Fourth Edition

Safety and Security Review for the Process Industries

Application of HAZOP, PHA, What-IF and SVA Reviews

Dennis P. Nolan

Safety and Security Review for the **PROCESS INDUSTRIES**

Dedicated to
Kushal, Nicholas, and Zebulon

Safety and Security Review for the PROCESS INDUSTRIES

Application of HAZOP, PHA, What-IF and SVA Reviews

Fourth Edition

DENNIS P. NOLAN, PH.D., P.E.

ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO
Gulf Professional Publishing is an imprint of Elsevier

Gulf Professional Publishing is an imprint of Elsevier
225 Wyman Street, Waltham, MA 02451, USA
The Boulevard, Langford Lane, Kidlington, Oxford, OX5 1GB, UK
525 B Street, Suite 1800, San Diego, CA 92101-4495, USA

Notices

Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

ISBN: 978-0-323-32295-9

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the Library of Congress.

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

Typeset by MPS Limited, Chennai, India
www.adi-mps.com

Printed and bound in the United States

CONTENTS

This page intentionally left blank

ABOUT THE AUTHOR

Dr. Dennis P. Nolan has had a long career devoted to risk engineering, fire protection engineering, loss prevention engineering, and systems safety engineering. He holds a Doctor of Philosophy degree in Business Administration from Berne University, a Master of Science degree in Systems Management from Florida Institute of Technology, and a Bachelor of Science Degree in Fire Protection Engineering from the University of Maryland. He is a US-registered professional engineer in fire protection engineering in the state of California.

He is currently on the Executive Management staff of Saudi Aramco, located in Dhahran, Saudi Arabia, as a Loss Prevention Consultant/Chief Fire Prevention Engineer. He covers some of the largest oil and gas facilities in the world. The magnitude of the risks, worldwide sensitivity, and foreign location make this one of the most highly critical fire risk operations in the world. He has also been associated with Boeing, Lockheed, Marathon Oil Company, and Occidental Petroleum Corporation in various fire protection engineering, risk analysis, and safety roles in several locations in the United States and overseas. As part of his career, he has examined oil production, refining, and marketing facilities under severe conditions and in various unique worldwide locations, including Africa, Asia, Europe, the Middle East, Russia, and North and South America. His activity in the aerospace field has included engineering support for the NASA Space Shuttle launch facilities at Kennedy Space Center (and for those undertaken at Vandenberg Air Force Base, California) and "classified" national defense systems.

Dr. Nolan has received numerous safety awards and is a member of the American Society of Safety Engineers. He is the author of many technical papers and professional articles in various international fire safety publications. He has written four other books: *Handbook of Fire and Explosion Protection Engineering Principles for Oil, Gas, Chemical, and Related Facilities* (1st, 2nd, and 3rd editions), *Fire Fighting Pumping Systems at Industrial Facilities* (1st and 2nd editions), *Encyclopedia of Fire Protection* (1st and 2nd editions), and *Loss Prevention and Safety Control Terms and Definitions*. Dr. Nolan has also been listed for many years in

"Who's Who in California," "Who's Who in the West," "Who's Who in the World," and "Who's Who in Science and Engineering" publications. He was also listed in "Outstanding Individuals of the 20th Century" (2001) and "Living Legends" (2004), published by the International Biographical Center, Cambridge, England.

PREFACE

This book is intended as a typical resource and reference book that may be applied to industrial facilities, commercial processes, and systems. It is suggested that this resource be used as a practical reference to prepare the safety review requirements for a process safety or security management system.

The first edition of this book was titled *Application of HAZOP and What-If Safety Reviews in the Petroleum, Petrochemical, and Chemical Industries* and was originally published in 1994. Since that time, the use of Preliminary Hazard Analyses (PHAs) has become more prevalent and the threat to industrial and commercial facilities from security incidents has also become more relevant. Numerous other industrial and trade organizations have also since published similar guidance documents for PHAs and Security Vulnerability Analyses (SVAs). It was therefore prudent to update this book to include these aspects and also incorporate additional technical updates and features.

The third edition of this book added similar safety reviews related to PHAs and HAZOPs such as Bow-Tie Analysis (BTA), Layers of Protection Analysis (LOPA), and Safety Integrity Levels (SIL). This fourth edition includes recent variations on the HAZOP, that is, Control or Computer HAZOPs (CHAZOPs) and Power HAZOPs (PHAZOPs), utilization of the fishbone technique, and the integration of these safety reviews with the current trend of operational excellence that is being applied throughout the management of process facilities. Further refinements in the scope, overall content, regulatory changes, economics, and timing have also been incorporated. Using these methodologies to examine industrial facilities will greatly reduce the probability of an incident occurring from process upsets, unknown hazards, or security threats.

This page intentionally left blank

ACKNOWLEDGMENTS

Figure 9.1 was provided by Issam Karkoutlie of INOVx Solutions, EAM Plant Solutions, Irvine, CA, reprinted with permission. Figures 10.1–10.4 were provided by Steve Metzler of Primatech, Inc., Columbus, OH, reprinted with permission.

