



ENGLISH

DOE-HDBK-1100-2004
August 2004
Superseding
DOE-HDBK-1100-96
February 1996

DOE HANDBOOK

CHEMICAL PROCESS HAZARDS ANALYSIS



U.S. Department of Energy
Washington, D.C. 20585

AREA SAFT

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

This document has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from the ES&H Technical Information Services, U.S. Department of Energy, (800) 473-4375, fax: (301) 903-9823.

Available to the public from the U.S. Department of Commerce, Technology Administration, National Technical Information Service, Springfield, VA 22161; (703) 605-6000.

FOREWORD

The Office of Health (EH-5) under the Assistant Secretary for the Environment, Safety and Health of the U.S. Department of Energy (DOE) has published two handbooks for use by DOE contractors managing facilities and processes covered by the Occupational Safety and Health Administration (OSHA) Rule for Process Safety Management of Highly Hazardous Chemicals (29 CFR 1910.119), herein referred to as the PSM Rule. The PSM Rule contains an integrated set of chemical process safety management elements designed to prevent chemical releases that can lead to catastrophic fires, explosions, or toxic exposures. The purpose of the two handbooks, "Process Safety Management for Highly Hazardous Chemicals" and "Chemical Process Hazards Analysis," is to facilitate implementation of the provisions of the PSM Rule within the DOE.

The purpose of this handbook is to facilitate, within the DOE, the performance of chemical process hazards analyses (PrHAs) as required under the PSM Rule. It provides basic information for the performance of PrHAs, and should not be considered a complete resource on PrHA methods. Likewise, to determine if a facility is covered by the PSM rule, the reader should refer to the handbook, "Process Safety Management for Highly Hazardous Chemicals" (DOE-HDBK-1101-2004).

Promulgation of the PSM Rule has heightened the awareness of chemical safety management issues within the DOE. This handbook is intended for use by DOE facilities and processes covered by the PSM rule to facilitate contractor implementation of the PrHA element of the PSM Rule. However, contractors whose facilities and processes not covered by the PSM Rule may also use this handbook as a basis for conducting process hazards analyses as part of their good management practices.

This handbook explains the minimum requirements for PrHAs outlined in the PSM Rule. Nowhere have requirements been added beyond what is specifically required by the rule.

ACKNOWLEDGEMENTS

The U.S. Department of Energy (DOE) wishes to thank all persons who commented on this handbook for their help in clarifying and focusing this guidance. Ms. Pamela Sutherland of Battelle-Columbus managed the preparation of this handbook by Battelle Memorial Institute staff in Columbus and at Pacific Northwest Laboratories (PNL).

TABLE OF CONTENTS

	<u>Page</u>
FOREWORD.....	iii
ACKNOWLEDGEMENTS	iv
LIST OF TABLES	vii
LIST OF FIGURES.....	viii
ACRONYMS	ix
GLOSSARY.....	x
1.0 INTRODUCTION.....	1
2.0 OVERVIEW OF REQUIREMENTS FOR PROCESS HAZARD ANALYSIS	
UNDER THE PSM RULE	3
2.1 Process Safety Information.....	3
2.2 Process Hazard Analysis	4
3.0 ESSENTIAL ELEMENTS OF PROCESS HAZARD ANALYSIS	7
3.1 Step-by-Step Procedure	7
3.2 Elements Common To All Process Hazard Analyses	11
3.3 Presentation of Results	22
4.0 PROCESS HAZARD ANALYSIS METHODS WITH EXAMPLES	23
4.1 Checklist Analysis.....	23
4.2 What-If Analysis	30
4.3 What-If/Checklist Analysis	36
4.4 Hazard and Operability Study	44
4.5 Failure Mode and Effects Analysis	52
4.6 Fault Tree Analysis	59
5.0 REPORTING AND REVIEW OF ANALYSES	66
5.1 Reporting the Process Hazard Analysis	66
5.2 Review of the Process Hazard Analysis.....	68
6.0 ESTABLISHING A SYSTEM FOR RESOLVING ACTION ITEMS	
AND IMPLEMENTING CORRECTIVE ACTIONS	71
6.1 Process Hazard Analysis Action Items and Recommendations	71
6.2 Criteria for Corrective Actions and Safety Improvements.....	71
6.3 The Corrective Actions System.....	72

7.0	UPDATING THE PROCESS HAZARD ANALYSIS	73
7.1	Update Team	73
7.2	Approach	73
7.3	Documentation	73
8.0	RELATIONSHIPS OF PROCESS HAZARD ANALYSES TO OTHER DOE REQUIRED HAZARD ANALYSES	74
9.0	REFERENCES	76

LIST OF TABLES

	<u>Page</u>
Table 3.1. Process Hazards.....	13
Table 3.2. Checklist for Worker Exposures	18
Table 3.3. Checklist of Facility Siting Issues.....	19
Table 3.4. Example Human Factors in Process Operations	21
Table 4.1. Simplified Process Hazards Analysis Checklist.....	27
Table 4.2. Main Headings of Well's Checklist.....	28
Table 4.3. Main Headings of Baleman's Checklist	29
Table 4.4. Approximate Checklist Analysis Time Requirements	30
Table 4.5. Checklist Analysis of Dock 8 HF Supply System.....	32
Table 4.6. Checklist Analysis of Cooling Water Chlorination System.....	33
Table 4.7. Typical Format for a What-If Analysis Worksheet.....	35
Table 4.8. Approximate Time Requirements for What-If Analyses	35
Table 4.9. What-If Analysis of Dock 8 HF Supply System	38
Table 4.10. What-If Analysis of Cooling Water Chlorination System	40
Table 4.11. Approximate What-If/Checklist Analysis Time Requirements	41
Table 4.12. What-If/Checklist Analysis of Dock 8 HF Supply System.....	42
Table 4.13. What-If/Checklist Analysis of Cooling Water Chlorination System	43
Table 4.14. Guide Words for HAZOP Studies.....	45
Table 4.15. Example HAZOP Study Process Parameters and Deviations	46
Table 4.16. Typical Format for a HAZOP Study Worksheet.....	48
Table 4.17. Time Estimates for Using the HAZOP Study Method.....	49
Table 4.18. Example HAZOP Study for the Dock 8 HF Supply System.....	50
Table 4.19. Example HAZOP Study for the Cooling Water Chlorination System.....	51
Table 4.20. Example FMEA Worksheet	56
Table 4.21. Time Estimates for Using the Failure Mode and Effects Analysis Method.....	57
Table 4.22. Partial FMEA for the Dock 8 HF Supply System.....	58
Table 4.23. Partial FMEA for the Cooling Water Chlorination System	59
Table 4.24. Fault Tree Symbols	61
Table 4.25. Minimal Cutset Documentation	63
Table 4.26. Time Estimates for Using the Fault Tree Analysis Method.....	63
Table 5.1. Deviations Guide.....	69

LIST OF FIGURES

	<u>Page</u>
Figure 3.1. Process Hazard Analysis Task Structure	9
Figure 3.2. Example Interaction Matrix for Identifying Process Hazards	15
Figure 3.3. Anatomy of an Accident	17
Figure 4.1. Dock 8 HF Supply System.....	24
Figure 4.2. Cooling Water Chlorination System.....	25
Figure 4.3. Example FTA for the Dock 8 HF Supply System	64
Figure 4.4. Example FTA for the Cooling Water Chlorination System.....	65

