worked examples and other supporting documentation.
- Process and process control engineers, chemists, operations and maintenance personnel, and others who may participate in LOPA reviews or who may be affected by LOPA recommendations. This includes those who implement the recommendations and those who receive the outcomes from LOPA. Chapters 1, 2, and 6 may be helpful for this audience.
- Persons around the world who are responsible for compliance with process safety regulations—including the US Process Safety Management rule (OSHA, 1992), Seveso II Regulations in EU member countries—and related standards—including ISA S84.01 (ISA, 1996), IEC 61508 (IEC, 1998) and IEC 61511 (IEC, 2001).

1.2. History of LOPA

In a typical chemical process, various protection layers are in place to lower the frequency of undesired consequences: the process design (including inherently safer concepts); the basic process control system; safety instrumented systems; passive devices (such as dikes and blast walls); active devices (such as relief valves); human intervention; etc. There has been much discussion among project teams, hazard analysts, and management about the number of and strength of protection layers (see text box below). Decisions were sometimes made using subjective arguments, emotional appeals, and occasionally simply by the loudness or persistence of an individual.

LOPA has its origins in the desire to answer these key questions using a rational, objective, risk-based approach. In LOPA, the individual protection

KEY QUESTIONS FOR PROTECTION LAYERS

- How safe is safe enough?
- How many protection layers are needed?
- How much risk reduction should each layer provide?

LOPA answers the key questions about the number and strength of protection layers by

- providing rational, semiquantitative, risk-based answers,
- reducing emotionalism,
- providing clarity and consistency,
- documenting the basis of the decision,
- facilitating understanding among plant personnel.

layers proposed or provided are analyzed for their effectiveness. The combined effects of the protection layers are then compared against risk tolerance criteria. Characteristics of the answers provided by LOPA are listed in the text box above.

The genesis of this method was suggested in two publications:

1. In the late 1980s, the then Chemical Manufacturers Association published the *Responsible Care® Process Safety Code of Management Practices* which included "sufficient layers of protection" as one of the recommended components of an effective process safety management system (American Chemistry Council, 2000). The Chemical Manufacturers Association is now the American Chemistry Council.
2. In 1993, CCPS published its *Guidelines for Safe Automation of Chemical Processes* (CCPS, 1993b). Although it was called the risk-based SIS integrity level method, LOPA was suggested as one method to determine the integrity level for safety instrumented functions (SIFs). (See Table 7.4 in *Safe Automation;* CCPS, 1993b.) "Interlock" is an older, imprecise term for SIF. The method used was not as fully developed as the LOPA technique described in this book. However, it did indicate a path forward, which was pursued by several companies independently. The reasons for this effort included the desire to

   - classify SIF to determine the appropriate safety integrity level (SIL) (this was the starting point for some companies),
   - develop a screening tool to reduce the number of scenarios requiring a full (chemical process) quantitative risk assessment (CPQRA),
   - develop a tool that would identify "safety critical" equipment and systems to focus limited resources,
   - develop a semiquantitative tool to make consistent risk based judgments within an organization,
   - harmonize terminology and methodology with recently developed and developing international process sector standards, and
   - facilitate communication (e.g., SIS, SIF, SIL, IPL) between the hazard and risk analysis community and the process control community (e.g., integrators, manufacturers, instrument and electrical engineers, plant personnel).

The initial development of LOPA was done internally within individual companies, in some cases focusing on existing processes, e.g., converting a control system to DCS. However, once a method had been developed and refined, several companies published papers describing the driving forces behind their efforts to develop the method, their experience with LOPA, and examples of its use (Dowell, 1997; 1998; 1999a; 1999b; Bridges and Williams, 1997; Fuller and Marszal, 1999; Lorenzo and Bridges, 1997; Ewbank and York, 1997; Huff and Montgomery, 1997). In particular, the papers and discussion among the attendees at the *CCPS International Conference and Workshop on Risk Analysis in Process Safety* in Atlanta in October 1997 brought agreement that a book describing the LOPA method should be developed.

In parallel with these efforts, discussions took place on the requirements for the design of safety instrumented functions (SIF) to provide the required PFDs (probability of failure on demand). United States (ISA S84.01, (ISA, 1996)) and international standards (IEC 61508, (IEC, 1998) and IEC 61511, (IEC, 2001)) described the architecture and design features of SIFs. Informative sections of the ISA and IEC standards suggested methods to determine the required SIL (safety integrity level), but LOPA was not mentioned until the draft of IEC 61511, Part 3 appeared in late 1999. These issues were summarized in the CCPS workshop on the application of ISA S84.01 (CCPS, 2000c).

In response to all this activity, CCPS assembled in 1998 a team from A. D. Little, ARCO Chemical, Dow Chemical, DuPont, Factory Mutual, ABS Consulting (includes former JBF Associates), International Specialty Products, Proctor and Gamble (P&G), Rhodia, Rohm and Haas, Shell (Equilon), and Union Carbide to tabulate and present industry practice for LOPA in this book.