This page intentionally left blank

LIST OF ACRONYMS

AIChE	American Institute of Chemical Engineers
ALARP	As Low As Reasonably Practical
ANSI	American National Standards Institute
API	American Petroleum Institute
ASME	American Society of Mechanical Engineers
BPCS	Basic Process Control System
BS & W	Basic Sediment and Water
BTA	Bow-Tie Analysis
CCPS	Center for Chemical Process Safety
CFATS	Chemical Facility Anti-Terrorism Standard
CFR	Code of Federal Regulations
CHAZOP	Computer Hazard and Operability Study
CSAT	Chemical Security Assessment Tool
CSB	Chemical Safety and Hazard Investigation Board
CSVA	Cyber Security Vulnerability Analysis
DHS	Department of Homeland Security
DMR	Dual Modular Redundant
EHAZOP	Electrical Hazard and Operability Study
EPA	Environmental Protection Agency
ERP	Emergency Response Plan
ESD	Emergency Shutdown
FBI	Federal Bureau of Investigation
FDA	Food and Drug Administration
FEED	Front End Engineering Design
FMEA	Failure Modes and Effects Analysis
FTA	Fault Tree Analysis
GW	Guideword
H_2S	Hydrogen Sulfide
HAZOP	Hazard and Operability
HIPS	High Integrity Protective Systems
HSE	Health, Safety, and Environment
HVAC	Heating, Ventilation, and Air Conditioning
ICI	Imperial Chemical Industries, Ltd.
I/O	Input/Output
IPL	Independent Protection Layer
ISA	International Society of Automation

JSA	Job Safety Analysis
LNG	Liquefied Natural Gas
LOPA	Layers of Protection Analysis
LPG	Liquefied Petroleum Gas
MOC	Management of Change
MSDS	Material Safety Data Sheet
MTBF	Mean Time Between Failures
NACE	National Association of Corrosion Engineers
NFPA	National Fire Protection Association
NIST	National Institute of Science and Technology
OE	Operational Excellence
OSHA	Occupational Safety and Health Administration
PC	Personal Computer
PCV	Pressure Control Valve
PET	Project Estimated Time
PFD	Process Flow Diagram
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List
P&ID	Piping and Instrumentation Diagram
PL	Protection Layer
PLC	Programmable Logic Controller
PSM	Process Safety Management
PSSR	Pre-Startup Safety Review
PSV	Pressure Safety Valve
QA	Quality Assurance
RAM	Risk Assessment Matrix
ROPA	Ring of Protection Analysis
RP	Recommended Practice
RR	Risk Reduction
RRF	Risk Reduction Factor
SAFE	Safety and Failure Effects
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SSP	Site Security Plan
SVA	Security Vulnerability Analysis
TMR	Triple Modular Redundant
UK	United Kingdom

NOTICE

Reasonable care has been taken to assure that the book's content is authentic, timely, and relevant to the industry today; however, no representation or warranty is made as to its accuracy, completeness, or reliability. Consequentially, the author and publisher shall have no responsibility or legal liability to any person or organization for loss or damage caused or believed caused, directly or indirectly, by this information. In publishing this book, the publisher is not engaged in rendering legal advice or other professional services. It is up to the reader to investigate and assess his or her own situation. Should such study disclose a need for legal or other professional assistance, the reader should seek and engage the services of qualified professionals.

This page intentionally left blank

CHAPTER 1

Purpose

This publication is intended to provide guidance to qualitative hazard analyses conducted for industrial and commercial process, specifically for PHA (Preliminary Hazard Analysis), What-If, and HAZOP (Hazard and Operability) review teams. It also highlights how the methodology and procedures used for these reviews can be adopted and applied for Security Vulnerability Analysis (SVA). This book describes the nature, responsibilities, methods, and documentation required in the performance of such reviews. This ensures that these reviews are conducted in a timely, effective, objective, and consistent manner as may be prescribed by a company's Process Safety Management (PSM) policy and security requirements. This book relies heavily on the common practices in the petroleum, chemical, and petrochemical industries because most of the major hazardous processes are located in these industries and these facilities are increasingly becoming a potential target for security incidents.

The safety and security of process facilities are an important part of a company's operations. Worldwide petrochemical safety regulations, international security threats, and a company's own PSM policies require that a hazard identification, process safety, and security analysis review of its existing and proposed operations be accomplished.

The worldwide petroleum and chemical insurance market estimates for the period 1993–2013 that there have been about 1,100 major insurance claims (i.e., major incidents), amounting to approximately $32 billion (for property damage and business interruption). Their analysis estimates that the worldwide risk has been constant over this period, that is, the average frequency and cost impact has been a constant trend, neither decreasing nor increasing. This equates on average to 110 losses totaling $2–3 billion per year. Additionally, these losses would fit a traditional loss incident ratio triangle (see Figure 1.1) with an ever-increasing number of losses as the magnitudes of the losses decrease (i.e., as the steps in the triangle widen).