ACRONYMS

ANSI	American National Standards Institute
API	American Petroleum Institute
ASME	American Society of Mechanical Engineers
ASTM	American Society for Testing and Materials
CCPS	Center for Chemical Process Safety
DOE	U.S. Department of Energy
DOT	U.S. Department of Transportation
ERPG	Emergency Response Planning Guideline
EVC	Equilibrium Vapor Concentration
FTAP	Fault Tree Analysis Program
FMEA	Failure Mode and Effects Analysis
HAZOP	Hazard and Operability
HHC	Highly Hazardous Chemical
IDLH	Immediately Dangerous to Life or Health
IRRAS	Integrated Reliability and Risk Analysis System
IEEE	Institute of Electrical and Electronic Engineers
ISA	Instrument Society of America
JHA	Job Hazard Analysis
LFL	Lower Flammability Limit
M&O	Management and Operation
MCS	Minimal Cut Set
MOC	Management of Change
MSDS	Material Safety Data Sheet
NFPA	National Fire Protection Association
ORC	Organization Resources Counselors
ORR	Operational Readiness Review
OSHA	Occupational Safety and Health Administration
P&ID	Piping and Instrumentation Diagram
PEL	Permissible Exposure Limit
PHA	Preliminary Hazards Analysis
PrHA	Process Hazard Analysis
PSI	Process Safety Information
PSM	Process Safety Management
PSR	Pre-Startup Safety Review
SAR	Safety Analysis Report
SHI	Substance Hazard Index
SOP	Standard Operating Procedure
TLV	Threshold Limit Value
TQ	Threshold Quantity
UFL	Upper Flammability Limit

GLOSSARY

Accident, Accident Event Sequence

An unplanned event or sequence of events that has an undesirable consequence.

Aggregate Threshold Quantity

The total amount of a hazardous chemical contained in vessels that are interconnected, or contained in a process and nearby unconnected vessels, that may be adversely affected by an event at that process.

Catastrophic Release

A major uncontrolled emission, fire, or explosion, involving one or more highly hazardous chemicals that presents serious danger to employees in the workplace or to the public.

Employee

Under 29 CFR 1910.119, "Process Safety Management of Highly Hazardous Chemicals," an hourly, salaried, or contract person who works at a facility and comes in direct contact with a covered process.

Event

An occurrence involving process, equipment, or human performance either internal or external to a system that causes system upset. In terms of accidents, an event is either a cause or a contributing cause of a "near miss" or accident, or a response to the accident initiating event.

Facility

The buildings, containers, or equipment that contain a chemical process.

Flammable Gas

A gas that, at ambient temperature and pressure, forms a flammable mixture with air at a concentration of 13 percent by volume or less; or a gas that, at ambient temperature and pressure, forms a range of flammable mixtures with air wider than 13 percent by volume, regardless of the lower limit.

Flammable Liquid

Liquid with a flash point below 100 deg F (37.8 °C), except mixtures where such liquids account for 1 percent or less of the total volume.

Hazard

A chemical property, energy source, or physical condition that has the potential to cause illness, injury, or death to personnel, or damage to property or to the environment, without regard for the likelihood or credibility of potential accidents or the mitigation of consequences.

Highly Hazardous Chemical

Toxic, reactive, flammable, or explosive substances, as defined in Appendix A of 29 CFR 1910.119, "Process Safety Management of Highly Hazardous Chemicals."

Incident

An unplanned event that may or may not result in injuries and/or loss.

Near Miss

An event that did not result in an accidental release of a highly hazardous chemical, but which could have, given another "failure." Near misses, sometimes called "precursors," include:

- the occurrence of an accident initiator where the protection functioned properly to preclude a release of a highly hazardous chemical; or,
- the determination that a protection system was out of service such that if an initiating event had occurred, a release of a highly hazardous chemical would have taken place.

Normally Unoccupied Remote Facility

A facility that is operated, maintained, or serviced by workers who visit the facility only periodically to check its operation and to perform necessary operating or maintenance tasks. No workers are regularly or permanently stationed at the facility. Such facilities are not contiguous with, and must be geographically remote from, all other buildings, processes, or persons. If workers spend more than 1 hour at a facility each day, that, facility is not considered to be normally unoccupied.

Probability

An expression of the expected likelihood of occurrence of an event or event sequence during an interval of time, or the likelihood of the success or failure of an event on test or on demand. By definition probability must be expressed as a number ranging from 0 to 1.

Process

Any onsite activity that involves a highly hazardous chemical, including any use, storage, manufacturing, handling, or movement of a highly hazardous chemical, or combination of these activities. Any interconnected group of vessels is considered a single process. Vessels with no physical interconnections located such that an accident in one vessel could spread to adjacent vessels are considered a single process.

Process Hazard

An inherent chemical or physical characteristic with the energy potential for damaging people, property, and/or the environment.

Process Hazards Analysis (PrHA)

The application of one or more analytical methods to identify and evaluate process hazards for the purpose of determining the adequacy of or need for control measures.

Process Safety Management

The application of management principles, methods, and practices to prevent and control accidental releases of process chemicals or energy.

PSM Rule

The Occupational Safety and Health Administration's rule "Process Safety Management of Highly Hazardous Chemicals," 29 CFR 1910.119.

Risk

The quantitative or qualitative expression of possible loss that considers both the probability that a hazard will result in an adverse event and the consequences of that event.

Threshold Quantity

As defined in 29 CFR 1910.119, the minimum amount of a toxic, reactive, or flammable chemical judged by OSHA as capable of causing a catastrophic event. The threshold quantity triggers application of the rule's requirements.

1.0 INTRODUCTION

On February 24, 1992, the Occupational Safety and Health Administration (OSHA) released a revised 29 CFR Part 1910 that added Section 1910.119, "Process Safety Management of Highly Hazardous Chemicals; Explosives and Blasting Agents," to protect employees by preventing or minimizing the consequences of chemical accidents. This regulation, hereafter referred to as the PSM Rule, prescribes a total safety management program with 14 defined elements. DOE O 440.1, WORKER PROTECTION MANAGEMENT FOR DOE FEDERAL AND CONTRACTOR EMPLOYEES, requires that covered chemical processes within DOE comply with the PSM Rule. In June 2004 the DOE sent the Office of Management and Budget, DRAFT 10 CFR 851 "Worker Safety and Health" for subsequent publication in the Federal Register as the new DOE Worker Safety and Health Rule. This new Rule will require contractors to follow all applicable portions of 29 CFR 1910. Guidance for implementing the PSM Rule is provided in "Process Safety Management for Highly Hazardous Chemicals" (DOE-HDBK-1101-2004).

One of the most important elements of the PSM Rule is the process hazard analysis (PrHA)¹. It requires the systematic identification of hazards and related accident scenarios. The PSM Rule allows the use of different analysis methods, but the selected method must be based on the process being analyzed. The PrHA and the other PSM elements must be in place prior to process startup. PrHAs must be reviewed and updated at least every 5 years.

This handbook should be considered basic information for the required PrHA element, not a complete resource on PrHA methods. Summary descriptions and basic step-by-step instructions are provided. However, existing references, which are identified in each section, provide additional insight and should be used. The primary reference should be Guidelines for Hazard Evaluation Procedures (CCPS, 1992). IN addition, resources from relevant professional organizations should be used on a continuing basis to maintain competence in PrHA. These resources include books and publications, technical meetings, and continuing education. Each DOE facility that stores or uses hazardous chemicals in above-threshold quantities is required to have staff knowledgeable in PrHA. At least one member of the PrHA team must be knowledgeable in the specific process methodology being used.

1. To those already familiar with hazard/risk analysis methods, a "PHA" designates a Preliminary Hazard Analysis. Unfortunately, the PSM Rule uses these same letters to designate Process Hazard Analysis. In this document, PrHA will designate Process Hazard Analysis to avoid confusion with Preliminary Hazard Analysis. Note that other literature may be confusing on this issue.