This book extends the method outlined in *Safe Automation of Chemical Processes* (CCPS, 1993b) by

- developing concepts and definitions for use throughout industry,
- showing how numerical risk tolerance criteria have been developed by different companies,
- defining the requirements for a safeguard to be considered an independent protection layer (IPL),
- demonstrating how LOPA can be used for purposes other than the classification of SIF systems, and
- recommending documentation procedures to ensure consistency of application within an organization.

While the LOPA methods used by various companies differ, they share the following common features:

- a consequence classification method that can be applied throughout the organization;
- numerical risk tolerance criteria. Individual companies use different criteria which include:

  - ◇ frequency of fatalities,
  - ◇ frequency of fires,
  - ◇ required number of independent protection layers (IPLs), and
  - ◇ maximum frequency for specified categories of consequence based on release size and characteristics or lost production;
- a method for developing scenarios;
- specific rules for considering safeguards as IPLs;
- specified default data for initiating event frequencies and values for IPLs;
- a specified procedure for performing the required calculations; and
- a specified procedure for determining whether the risk associated with a scenario meets the risk tolerance criteria for an organization and, if it does not, how this is resolved and documented.

1.3. Use of LOPA in the Process Life Cycle

LOPA can be effectively used at any point in the life cycle of a process or a facility (see Figure 1.1), but it is most frequently used during:

- the design stage when the process flow diagram and the P&IDs are essentially complete. LOPA is used to examine scenarios, often generated by other process hazard analysis (PHA) tools, such as HAZOP, what-if, checklist, etc.; as part of the SIF design; or as part of a design study on a system to classify the various process alternatives and to select the best method;
- modifications to an existing process or its control or safety systems (i.e., management of change).

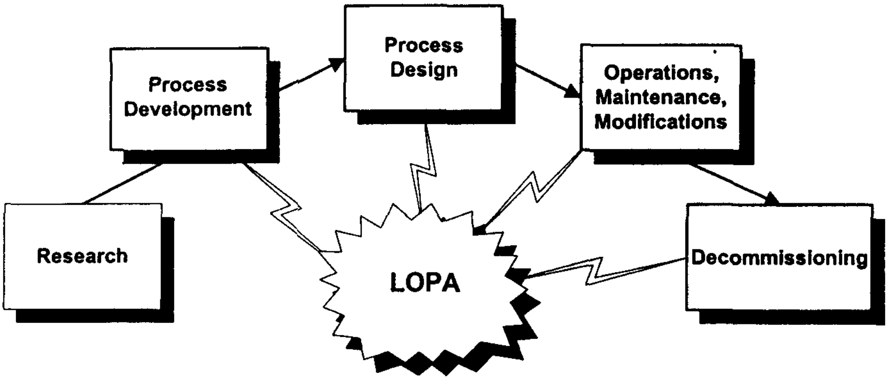

FIGURE 1.1. The process life cycle showing where LOPA is typically used (after *Inherently Safer Chemical Processes: A Life Cycle Approach*, CCPS 1996b)

However, LOPA can also be used in all phases of the process life cycle:

- LOPA can be used during the initial conceptual process design to examine basic design alternatives and provide guidance to select a design that has lower initiating event frequencies, or a lower consequence, or for which the number and type of IPLs are "better" than alternatives. Ideally, LOPA could be used to design a process that is "inherently safer" by providing an objective method to compare alternative designs quickly and quantifiably.
- LOPA can be used during the regular cycle of process hazard analyses (PHAs) performed on a process. Experience with LOPA at several companies has shown that its scenario-focused methodology can reveal additional safety issues in fully mature processes that have previously undergone numerous PHAs. In addition, its objective risk criteria have proven effective in resolving disagreements on PHA findings.
- LOPA can readily determine if the risk is tolerable for a process. If an SIF is required, LOPA can determine the required SIL. LOPA can examine alternatives to a SIF (modifying the process, adding other IPLs, etc.). Note that IEC 61508 (IEC, 1998) and IEC 61511 (IEC, 2001) define a safety system life cycle that covers all the activities associated with safety instrumented functions. LOPA can be a valuable tool in that safety system life cycle.
- LOPA can be used to identify equipment that, as part of an IPL, is relied upon to maintain the process within the tolerable risk criteria of an organization. Such equipment may be denoted as "safety critical" (ISA S91.01, 1995) and is subjected to specified testing, inspection and maintenance. At least one company has found that LOPA has significantly **decreased** the number of safety critical equipment items. (The amount of safety critical equipment had erroneously grown over time by adding equipment on a qualitative "better safe than sorry" basis.)
- LOPA can be used to identify operator actions and responses that are critical to the safety of the process. This will allow focused training and testing to be performed during the life of the process and for the operating manuals to reflect the importance of a limited number of process variables, alarms and actions.

LOPA can also be used for other risk assessment studies within an organization, including transportation studies (road, rail, pipeline), terminal operations, toll conversion operations, auditing of third parties, loss prevention and insurance issues, etc.

In some companies LOPA is now used for a wide variety of purposes beyond the initial use for which it was developed (see Chapter 10).