Safety and Security Review for the Process Industries
DOI: http://dx.doi.org/10.1016/B978-0-323-32295-9.00001-X

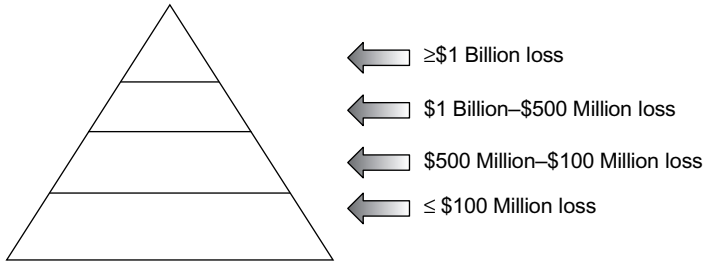

Figure 1.1 Loss triangle, number versus magnitude.

Today, new projects are in the region of $50 + billion, which equates to the Deepwater Horizon incident loss (April 20, 2010), and the potential for even larger losses from a single incident is still a possibility. The industry must do more to prevent these incidents and improve safety so that this trend decreases.

Most incidents occur during periods of nontypical operations, such as maintenance activities, startup or shutdown, and drilling activities. This is when more attention, knowledge, and experience are required from personnel to safely manage the facility. Therefore, special attention needs to be applied to circumstances that are out of the normal operating mode of processes.

The limits of hazardous substances cited by both the US Occupational Safety and Health Administration (OSHA) and the Environmental Protection Agency (EPA) regulations dictate the application of PSM elements at almost all of a company's facilities. These reviews are intended to reduce the probability and consequences of a major incident that would have a detrimental impact on employees, the public's well-being, onsite or offsite properties, the environment, and most importantly to the company itself, its continued business operation and survival. It should also be noted that there may be a general adverse public reaction and therefore a company's reputation may suffer. Hazard identification and process analysis reviews are not intended to identify the minor "slips, trips, or falls"; these are the responsibility of the company's general safety requirements and can be analyzed with other tools (for example, Job Safety Analysis (JSA)).

In March 2003, the United States implemented Operation Liberty Shield to increase readiness and security in the United States, primarily due to international threats from nongovernment affiliated, self-motivated political and religious groups. One objective of this operation was to implement comprehensive process security management programs into existing OSHA, EPA, and FDA laws to address deliberate acts of threats of terrorism, sabotage, and vandalism. In April 2007, the Department of Homeland Security (DHS) issued the Chemical Facility Anti-Terrorism Standard (CFATS). DHS uses this document to help identify, evaluate, and ensure effective security at high-risk chemical facilities. Included in this responsibility is the requirement for chemical facilities handling chemicals above a threshold amount to submit an SVA for DHS review and approval along with a Site Security Plan (SSP). A potential fine of $25,000 per day, an inspection and audit by DHS, or an order to cease operations is stated for noncompliance. The type and amount of chemicals handled that require submission of screening review and SVA submittals are listed on the DHS website. Additionally, internal company security procedures, although confidential, would also require that an adequate security review be undertaken to identify and assess such risks. Because the methodology of conducting process security reviews are

similar to existing process hazard analysis reviews, they can be adapted to fit within the parameters of existing procedures established for these analyses. Both API and AIChE have also issued their own guidelines to assist companies undertaking process security reviews. A major process safety consultant recently stated that statistics show that the use of outside security experts for protective services consultations has increased by 200% in the last 5 years. This is due to escalating concerns over workplace and domestic violence, privacy and security practices, and terrorist threats. Process security reviews are not intended to identify minor thefts or mishaps; these are the responsibility of the company's general security requirements and can be examined with other financial auditing tools.

Recent cybersecurity attacks worldwide have emphasized the importance of software security for financial and operational applications within process entities. The National Institute of Standards and Technology (NIST) has recently released a document entitled "Framework for Improving Critical Infrastructure Cybersecurity." This framework provides a structure that organizations can use to develop and improve cybersecurity programs. NIST was charged with putting the framework together under US Presidential Executive Order 13636 (February 2013), which calls for the development of a voluntary, risk-based cybersecurity framework.

The framework document is described as a living document that will need to be updated to keep pace with changes in technology, threats, and other factors, and to incorporate lessons learned from its use. The document describes three main elements: framework core, tiers, and profiles. The framework core presents five functions: identify, protect, detect, respond, and recover. Together, they allow an organization to understand and shape its cybersecurity program. Tiers describe the degree to which an organization's cybersecurity program meets goals identified in the framework. Profiles help organizations improve their current cybersecurity programs.

The purpose of the safety and security evaluations described in this book is to identify the major risks facing the industry that have the potential for severe impacts. It identifies simple processes and procedures to apply these reviews in an easy, practical manner.

PHA, What-If, and HAZOP reviews are the most common industry qualitative methods used to conduct process hazard analyses, while SVAs are typically applied for process security analyses. It is qualitatively estimated that up to 80% of a company's hazard identification and process safety analyses may consist of PHA, What-If, and HAZOP reviews, with

the remaining 20% from Checklist, Fault Tree Analysis, Event Tree, Failure Mode and Effects Analysis, and so on. Chapter 5 highlights other reviews that are periodically utilized by the process industries.