This Page Intentionally Left Blank

2.0 OVERVIEW OF REQUIREMENTS FOR PROCESS HAZARD ANALYSIS UNDER THE PSM RULE

Under the PSM Rule, the PrHA element requires the selection and application of appropriate hazard analysis methods to systematically identify hazards and potential accident scenarios associated with highly hazardous chemicals. The components of a PrHA are summarized and explained below.

2.1 Process Safety Information

The PSM Rule requires that up-to-date process safety information exist before conducting a PrHA, with the exception of technology information that can be created in conjunction with the PrHA. Complete and accurate written information about process chemicals, technology, and equipment is essential to the team that performs a PrHA. It is also needed by personnel developing training programs and operating procedures, subcontractors whose employees work with the process, teams conducting pre-startup reviews, and local emergency preparedness planners.

2.1.1 Information About Highly Hazardous Process Chemicals

Information about the chemicals used in a process, as well as chemical intermediates, must be comprehensive enough for an accurate assessment of fire and explosion characteristics, reactivity hazards, safety and health hazards to workers, and corrosion and erosion effects on process equipment and monitoring tools. Information must include, at a minimum: (1) toxicity information; (2) permissible exposure limits; (3) physical data such as boiling point, freezing point, liquid/vapor densities, vapor pressure, flash point, autoignition temperature, flammability limits (LFL and UFL), solubility, appearance, and odor; (4) reactivity data, including potential for ignition or explosion; (5) corrosivity data, including effects on metals, building materials, and organic tissues; (6) identified incompatibilities and dangerous contaminants; and (7) thermal data (heat of reaction, heat of combustion). Current Material Safety Data Sheets (MSDSs) may be used to help meet this requirement. Where applicable, process chemistry information should be included about potential runaway reactions and overpressure hazards and hazards arising from the inadvertent mixing of incompatible chemicals.

2.1.2 Information About Process Technology

Process technology information must include at least: (1) block flow diagrams or simplified process flow diagrams such as the type shown in Figure 4.1; (2) process chemistry; (3) DOE contractor-established criteria for maximum inventory levels for process chemicals; (4) process limits that, when exceeded, are considered an upset condition; and (5) qualitative estimates of the consequences of deviations that could occur if established process limits are exceeded. If the original technology information is not available, it can be created in conjunction with the PrHA.

Block flow diagrams may be used to show major process equipment and interconnecting process flow lines, flow rates, stream composition, temperatures, and pressures. When necessary for completeness, process flow diagrams should be used to show all main flow streams including valves; pressures and temperatures on all feed and product lines within all major vessels; and points of pressure and temperature control. Construction materials, pump capacities, pressure heads, compressor horsepower, and vessel design pressures and temperatures are shown when necessary for clarity. Major components of control loops are usually shown along with key utilities. Piping and instrumentation diagrams (P&IDs), which are required under process equipment information, may be more appropriate to show some of these details.

2.1.3 Information About Process Equipment

Process equipment information must include at least: (1) materials of construction; (2) P&IDs; (3) electrical classification; (4) relief system design and design basis; (5) ventilation system design; (6) design codes and standards; (7) material and energy balances for processes ; and (8) safety systems.

Process equipment design and materials must be documented by identifying the applicable codes and standards (e.g., ASME, ASTM, API). If the codes and standards are not current, the DOE contractor must document that the design, construction, testing, inspection, and operation are still suitable for the intended use. If the process technology requires a design that departs from the applicable codes and standards, the contractor must document that the design and construction are suitable for the intended purpose.

2.2 Process Hazard Analysis

A PrHA is an organized and systematic method to identify and analyze the significance of potential hazards associated with processing or handling highly hazardous chemicals. A PrHA helps employers and workers to make decisions for improving safety and reducing the consequences of unwanted or unplanned releases of hazardous chemicals. It is used to analyze potential causes and consequences of fires, explosions, releases of toxic or flammable chemicals, and major spills of hazardous chemicals. It focuses on equipment, instrumentation, utilities, routine and non-routine human actions, and external factors that might impact a process.

The PSM Rule specifies that a PrHA be performed on every process covered under the rule. If several processes require PrHAs, the PrHAs must be prioritized. A preliminary hazard analysis (PHA) may be used to determine and document the priority order for conducting PrHAs. At a minimum, the PSM Rule requires the prioritization to consider the potential severity of a chemical release, the number of potentially affected employees, and the operating history of the process, including the frequency of past chemical releases and the age of the process.

2.2.1 Schedule

Covered chemical processes must comply with the following:

- The PrHA must be in place prior to process startup.
- Each PrHA must be updated and revalidated at least every 5 years to assure that it is consistent with the current process.

2.2.2 Scope

To help assure that all hazards are identified and evaluated, PrHAs must address the following.

- The hazards of a process. These hazards may be identified by performing a PHA.
- Previous incidents that had the potential for catastrophic consequences in the workplace.
- Engineering and administrative controls applicable to the hazards and their interrelationships.
- The consequences of failure of engineering and administrative controls.
- The influence of facility siting.
- Human factors.
- A qualitative range of possible safety and health effects on employees in the workplace caused by failure of controls.

2.2.3 Team

PrHAs must be performed by a team. Teams can vary in size and in operational background, but must have expertise in engineering and process operations. Individuals may be full-time team members or may be part of a team for only a limited time. That is, team members may be rotated according to their expertise in the part of the process being reviewed.

The team conducting a PrHA must understand the method being used. In addition, one member of the team must be fully knowledgeable in the implementation of the PrHA method.² The PSM Rule also requires that at least one team member be an "employee" with experience and knowledge specific to the process being evaluated. Some organizations have interpreted the term "employee" to mean an hourly employee such as a senior operator.

The ideal PrHA team has an intimate knowledge of the standards, codes, specifications, and regulations applicable to the process. Team members must be compatible, and the team leader must be able to manage the team and the study.

2. OSHA does not specify that the team leader be the member of the team who is knowledgeable in the implementation of the PrHA method.

2.2.4 Findings and Recommendations

DOE contractors should establish a system to:

- promptly address the team's findings and recommendations;
- assure that recommendations are resolved in a timely manner and that resolutions are documented;
- document actions to be taken;
- develop a written completion schedule for the action steps;
- complete actions as soon as possible;
- communicate the actions to all affected personnel.

DOE contractors must retain PrHAs and updates for each process covered by the PSM Rule, along with documented resolutions of recommendations, for the life of the process.

2.2.5 Acceptable Methodology

The PSM Rule specifies that DOE contractors use one or more of the following methodologies, as appropriate, to determine and evaluate the hazards of the process being analyzed:

- What-If
- Checklist
- What-If/Checklist
- Hazard and Operability Study
- Failure Mode and Effects Analysis
- Fault Tree Analysis
- An appropriate equivalent methodology.

3.0 ESSENTIAL ELEMENTS OF PROCESS HAZARD ANALYSIS

This section addresses topics common to all PrHA methods. A step-wise procedure for conducting a PrHA according to PSM Rule requirements is presented, followed by recommended approaches for analyzing scenarios, deciding on action items, and incorporating facility siting and human factors into the PrHA.

3.1 Step-by-Step Procedure

This section describes the tasks required for compliance with the PSM Rule regardless of the PrHA method selected. The sequence of these tasks is shown in Figure 3.1. This figure also indicates where process safety information (PSI) requirements fit into PrHA tasks, and what documents are generated as a result of each task. Concepts common to all PrHA methods are also discussed.

To conduct an effective PrHA, both operating management and the PrHA team must understand their respective responsibilities. In general, the tasks breakdown as follows:

TASK	RESPONSIBILITY
A - F	Operating management
G, H, I	PrHA team
J, K	Operating management and PrHA team

TASK A: LIST PROCESSES THAT ARE COVERED. Identify all onsite processes having threshold quantities (TQs) or more of the highly hazardous chemicals (HHCs) listed in the PSM Rule, 29 CFR 1910.119 (Appendix A)³. Be specific about the boundaries of each "process." Assure that they include all connected vessels and equipment whose upset could result in a release of HHCs from a location remote from the bulk quantity. The DOE hotline for OSHA questions and concerns (1-800-292-8061) may help regarding the applicability of the PSM Rule to a given process or the necessary boundaries of a process.

TASK B: RANK THE PROCESSES BY RISK AND DEVELOP A SCHEDULE OF PrHAS. If a chemical facility contains more than one process covered by the PSM Rule, the rule requires that processes posing the greatest risk to workers be analyzed first. A methodology for ranking is not specified, but any method chosen must account for (1) the extent of the process hazards; (2) the number of potentially affected employees; (3) the age of the process; and (4) the operating history of the process. The following factors should be considered when selecting a ranking methodology: ease of application, qualitative versus semi-quantitative (order of magnitude) results, manpower required, and traceability. After a prioritized list of processes is developed, a schedule for PrHAs can be established.

3. Although not required under the PSM Rule, DOE contractors may want to consider performing PrHAs on processes using large volumes of hazardous chemicals that do not appear in the Appendix A list. In addition, contractors may want to consider conducting PrHAs on processes containing/using quantities of listed HHCs that are just below TQ requirements for coverage under the PSM Rule.

TASK C: SELECT A PrHA METHOD FOR EACH PROCESS. Paragraph (e)(2) of the PSM Rule implies that it is the responsibility of the DOE contractor to select the review method, not the choice of the team conducting the review. In some cases, a combination of methods may be used.

TASK D: ESTIMATE THE MANPOWER REQUIRED AND DEVELOP A STAFFING PLAN. The manpower required to conduct a PrHA depends on many factors, including the review method selected, the training and experience of the review team, the extent and complexity of the process, its instrumentation and controls, and whether the process is a procedure-oriented operation (such as a batch reaction) or a continuous operation (such as petroleum refining). In addition, reviews and updates of existing PrHAs tend to be less time consuming than initial analyses. Guidance for estimating PrHA time requirements is given for each review method in Sections 4.1 to 4.6.

Based on the analysis methods selected in Task C, the status of existing PrHAs, and the time requirements for the methods reviewed in Sections 4.1 to 4.6, the manpower requirements for PrHAs, and reviews and updates, can be estimated. Comparing these requirements with available personnel indicates where additional staffing may be needed, either on a temporary or longer-term basis.

TASK E: SELECT A PROCESS TO BE ANALYZED. This selection should be straightforward: the process to be analyzed should be the process highest on the prioritized list (Task B). If there are exceptions, justifications should be carefully documented. For example, if the highest process on a prioritized list has some significant process changes planned, it may be reasonable to analyze the process being modified along with its proposed changes.

TASK F: ASSEMBLE THE PrHA TEAM AND TRAIN THE TEAM MEMBERS. Regardless of the method selected, the PSM Rule requires all PrHAs to be performed by a team. This team is an ad hoc committee, formed solely to conduct a PrHA for an assigned process. It is disbanded after the analysis, including documentation, has been completed.

The review team must have expertise in engineering and process operations, and at least one team member must have experience and knowledge specific to the process being evaluated. If the process is a new design, the experience requirement may be satisfied by bringing in a person from a sister plant or from a similar or precursor process. In addition, at least one member of the team must be knowledgeable in the hazard analysis methodology being used (see note at the end of Section 1.0).

All team members should be familiar with PrHA objectives, the PrHA method to be used, and their roles in performing the PrHA. A 1- or 2-hour overview at the beginning of the first team

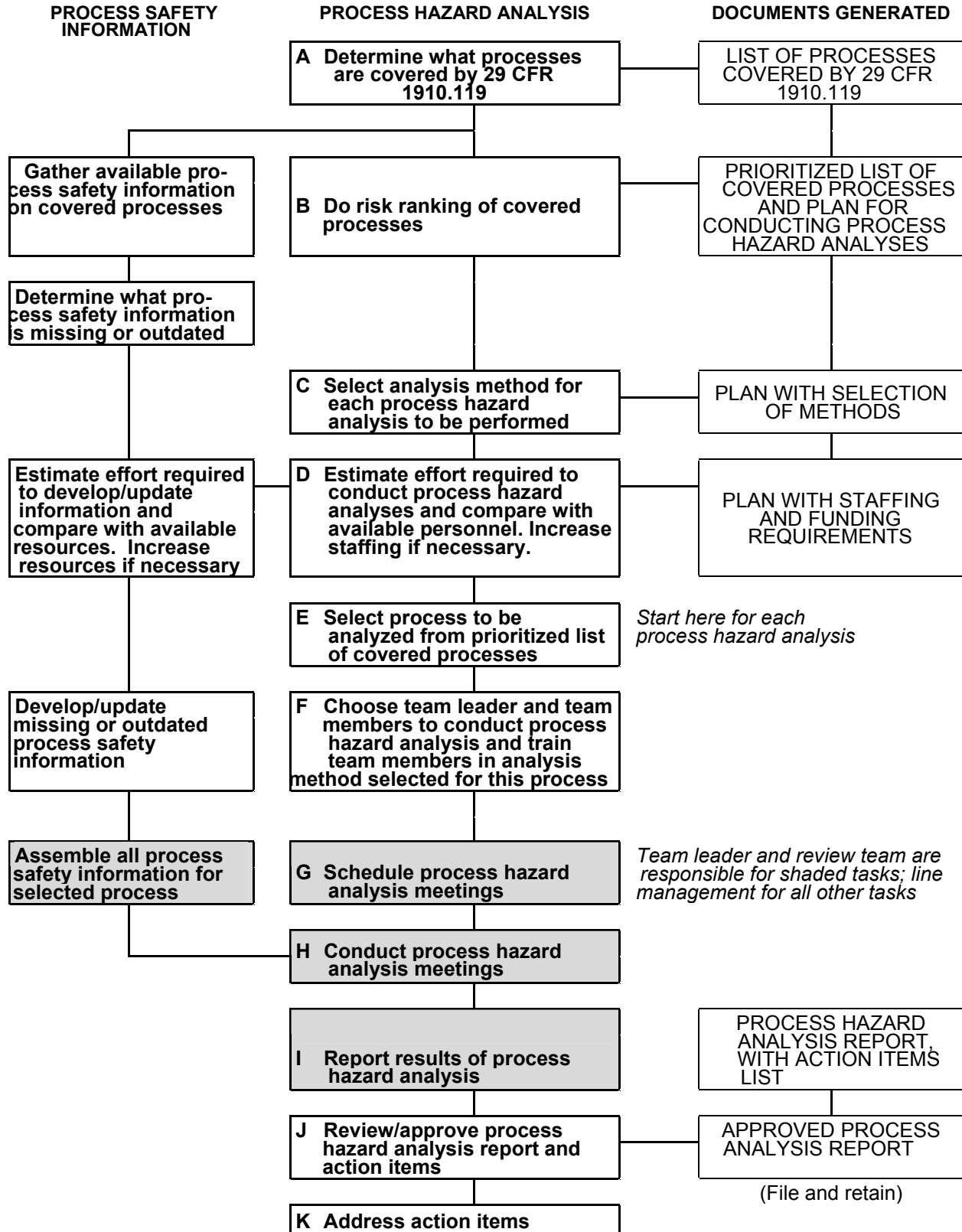


Figure 3.1 Process Hazard Analysis Task Structure

review session is generally sufficient for this purpose. However, the more demanding PrHA methods, such as fault tree analysis (FTA), require more training and/or a greater depth of experience than less-rigorous methods, such as what-if and checklist analyses.