An experienced review team can use the analyses described to generate possible deviations from design, construction, modification, and operating intent or from deliberate actions that define potential consequences. These consequences can then be prevented or mitigated by the application of the appropriate safeguards.

The reader is reminded that a PHA, What-If, HAZOP, or an SVA report is a living document for a facility. As changes are made to a facility or its procedures, the applicable review is to be updated to represent the current facility. PHA reviews are also required to be updated and revalidated every 5 years as a minimum according to US regulations (OSHA and EPA). Also, because terrorist threats still exist, threat assessment/vulnerability analysis needs to be continually reevaluated.

A completed review can be used to demonstrate to interested parties that a prudent analysis has been accomplished and all possible actions have been examined and implemented to eliminate major hazards or minimize the threat. The Chemical Safety and Hazard Investigation Board (CSB) routinely examines and reviews hazard analyses that have been performed on processes to ensure that they were performed adequately.

This document can also be referred to by review team members. It will serve as a reminder of their duties and responsibilities in the performance of the required reviews and report development.

CHAPTER 2

Scope

These guidelines should be considered for all of a company's facilities, domestically and internationally. They are intended to be applied at both permanent and temporary facilities, whether located on- or offshore.

The typical review is usually intended to be a formal audit review of an "essentially" complete project design or modification to ensure that the probabilities or consequences of major incidents have been eliminated or reduced to acceptable levels prior to being placed in service. Risk analyses should be continually conducted as part of the project design to avoid the identification of major concerns in later reviews. In fact, documentation from a design risk analysis should supplement the formal HAZOP, PHA, What-If, or SVA review.

Process safety and security reviews are not intended to replace or duplicate a project design review. Unusually complex or large projects may require several levels of a safety or security review during their design phase. These may be initiated at the conceptual design stage, preliminary design, detailed design, and at the final design. Such levels are usually encountered in multimillion-dollar offshore facilities, refineries, or chemical processing plant projects where major changes occurring later in the design would be severe in economic and schedule terms. These multilevel reviews start at a broad viewpoint and gradually narrow to specifics

Safety and Security Review for the Process Industries
DOI: http://dx.doi.org/10.1016/B978-0-323-32295-9.00002-1

as the project design proceeds. Where operating procedures are not available during the design, a supplemental PHA, What-If, HAZOP, or SVA review may be considered for these documents. In fact, an initial review may recommend that subsequent final designs be again evaluated by a PHA, What-If, HAZOP, or SVA as a follow-up. It is essential that these follow-up reviews be completed because incidents investigated by the CSB have identified failure to perform a follow-up risk analysis as a contributing factor in some incidents.

During the period of initial implementation of process safety and security management policies, existing facilities may also be the subject of PHA, What-If, HAZOP, or SVA reviews.

Typically, most reviews will be concentrated on processes that have the potential for major incidents (i.e., hydrocarbon or chemical processing equipment and operations). It should be remembered that where there are utility systems that could pose severe consequences to individuals or the company (e.g., toxic vapor releases, exposed high-voltage electrical components), a review of their system or components also should be considered.

The basic approach for these reviews is quite flexible. They can be used to analyze a variety of operations and processes such as oil and gas well drilling, product manufacturing, chemical production, factory processes, chemical processing, transportation, marketing, computer control logic, operating procedures, organizational changes, security control, and monitoring.

CHAPTER 3

Objective and Description of PHA, What-If, and HAZOP Reviews

Most hazards that arise in a system are thought to be due primarily to defects in design, material, workmanship, or human error.

There are many methods of safety analysis reviews that are available and can be applied to a facility or project design to overcome human errors and the various failures of the process system. The methods may be either qualitative or quantitative in nature.

Qualitative Methods	Quantitative Methods
• Checklists • Preliminary Hazard Analysis (PHA) • What-If Reviews • Hazard and Operability Reviews (HAZOP) • Bow-Tie Analysis (BTA) • Fishbone	• Event Trees • Fault Trees • Failure Modes and Effects Analysis • Layers of Protective Analysis (LOPA; semiqualitative) • Safety Integrity Level (SIL) Analysis

Quantitative methods are usually applied to obtain a more precise evaluation of an identified hazard. These are typically employed for design evaluations and resolution of recommendations when the identified risk is above normally acceptable industry levels and when major capital expenditures need additional justification. The reader is referred to other publications for guidance on quantitative methods.

Safety reviews are primarily looking for the possibilities of where human errors may occur. Human error is commonly thought of as mainly occurring during the operational phase of the facility or system, but human error can also be the cause of defects in the design, material, or workmanship. Because most petroleum or chemical facilities are not mass produced for specific applications but individually designed, there is a large potential for human errors to occur during design, procurement,

Safety and Security Review for the Process Industries
DOI: http://dx.doi.org/10.1016/B978-0-323-32295-9.00003-3

and construction. The extended operation lives of most facilities balance the equation so that "operational" human failures are equally important.

Human error is considered when one of the following events occur (which may be applied equally to the design or operation of a facility):

1. An individual fails to perform a task or some portion of a task.
2. The task (or portion) is performed incorrectly.
3. Some step(s) is introduced into the sequence that should not have been included.
4. A step is conducted out of sequence.
5. The task is not completed within an allocated time period.

Human errors may occur from all personnel—designers, engineers, operators, and managers. Some theories attribute the majority of all incidents to human errors.

3.1 DEFINITION

PHA, What-If, and HAZOP reviews are basically a communication exercise. Information is presented, discussed, analyzed, and recorded. Specifically, the safety aspects are identified to determine if adequate design measures have been taken to prevent major incidents as perceived by the review team. Communication and evaluation are the prime facets of the procedures.

HAZOP reviews follow a definitive, step-by-step guideword approach. PHA and What-If analyses are usually combined with a checklist to provide a "road map" for the review.

3.2 OBJECTIVES

The primary objective of PHA, What-If, and HAZOP reviews are to assure that catastrophic incidents will be avoided during the lifetime of the facility from the processes under review. The objectives of the reviews are to be thorough, impartial, and adequate.

3.3 ORIGINS OF QUALITATIVE SAFETY REVIEWS

HAZOP reviews originally began in the chemical industry in the United Kingdom during the 1960s. Imperial Chemical Industries Ltd. (ICI) developed a standardized method of analyzing processing hazards based on basic operation conditions and then changed individual parameters one at a time to see the subsequent consequences. This evolved into a standard practice within their company and soon found its way into the general chemical industry (although it was not universally or consistently applied).

At the same time, most petroleum and chemical companies created safety reviews that asked "What-If" questions of the process (e.g., SOHIO ca. 1967). This was a common practice in the industry and during design phases of a facility but was usually verbal and less formal in application. Because of this there is not as much historical documentation available on it as compared to the HAZOP method.

3.4 LIMITATIONS AND DISADVANTAGES

PHA, What-If, and HAZOP methods all have limitations and advantages. The following is a brief discussion of these.

3.4.1 Limitations

3.4.1.1 Preliminary Hazard Analysis

1. It is based on experience of the team members.

   These reviews usually cannot be relied on for identifying unrecognized hazards. A review team may fail to delve deep enough into the process or the process control with which they have become

superficially familiar. Unless the right questions are asked by the review team, hazards may go unidentified.

2. It is not systematic.

   They are typically considered a brainstorming session. Personnel familiar with the facility discuss aspects in a random fashion, whatever comes to mind. Most PHA or What-If reviews therefore refer to a checklist to overcome this handicap.

3. It is usually applied when limited information is available or may change.

   A PHA is usually conducted early in a project life cycle, usually in the initial conceptual stage or early design phase. Some parts of the project may not be fully defined for an adequate review or the project scope or conceptual design may change significantly during this period.

3.4.1.2 What-If Reviews

1. It is based on experience of team members.

   These reviews usually cannot be relied on for identifying unrecognized hazards. A review team may fail to delve deep enough into the process or the process control with which they have become superficially familiar. This may be true for older team members where new technological control systems have made the application of 25–30 years of experience in older process control methods less relevant (i.e., PLCs versus relays, and analog versus digital). However, experience and insight together will allow the identification of hazard scenarios that are not readily apparent. Unless the right questions are asked by the review team, hazards may go unidentified.

2. It is not systematic.

   They are typically considered a brainstorming session. Personnel familiar with the facility discuss aspects in a random fashion, whatever comes to mind. Most PHA or What-If reviews therefore refer to a checklist to overcome this handicap.

3.4.1.3 HAZOP Reviews

1. It needs a moderate level of skill to implement.

   The review is a thorough and systematic process that has to be conducted in a proper fashion and accurately recorded. In order to perform a HAZOP review, a specialized team leader is typically used to guide the review team during the process. The team leader usually has had specialized training and experience in conducting HAZOP reviews.

2. It may be slower to implement than other methods.

   In order to perform a HAZOP review, a specialized team leader is used to guide the review team through the process. The team leader follows a standard format with special guidewords and deviations that need to be addressed. Because a standardized listing is used for all systems, some unnecessary and unimportant issues may be addressed in some portions of the system under review.

3.4.2 Advantages

3.4.2.1 Preliminary Hazard Analysis

1. It can identify concerns early in the project.

   Because a PHA is usually conducted early in a project life cycle, it can identify concerns early in the project's conceptual stage and avoid costly changes later.
2. It is generally economical.

   The conceptual project stage usually has a limited information base, so that the time/personnel-hours needed to perform the review will not be extensive.

3.4.2.2 What-If Reviews

1. It can be accomplished with a relatively low skill level.

   The typical What-If review is a basic brainstorming session; all sorts of topics may be randomly addressed as they come to mind. Combined with a checklist format, the review may become simple questions to answer.
2. It is fast to implement compared to other qualitative techniques.