TASK G: SCHEDULE THE PrHAs. To assure full participation by all team members, the team leader should set up a meeting schedule that is realistic but as condensed as possible to provide a concentrated, focused analysis.

A typical schedule is 1 to 3 days per week, with the team meeting 4 to 6 hours per day, until the analysis is completed. The involvement of remote site personnel and/or consultants may necessitate an even more ambitious schedule. However, the efficiency of the team tends to decline if there are more than three, 6-hour meetings per week.

The team leader must devote additional time outside of team meetings for meeting preparation and documentation. Preparation, such as assembling pertinent documents and deciding how each review is approached, may take 8 to 12 hours per P&ID. Documentation typically takes another 8 hours per P&ID.

TASK H: CONDUCT THE PrHA. PrHAs are conducted after all up-to-date process safety information is assembled and the team members are appropriately trained. The team should walkdown the process and facility immediately prior to the analysis, to have the process fresh in mind and to get a sense of the scale and orientation of the process, the surrounding facilities, and the location of operating and co-located personnel.

A description of PrHA methods is given in Section 4 of this document. Keys to successful PrHAs are full preparation, punctuality, focused discussions, careful evaluation of each scenario for risk to onsite and offsite persons, and documentation of the analysis as soon as possible after each team meeting.

TASK I: REPORT THE ANALYSIS RESULTS. The PrHA report documents the scope, approach, identified hazards, analyzed scenarios, and action items resulting from the PrHAs. The report should receive close scrutiny, both for compliance with the PSM Rule and for explanations of each action item. Guidance for reporting the PrHA results are given in Section 5.1.

TASK J: APPROVE THE REPORT AND ACTION ITEMS. The PrHA team should present its findings to operating management when the draft report is complete. Operating management may wish to ask questions about the analysis or have a debriefing meeting on ways to improve the PSM program. The team should then finalize the report. The approval of the final PrHA report by operating management is a commitment by management to implement all action items. Section 5.2 addresses the PrHA review process.

TASK K: ADDRESS THE ACTION ITEMS. All action items must be addressed by operating management, and their resolutions must be documented. Corrective actions and safety improvements approved by management must be fully implemented in a timely manner. Timeliness can be assured by assigning responsibilities and completion dates to all action items

and establishing a tracking system to monitor implementation. Computer spreadsheets and databases have been used successfully for this purpose. Operating management should review all open corrective action items and activities on a regular basis, such as quarterly. Establishing a system for resolving action items and safety recommendations is discussed in Section 6.

3.2 Elements Common To All Process Hazard Analyses

This section presents "how-to" approaches for subjects common to all PrHA methods. The PSM Rule requires that every PrHA include these activities.

- Identify process hazards.
- Review previous incidents.
- Analyze engineering and administrative controls and consequences of control failures.
- Consider facility siting.
- Address human factors.
- Evaluate effects of incidents on employees.
- Decide when action items are warranted.

3.2.1 Identify Process Hazards

A *process hazard* is an inherent chemical or physical characteristic with the energy potential for damaging people, property, and/or the environment. The key word in this definition is *potential*. In a process or system, hazards are not always obvious. Energy may be stored in many different forms, including chemical (reactivity, flammability, corrosivity, toxicity), mechanical (kinetic, potential) and thermal.⁴ Hazards exist whenever a system is above or below an ambient energy level, regardless of how the energy is stored. For example, for the process parameter of pressure, the ambient condition is atmospheric pressure. The higher the system pressure is above atmospheric, the greater the stored energy and the greater the hazard. A system pressure below atmospheric (i.e., a vacuum) can also pose hazards, such as the potential for collapse of a storage tank.

Table 3.1 presents a list of hazards commonly found in process operations, grouped according to how energy is stored. It can be used as a starting point to develop a checklist for identifying process hazards. However, the list is not exhaustive. Thus, a PrHA team may have to augment it as they consider the unique hazards of the process they are analyzing.

The following five steps should be taken to help identify hazards:

4. Nuclear energy, another source of hazards at DOE facilities, is not addressed in this document.

1. List all obvious hazards. Most processes include a number of hazards that are already fully recognized, such as the flammability of propane or the inhalation toxicity of chlorine.
2. Examine the hazardous characteristics of each process chemical. Review the MSDSs, which should have information on the toxicity, flammability, and reactivity of process chemicals and on their incompatibilities with other materials.
3. Examine all process parameters. Parameters (e.g., pressure, temperature, flow rate, level, pH) that are controlled or measured in a process are good indicators of possible process hazards. Process parameters should be examined for all modes of operation, independent of process chemicals, because some hazards exist that do not involve the chemicals. For example, if a process uses high-pressure steam, then both thermal energy and pressure-volume energy hazards exist even though steam is non-toxic, non-flammable, and non-reactive with most materials.
4. Examine material interactions for incompatibilities. Even if process chemicals are relatively non-hazardous when considered independently, some potentially dangerous interactions may occur when materials are combined. Interactions between process chemicals, containment materials, or other materials with which the chemicals come in contact can be examined in pairs by using an interaction matrix. A sample matrix is shown in Figure 3.2.
5. Document the identified hazards. The PrHA report should list identified hazards in tabular form and/or discuss each hazard briefly in the text. Doing both is preferred. New or previously unidentified hazards should receive particular attention and discussion.

3.2.2 Analyze Process Hazards by Developing Accident Scenarios

The parts of an accident event involving a process operation are shown in Figure 3.3. Each sequence of failures and conditions leading to an accident is a unique scenario. Every accident scenario starts with an *initiating event* or *cause*, which is a mechanical failure, operational error, external event, or other condition that causes normal operation to be interrupted or changed. Initiating events can lead to process *deviations*. For example, failure of a cooling water pump (initiating event) may result in loss of cooling to a process involving an exothermic reaction. A deviation occurs when the process temperature exceeds the upper limit of the normal operating temperature for the reaction

Table 3.1 Processing Hazards

FORM OF ENERGY	ASSOCIATED HAZARD(S)	TYPICAL ACCIDENTAL EVENT(S)
CHEMICAL ENERGY	Ability to self-polymerize	Uncontrolled polymerization
	Shock-sensitivity	Detonation of solid or liquid explosive or explosive mixture
	Thermal instability	Thermal explosion following bulk self-heating and runaway reaction
	Rearranging ability	Uncontrolled rearrangement reaction (e.g., ethylene oxide)
	Pyrophoricity	Fire upon atmospheric contact
	Flammability	Vessel/enclosure rupture following ignition of contained vapors+air
		Vapor cloud explosion
		Flash fire
		Pool fire
	Combustibility	Bulk material fire
		Dust explosion
		Aerosol ignition and fast fire
		Flash fire of vapors from heated combustible solid or liquid
	Peroxidizing ability	Contact with oxygen over time; energetic peroxide decomposition
	Water-reactivity	Release of water-reactive material and energetic reaction with water or humidity
	Oxidizing or reducing ability	Contact of oxidizer with organic material; bulk material fire
		Uncontrolled redox reaction
	Acidity or causticity	Acid gas release (e.g., anhydrous HCl)
		Corrosive liquid or solid spill
		Uncontrolled acid/base reaction
	Toxicity	Toxic vapor release
		Toxic liquid or solid spill

Table 3.1 Process Hazards (continued)