   Because the What-If review is a direct question method (possibly from a standardized checklist), the questions can be easily and usually rapidly addressed.
3. It can analyze a combination of failures.

   The option of addressing continuing sequential failures can be investigated to the final outcome.
4. It is flexible.

   It is readily adaptable to any type of process flow or facility. Questions can focus on specific potential failures.

Table 3.1 Comparison of PHA, What-If, and HAZOP Methods

	PHA	What-If	HAZOP
Experienced based	Yes	Yes	No
Systematic	Partially	Partially	Yes
Skill	Low	Moderate–low	Moderate
Speed	Fast	Fast–moderate	Slow
Level of detail	General	Medium specific	Very specific
Relative cost	Moderate–low	Moderate–low	High–moderate
Flexible	Yes	Yes	Yes

3.4.2.3 HAZOP Reviews

1. It uses a systematic and logical approach.

   It has a specific guideword listing and the process under review is subdivided into small sections for analysis.
2. It can analyze a combination of failures.

   The option of addressing continuing sequential failures can be investigated to the final outcome.
3. It provides an insight into operability features.

   Operation control methods are fully investigated for potential varying conditions to the entire process flow. From this review an operator can readily deduct what hazards may be present at the facility (Table 3.1).

CHAPTER 4

Adaptation to Security Vulnerability Analysis

A Security Vulnerability Analysis (SVA) is quite similar to a Process Hazard Analysis (PHA), as they both perform a risk assessment and evaluate the results. An SVA evaluates risk from deliberate acts that could result in major incidents. It is performed in a systematic and methodical manner by a multidisciplined team approach coached by a leader. It analyzes potential threats and evaluates these threats against plant vulnerabilities. From this analysis, it determines possible consequences and whether safeguards to prevent or mitigate their occurrence are recommended. This procedure and documentation is similar in manner to existing PHA methodologies, so that it can be easily adapted into existing programs efficiently and effectively. Sections in this book that describe PHA procedures have been expanded to also include SVA steps. Some consulting companies that offer PHAs have added SVAs to their capabilities due to the similar nature and overlapping objectives. They have easily adapted PHA software to SVAs in order to conduct these reviews. The DHS primarily relies on the methodology of AIChE and Sandia VAM but accepts equivalent methodologies developed in the industry. Current equivalent methodologies specifically identified as acceptable by the DHS are listed next. API has recently issued their own guidance for the analysis of process facility security known as API Standard 780, *Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries*.

- Air Products and Chemicals SVA
- API/NPRA (only for petroleum sites)
- Asmark SVA (only for Ag chemicals distribution)
- Bayer SVA
- BASF SVA
- ExxonMobil SSQRA
- FMC SVA
- Georgia Pacific SHA
- Marathon Ashland Petroleum
- National Paint and Coatings Association (only for paint and coating formulators)
- PPG SVA
- SOCMA (manual method use only)
- SRM (Chemical Extended Version, Straec)
- SVA-Pro by Dyadem

Safety and Security Review for the Process Industries
DOI: http://dx.doi.org/10.1016/B978-0-323-32295-9.00004-5

4.1 COMPARISON TO PHA REVIEWS

All the methodologies utilize what is frequently termed a "Threat Analysis" to identify the "deviations" against protective measures, similar to PHA/What-If questions and guidewords in a HAZOP. These are then applied as through a vulnerability assessment, which is a variation on process intention similar to the PHA. Subsequentially, the consequences are determined and the effectiveness of protective measures evaluated. Where these are considered inadequate, recommendations are recorded to prevent or mitigate the event, similar to PHA reviews. Communication and evaluation are the prime facets of both methodologies.

4.2 SVA OVERALL PROCEDURE

The general steps in the process are:

1. Undertake a Threat Analysis (identifying sources, types, and likelihood of threats).
2. Divide facility in areas and also identify global concerns (to be addressed for the overall facility).
3. Evaluate each credible threat within the process area.
4. Identify vulnerabilities against each threat (brainstorming/checklist approach).
5. Determine the possible consequences.
6. List safeguards against threat scenarios and evaluate if protective measures are adequate.
7. Determine if recommendations are required (ranking of risk can be used to determine necessity).

These steps are easily followed and can be applied at a variety of facilities and operations at varying degree of detail as necessary.

4.3 MAJOR DIFFERENCES BETWEEN SVAS AND PHAS

Although SVAs are similar to PHAs, there are some noted differences that should be realized. The following are major differences:

- A PHA typically evaluates equipment and operator failures, while SVAs evaluate scenarios that originate with deliberate actions.
- An SVA has to identify sources, types, and likelihood of threats, while a PHA has to determine what hazards are to be considered.

- SVAs have to accommodate various threat levels based on current cultural perceptions.
- SVAs rely on or usually involve law enforcement.
- SVAs have to determine if threats are credible, while a PHA has to determine if a failure is credible.
- Safeguards for PHAs may not be applicable for SVAs.
- Likelihood definitions for SVAs (Threat Analyses) are different than likelihood (probabilities) for PHAs.
- SVAs may have to rely on specialty software or security consultants for assurance that the threat of cyberattacks can be prevented or blocked.