FORM OF ENERGY	ASSOCIATED HAZARD(S)	TYPICAL ACCIDENTAL EVENT(S)
CHEMICAL ENERGY (continued)	Other increased reactivity	Inadvertent mixing or contact with incompatible material; heat, pressure, or toxic gas generation
	Reduced chemical reactivity (inert material)	Personnel entry into confined space with reduced oxygen level
THERMAL ENERGY	Elevated temperature	Hot material release
		Contact with hot surface
		Steam explosion or equivalent
		Containment rupture from thermal expansion of blocked-in fluid
	Reduced temperature	Cryogenic material release
		Fracture of embrittled containment
PRESSURE-VOLUME ENERGY	Volume of compressible fluid held at elevated pressure	Tank or enclosure rupture
		High-velocity leak or spray
	Liquefied material stored under pressure	Rapid phase transition (boiling-liquid-expanding-vapor explosion or BLEVE)
	Volume of compressible fluid held under vacuum	Tank or enclosure collapse
POTENTIAL (POSITIONAL) ENERGY	Elevation of process material above a reference level	Toppling over of stacked drums
		Shifting of granular storage piles
		Fluid surge from failed container
		Falling material from spill/overflow
KINETIC ENERGY (MATERIAL TRANSFER)	Moving process material	Overpressure or overtemperature by dead-headed pumping
		Impingement by process material
		Water hammer damage
ELECTRO-MAGNETIC	Elevated electromagnetic radiation levels	Unshielded laser or microwave radiation associated with process
ELECTRICAL ENERGY	Elevated voltage	Electrical shock from process using electricity, such as electrolysis of brine

NH₃ anhydrous ammonia	combustible; toxic vapor; cryogenic liquid spill					
Cl₂ chlorine	explosive NCl ₃ formed with excess chlorine or heat	oxidizer; toxic vapor; cryogenic liquid spill				
HF anhydrous hydrogen fluoride	heat generation, liberating toxic vapors	heat generation, liberating toxic vapors	strong acid; corrosive; toxic vapor and liquid			
C₄H₆ 1,3-butadiene	heat generation, violent polymerization	fire, toxic gas generation	heat generation, violent polymerization	flammable; peroxidizes; polymerizes; decomposes		
Fe, etc. carbon steel	none predicted	iron/chlorine fire if above 250EC (or 100EC with impurities)	hydrogen blistering between steel laminations	none predicted	material of construction	
H₂O 150# steam	heat generation, liberating toxic vapors	none predicted	heat generation, liberating toxic vapors	antioxidant consumed, leading to polymerization	none predicted	elevated pressure, temperature
<i>combined with...</i>	NH₃ anhydrous ammonia	Cl₂ chlorine	HF anhydrous hydrogen fluoride	C₄H₆ 1,3-butadiene	Fe, etc. carbon steel	H₂O 150# steam

NOTE: Descriptions along diagonal are properties of materials by themselves.

All potential material interactions should be examined for incompatibilities. Even if process materials are relatively non-hazardous when considered independently, some potentially dangerous interactions may occur when materials are combined. Interactions between process chemicals, containment materials, and other materials with which the chemicals come in contact can be examined in pairs by using an interaction matrix.

Figure 3.2 Example Interaction Matrix for Identifying Process Hazards

stage. If the deviation proceeds uncorrected, loss of control can lead to an *accident event*, such as a vessel rupture explosion. Various *protection* systems, such as alarms, interlocks, and emergency relief systems, may be employed to keep the accident event from occurring.

3.2.3 Review Previous Incidents

The PSM Rule requires all PrHAs to address "any previous incident which had a likely potential for catastrophic consequences in the workplace," 29 CFR 1910.119(e)(3)(ii). An *incident* is an unplanned event that may or may not result in injuries and/or loss. For example, an incident might involve a flammable gas leak that does not ignite. An *accident*, on the other hand, is an unplanned event that actually leads to personal injury, property damage, environmental damage, and/or business interruption losses, such as the ignition of a flammable gas leak resulting in burns and fire damage.

Previous accidents and incidents involving a process under study must be reviewed as part of the PrHA. The importance of reviewing accident and incident records is discussed in the anatomy of a process accident outlined in the preceding section (see Figure 3.3). Incidents can indicate what could happen if protection systems, which are not totally reliable, do not work. Thorough incident investigations may also indicate root causes of initiating events and protective system failures and thus suggest action items to improve safety-management systems. Incident records also help show the likelihood of failures and operational errors.

3.2.4 Analyze Controls and Control Failures

Process safety is the successful elimination or control of process hazards over the lifetime of a process. Engineering and administrative controls must be in place to keep process parameters within safe operating limits and to prevent challenges to system integrity. A PrHA addresses engineering and administrative controls applicable to process hazards, as well as the interrelationship of these controls, by identifying and documenting the process safety levels. For example, the safety levels to keep a deviation from becoming an accident should be documented in the *protection* (or safety levels) column of a HAZOP study worksheet when that method is employed. The levels of protection to keep the accident from occurring are included in a FTA as protective system branches which come together with initiator branches at AND logic gates.

As examples of engineering and administrative controls, the PSM Rule lists "appropriate application of detection methodologies to provide early warning of releases." For systems handling toxic materials, detection methodologies are generally *mitigation* systems that reduce the severity of consequences after an accident occurs.

Most PrHA methods study protection systems but do not explicitly study mitigation systems. FTA looks at all events and combinations of events that could lead to a *top event*, such as

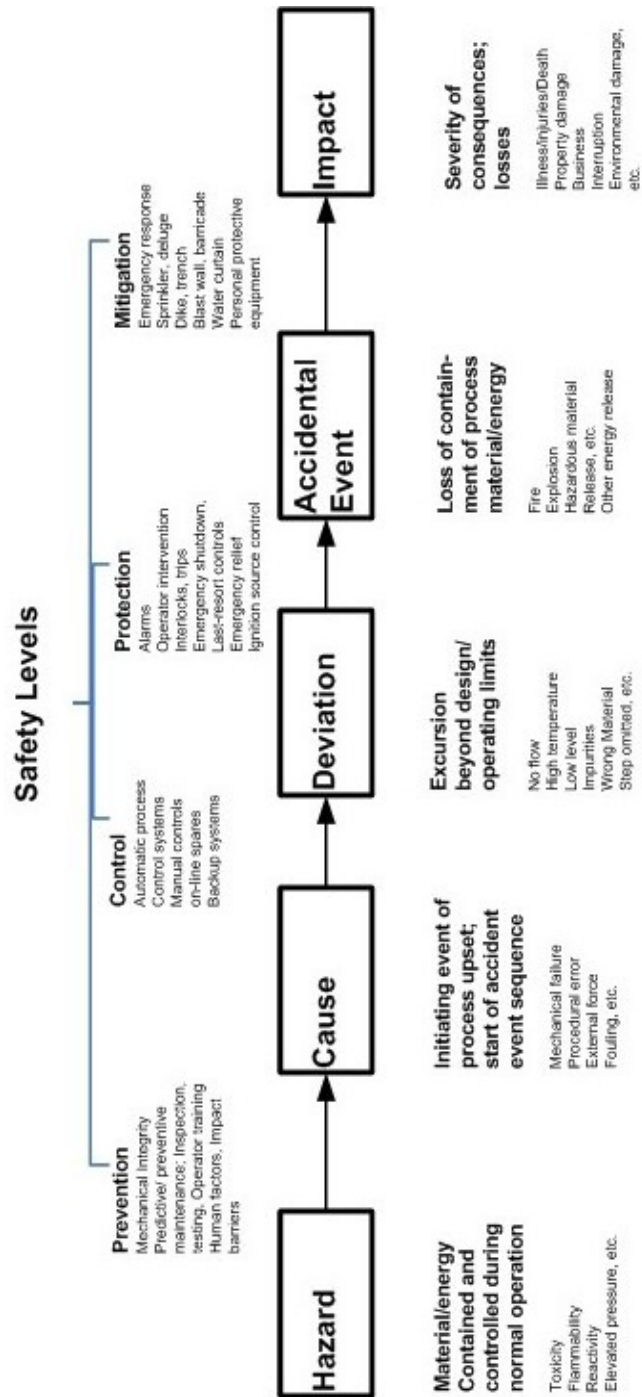


Figure 3.3 Anatomy of an Accident

explosions or toxic releases, but does not study the severity of the top event's consequences. To fully comply with the PSM Rule, it may be necessary to include in the PrHA report an analysis of *mitigation* systems that are in place to reduce the severity of consequences of accidents.

3.2.5 Consider Facility Siting

The PSM Rule requires facility siting to be addressed in all PrHAs. For a new facility, fulfilling this requirement can involve an analysis of plant layout and spacing between process units. However, most PrHAs are performed on existing facilities. For existing facilities, PrHAs should include the severity of consequences of potential accidents involving co-located workers and adjacent facilities. Shielding, barricades, escape routes, control room location, and control room design for employees involved in the operation of the process should also be discussed. In addition, the impacts of vehicular traffic and of adjacent operations should be considered.

It may be desirable to discuss facility siting issues at the beginning of the PrHA sessions. As a minimum, comments and assumptions about siting and plant layout can be included in the PrHA analysis documentation, such as on HAZOP study worksheets. Table 3.2 provides a sample checklist for worker/co-located worker exposures. A sample checklist for facility siting issues is presented in Table 3.3.

3.2.6 Address Human Factors

When operator error/response is involved in an initiating event or when operator action influences the level of protection, the PrHA team should discuss the circumstances under which failures might occur. For example, for a cylinder hook-up operation, an operator might connect the wrong cylinders. Uncovering the underlying causes of the error may lead to discussions of cylinder labeling, physical layout of the cylinder bay, or interchangeable threaded connections. These discussions should identify situations likely to lead to errors and the corrective actions that can be taken.

Table 3.4 presents a list of human factors that may positively or negatively influence the likelihood of operator error. This list may be used prior to, and/or during the analysis. In addition, the PrHA team may determine that human factors problems are of sufficient importance or complexity to require the assistance of a human factors specialist.

3.2.7 Evaluate Incident Effects

Quantitative evaluation of the severity of accident consequences is not required. However, the PrHA team must qualitatively evaluate the range of the possible employee safety and health effects. Such evaluation is generally made by discussing the severity of consequences of each scenario (see Section 4).

This evaluation may be performed more explicitly by assigning a qualitative term to each scenario. Typical qualitative terms such as "negligible, low, moderate, severe, and catastrophic" represent the order-of-magnitude consequences found in MIL-STD-882C.

Table 3.2 Checklist for Worker Exposures

PROCESS WORKER	OTHER WORKERS
☐ Is the worker within area of concern for exposure? ☐ Is there a requirement to respond to the accident to mitigate the exposure of others while increasing individual worker exposure? ☐ Is emergency equipment available to mitigate effects of material, and will it operate long enough to ensure escape? ☐ Are others aware of the location and status of workers near the release? ☐ Is the material released disabling such that escape is impaired? ☐ Is there a means of warning of the release in time to take action (alarms)? ☐ Is there a path to escape that minimizes exposure?	☐ Are the workers within area of concern for exposure? ☐ Does the material released have self-warning properties, or are exposed unaware of the exposure? ☐ Is the material released disabling such that escape is impaired? ☐ Is there a path to escape that minimizes exposure? Does the path depend on wind direction? ☐ Is there a plan and means to communicate to all workers in time to take effective action? ☐ Must many workers escape via limited paths?

Table 3.3 Checklist of Facility Siting Issues

General Considerations	1 ☐ Location of people relative to the unit 2 ☐ Location of critical systems 3 ☐ Dominant wind direction 4 ☐ Climate and weather extremes; earthquake, flooding, windstorms 5 ☐ Site topography 6 ☐ External hazards or threats (fire/explosion/toxic release from nearby process or facility; aircraft; subsidence; sabotage) 7 ☐ Traffic flow patterns and clearances from process vessels and lines 8 ☐ Security and reliability of all critical feeds and utilities 9 ☐ Command center and alternate command center locations 10 ☐ Evacuation routes, emergency exits, safe rally spots
Control Room	11 ☐ Minimum occupancy; only essential functions during emergencies 12 ☐ Control room construction 13 ☐ Fresh air intakes location/isolation; temporary safe havens 14 ☐ Control room location relative to unit, columns, and pipe bridges
Process Facilities	15 ☐ Area electrical classification 16 ☐ Accessibility for mechanical integrity (sampling, maintenance, repairs) 17 ☐ Protection of piping and vessels from vehicles and forklifts 18 ☐ Protection of small-bore lines, fittings from external impact, personnel 19 ☐ Routing of process piping, critical controls cable trays, critical utilities 20 ☐ Vent, drain, and relief valve discharge locations
Loading/Unloading and Storage Facilities	21 ☐ Incompatible materials segregated; storage, dikes, sumps, drains, waste 22 ☐ Siting, labeling of unloading spots for incompatible materials 23 ☐ Storage tank separation distances (to process, between tanks) 24 ☐ Spill control, drainage direction, destination, treatment capacity
Fire Protection	25 ☐ Access for fire fighting and any other emergency services 26 ☐ Ignition sources (continuous, occasional/intermittent, uncontrolled) 27 ☐ Access to hydrant, indicator, and deluge valves
Accident Mitigation	28 ☐ Detection of leaks/ruptures 29 ☐ Emergency shutdown switch locations 30 ☐ Accessibility of isolation valves 31 ☐ Potential for fire/explosion in unit affecting other equipment 32 ☐ Critical controls, mitigation, communication, and fire protection systems functional and accessible after initial explosion or release 33 ☐ Back-up power supply/redundant feeds for critical electrical systems 34 ☐ Water supply for fire fighting 35 ☐ Routing of utilities
Personnel Protection	36 ☐ Passageways, pedestrian traffic patterns vs. hazardous locations 37 ☐ SCBA/respirator locations; accessibility on all shifts

Table 3.4. Example Human Factors in Process Operations

CATEGORY		+	-
EQUIPMENT	Labeling	equipment clearly labeled; uniform coding	mislabeled or not labeled
	Access	immediately at hand	hard to reach or access
	Operability	power-assisted operation	difficult to operate/change position
	Layout	well-planned, logical arrangement	confusing/inconsistent arrangement
	Uniqueness	only component of its kind in area	several components look similar
CONTROLS	Labeling	controls clearly labeled; uniform coding	mislabeled or not labeled
	Mode	fully automatic; well-tuned	manual operation; many manual steps
	Involvement	operator continually involved	operator detached from process
	Displays	clear, simple, representational	unclear/complex/non-representational
	Feedback	immediate, unambiguous	none or potentially misleading
DEVIATIONS	Alarms	first-out; safety-critical alarms	many simultaneous or false alarms
	Coverage	dual operator coverage at all times	operator not always present
	Time	no time pressure for response	inadequate time to respond
	Preparedness	periodic simulation exercises	no drills/simulation of scenarios
	Last-Resort	shutdown not discouraged; fast access	shutdown discouraged or unsafe
TRANSIENT	Procedures	complete, accurate, current, verified	incomplete/too general/out of date
	Identifying	ID, location of devices/actions given	ambiguous device/action identification
	Format	graphical identification aids	confusing/inconsistent; difficult to read
	Aids	checklist or supervisory check	task sequence done by memory
SCHEDULING	Overtime	reasonable	extreme enough to affect performance
	Consistency	permanent shift assignments	inconsistent shift rotations/schedules
	# of Tasks	tasks, work force, and skills matched	tasks required exceed time available
	Task Freq.	routine task	very infrequent; no experience base
	Intensity	regular task at normal pace	differing tasks in rapid succession
COMMUNICATE	Shift Changes	status communicated verbally, plus turnover sheet used	inadequate communication between shifts of plant status
	Field/Control	constant communication with field	no communication with field operator
	Supervision	frequent supervisory communication	little or no supervisory checks
	Emergency	rapid, unambiguous plant alarm system	no distinction between area, type
ENVIRONMENT	Noise level	office environment noise level	area where hearing protection required
	Climate	indoors, climate-controlled	temp./humidity/precip./wind extremes
	Visibility	visibility enhancement of some kind	often foggy or other visibility limitation
	Lighting		inadequate lighting for task