4.4 THREAT ANALYSIS NECESSITY

Because exact guidewords or a definitive checklist is not available to cover the complete threat possibilities that may evolve in a PHA, a Threat Analysis is performed as one of the first steps in the SVA. Different methodologies may identify this process by other names (i.e., Consequence and Target Attractiveness), but they all have the same intention. A Threat Analysis is a continuing process of collecting and reviewing all available information concerning potential adversaries that may target an organization or facility. The main information will be related to the existence factors for an adversary's existence, its capabilities, intentions, history, targeting, and the security environment of the target. The technique utilizes a team brainstorming/checklist approach to identifying the threats to be examined and may qualitatively rank the findings to assist in identifying highly credible threats.

CHAPTER 5

Specialized Reviews—CHAZOP, EHAZOP, Bow-Tie Analysis, Layers of Protection Analysis, Safety Integrity Level, Fishbone Diagram, and Cyber Security Vulnerability Analysis

There are several other safety reviews that are sometimes employed within the process industries instead of or to supplement Process Hazard Analysis (PHA), What-If, and HAZOP (Hazard and Operability Study) safety reviews: CHAZOP (Computer Hazard and Operability Study), EHAZOP (Electrical Hazard and Operability Study), Bow-Tie Analysis (BTA), Layers of Protection Analysis (LOPA), Safety Integrity Level (SIL) Analysis, Fishbone Diagram, and Cyber Security Vulnerability Analysis (CSVA). These are briefly described in this chapter.

5.1 COMPUTER HAZARD AND OPERABILITY STUDY

A CHAZOP is a structured study of control and safety systems to assess and minimize the effect of failures of its subsystems impacting the plant or affecting the ability of an operator to take corrective action. It is extrapolated from HAZOP methodology but is specialized for control and safety systems, including appropriate guidewords and parameters; for example, no signal, out-of-range signal, no power, no communication, I/O card failure, software programming incorrect/inadequate, and cyber attack. It covers the entire safety instrumented loops, from the field instrumentation to the relays, PLCs (DCS/SCADA, PSD/ESD, F&G, etc.), I/O cards, circuit breakers, actuators, local control panels, power supply, programming instructions, and so on. The review can be performed for new designs or modification projects, at different project stages such as during Front End Engineering Design (FEED), detailed design, construction, and commissioning.

Safety and Security Review for the Process Industries
DOI: http://dx.doi.org/10.1016/B978-0-323-32295-9.00005-7

5.2 ELECTRICAL HAZARD AND OPERABILITY STUDY

An EHAZOP is a structured study of electrical power systems to assess and minimize potential hazards presented by incapability or failure of an electrical apparatus. It is extrapolated from HAZOP methodology but specialized especially for electrical systems, including appropriate guide-words and parameters such as power surges, 24 VDC supply failure, Uninterruptible Power Supply (UPS) availability, flashover, transformer incident, substation bus bar failure, and lack of maintenance. It covers power generation, transformation, transmission and distribution, load shedding philosophy, UPS, and so on. It can be performed in new designs or modification projects, and at different stages in the project design similar to other HAZOPs.

5.3 BOW-TIE ANALYSIS

A bow-time analysis is a type of qualitative PHA. It is thought that they were originally called "butterfly diagrams" and evolved from the "cause consequence diagram" of the 1970s. However, the Bow-Tie PHA methodology is an adaptation of three conventional system safety techniques: Fault Tree Analysis, Causal Factors Charting, and Event Tree Analysis. Existing safeguards (barriers) are identified and evaluated for adequacy. Additional protections are then determined and recommended where appropriate. Typical cause scenarios are identified and depicted on the pre-event side (left side) of the bow-tie diagram. Credible consequences and scenario outcomes are depicted on the post-event side (right side) of the diagram, and associated barrier safeguards are included (Figure 5.1).

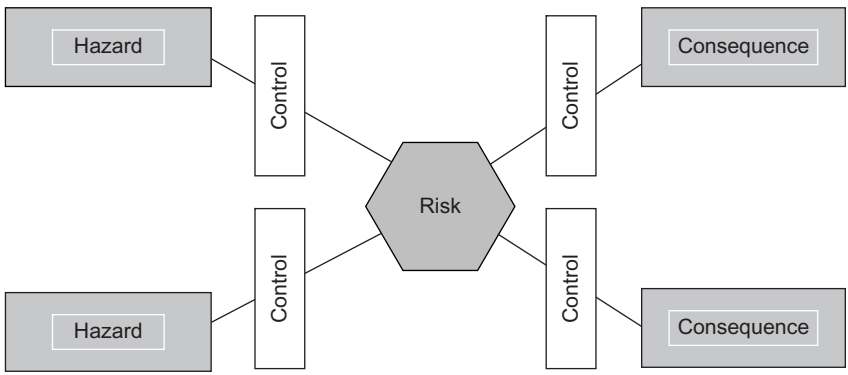

Figure 5.1 BTA arrangements.

BTA has become popular as a structured method to assess risk where a qualitative approach may not be possible or desirable. The success of the diagram is that it is simple and easy for the nonspecialist to understand, especially at all levels of operations and management. The ideal is a simple case of combining the cause (fault tree) and the consequence (event tree). When a fault tree is drawn on the left-hand side and the event tree on the right-hand side with hazard drawn as a "knot" in the middle, the diagram looks like a bow tie and hence its name.

By constructing the BTA diagram, one can simply see how multiple causes with failed preventive controls result in negative consequences. If the "preparedness" control also fails, the risk will occur and have a negative consequence. Mapping risks using the bow tie can provide a sound starting point from which one can ensure controls are actually addressing the real causes and consequences. In the bow-tie review diagram, "preventive controls" are placed at the hazard and "preparedness controls" are placed at the consequence.

Bow-tie reviews are most commonly used where there is a requirement to demonstrate that hazards are being controlled, and particularly where there is a need to illustrate the direct link between the controls and elements of the management system. The bow-tie methodology is an effective way of demonstrating that an organization's risks are reduced to As Low As Reasonably Practical (ALARP), with an overreliance on qualitative risk assessments from the past. The bow-tie methodology is accepted by safety case regulators as a demonstration of ALARP. Controls on the diagrams can also be categorized by the SIL, effectiveness, and other types of controls that may be required.

Bow ties can be also linked to a LOPA in various software packages (e.g., Bow-tieXP), which can provide a semiquantitative estimation of the risk. This is quite powerful as a risk profile can be developed directly from the bow ties that are automatically updated as safeguards are improved, lessons learned from incidents are incorporated, and so forth.

5.4 LAYERS OF PROTECTION ANALYSIS

A LOPA is a method of analyzing the likelihood (frequency) of a harmful outcome event based on an initiating event frequency and on the probability of failure of a series of independent layers of protection capable of preventing the harmful outcome. LOPA lies between the qualitative end of the scale (characterized by methods such as AZOP and What-If) and the quantitative end (characterized by methods using fault trees and event trees) and is therefore sometimes referred to as a semiquantitative review methodology. If additional Risk Reduction (RR) is required after the reduction provided by the process design, the Basic Process Control System (BPCS), alarms and associated operator actions, pressure relief/safety valves, and so on, then a Safety Instrumented Function (SIF) may be required. The SIL of the SIF can be determined directly by the additional RR required. LOPA is a recognized technique for selecting the appropriate SIL of a Safety Instrumented System (SIS) per the requirements of American National Standard Institute (ANSI)/International Society of Automation (ISA)-84.00.01 or IEC 61508. It is typically utilized to determine if a SIF is necessary and if it is the correct choice of RR. LOPA is the preferred method for determining what SIL is necessary, if a SIF is chosen as the RR method.

LOPA originated internally within individual companies in the late 1990s. The first book on LOPA was published by the CCPS in 2001 after which it became widely applied in the process industries.

The method starts with the data developed in the HAZOP analysis and accounts for each identified hazard by documenting the "initiating cause" and the Protection Layers (PLs) that prevent or mitigate the hazard. The total amount of RR can then be determined and the need for more RR analyzed. Specifically, the LOPA estimates the probability of the undesired consequence of failure by multiplying the frequency of initiating events by the product of the probabilities of failure for the applicable PLs. The severity of the consequences and the likelihood of the

occurrence are then assigned a probability, usually by reference to a standard table.

The determination of this value is called a mitigated consequence frequency and is compared to the organization's risk acceptance criteria. For the LOPA to be acceptable, the independence between initiating events and layers of protection and between separate layers of protection must be demonstrated.

PLs that perform their function with a high degree of reliability may qualify as Independent Protection Layers (IPLs).

The criteria to qualify a PL as an IPL are as follows:

- The protection provided reduces the identified risk by a large amount, typically a minimum of a tenfold reduction.
- The protected function is provided with a high degree of availability (90% or greater).
- The IPL has the following important characteristics:
  - **a.** *Specificity*: An IPL is designed solely to prevent or to mitigate the consequences of one potentially hazardous event (e.g., runaway reaction, release of toxic material, loss of containment, fire, and explosion). Multiple causes may lead to the same hazardous event and, therefore, multiple event scenarios may initiate the action of the one IPL.
  - **b.** *Independence*: An IPL is independent of the other PLs associated with the identified danger.
  - **c.** *Dependability*: It can be counted on to perform what it was designed to accomplish. Both random and systematic failure modes are addressed in the design.
  - **d.** *Auditability*: It is designed to facilitate regular validation of the protective functions. Proof testing and maintenance of the safety systems are necessary.

The typical "layers of protection" that are usually identified and provided for industrial process facilities are as follows:

- The basic process design
- Basic process control and alarms along with operator management of these systems (Note: alarms are usually to be less than 280 per console operator per day, with written procedures for alarm response actions)
- Critical process alarms along with operator management and intervention if necessary
- Automatic SIS
- Physical process protection devices; for example, relief/flare systems