This list does not contain management elements such as training and management of change.

"+" = factors beyond standard practice; may reduce the likelihood of human error or inadequate response.

"-" = factors may increase the likelihood of human error or inadequate response.

3.2.8 Decide on Need for Action

Regardless of the PrHA methodology, the team evaluates each accident scenario to determine whether design and/or operating changes are needed to further protect onsite workers. These judgments are usually based on risk rather than on either likelihood of occurrence or severity of consequences. For example, an event such as a seal water leak may be quite likely, but if the consequences are negligible, no safety-improvement recommendations are warranted. Similarly, if the consequences of a given accident are severe but the likelihood of occurrence is remote, then no safety-improvement recommendations may be warranted.

Qualitative evaluation often places the risk associated with each accident scenario into one of three categories: (a) the risk is too high, or a code violation is uncovered, such that design and/or operating changes are clearly warranted; (b) the risk is trivial or negligible, such that changes are clearly not warranted; or (c) the risk is borderline, and the decision is not clear-cut. In the last case, closer examination is needed to better define the accident scenario itself, its likelihood of occurrence, or the severity of its consequences. This closer examination can take the form of field inspections, examination of historical records, operator interviews, material testing, consequence modeling, and/or the use of more rigorous analysis methods, such as quantitative FTA

3.3 Presentation of Results

The critical results of a PrHA are a list of action items. Action items are written by the PrHA team any time additional effort is warranted to further analyze a specific accident scenario, eliminate the hazard, or reduce risks. Action items are not usually specific corrective actions. Rather, they alert management to potential problems that require action. Sometimes, action items suggest alternatives or recommend safety improvements. However, if a problem is simple, if a PrHA team is quite experienced, or if there is only one solution, an action item may recommend a specific corrective action.

All action items are presented to management for review and evaluation, and for determination of what, if any, corrective actions should be taken to eliminate hazards or reduce risks. Because many action items may be generated during a PrHA, the team may choose to rank the items according to the probability of occurrence and/or the severity of the consequences of their corresponding accident scenarios.

If the PrHA team is quite experienced, they may rank the action items according to the anticipated time and resources needed to implement changes. Or the team may make safety improvement and implementation recommendations. Ranking of action items or safety improvement recommendations may be valuable to management in several ways. It shows the significance that the PrHA team places on each item. It also allows management to prioritize the immediate efforts of corrective action and resolution. If resources are scarce, the ranking may affect the implementation schedule.

4.0 PROCESS HAZARD ANALYSIS METHODS WITH EXAMPLES

INTRODUCTION. The PSM Rule allows the use of several PrHA methods. DOE contractors should select the most appropriate methods for each facility or process and provide the rationale for their selections. Sometimes a combination of methods may be most appropriate.

The selection of a PrHA method depends on many factors including the size and complexity of the process and existing knowledge of the process. Has the process been in operation for a long time with little or no innovation, and has extensive experience been generated with its use? Or is the process new, or one that has been changed frequently by the inclusion of innovative features? All PrHA methods are subject to certain limitations. Because PrHAs depend on good judgment, assumptions made during a PrHA must be documented, understood, and retained for future PrHAs.

Sections 4.1 through 4.6 below discuss the PrHA methods identified specifically in the PSM Rule. They are preceded by two example processes (see Figures 4.1 and 4.2) that are referenced in discussions of methods and used to show a step-by-step approach. Three steps common to all methods are preparing for the analysis, performing the analysis, and documenting the results. All the basic information needed about the methods is included in this document, but there are numerous publications that provide additional information and examples.

4.1 Checklist Analysis

A checklist analysis is used to verify the status of a system. This analysis method is described in detail in Guidelines for Hazard Evaluation Procedures (CCPS, 1992).

The checklist analysis method is versatile, easy to use and can be applied at any stage in the life of a process. It is primarily used to indicate compliance with standards and practices. It is also a cost-effective way to identify common and customarily recognized hazards. Checklists also provide a common basis for management review of assessments. Many organizations use standard checklists to control the development of a process or an entire project from initial design through decommissioning. The completed checklist must be approved by all relevant staff members and managers before a project can move from one stage to the next.

4.1.1 Description of the Method

A checklist analysis uses a written list of items or procedures to verify the status of a system. Checklists may vary widely in level of detail, depending on the process being analyzed.

A traditional checklist analysis uses a list of specific items to identify known types of hazards, design deficiencies, and potential accident scenarios associated with common process equipment and operations. The method can be used to evaluate materials, equipment, or procedures. Checklists are most often used to evaluate a specific design with which a company or industry has a significant amount of experience, but they can also be used at earlier stages of

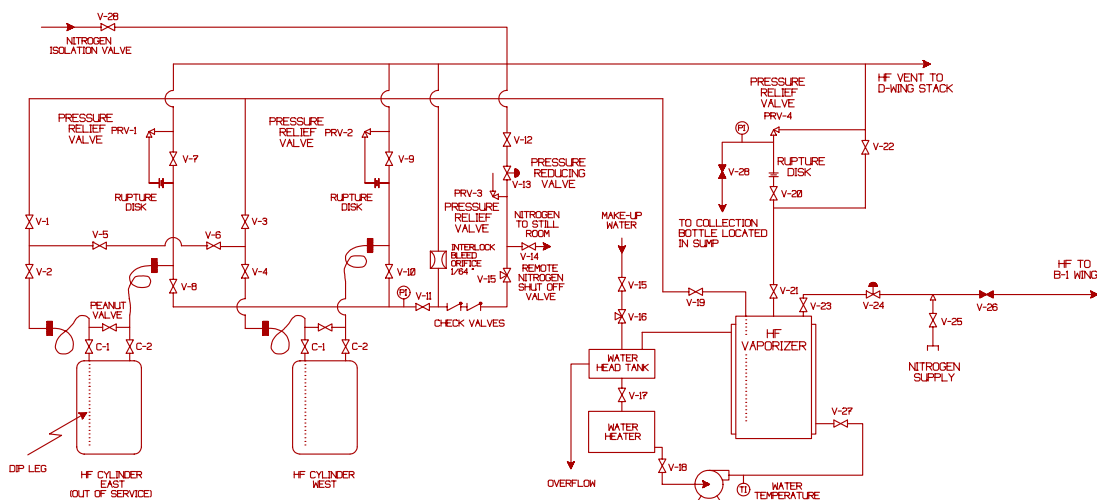


Figure 4.1 Dock 8 HF Supply System

EXAMPLE PROCESS 1: DOCK 8 HF SUPPLY SYSTEM.⁵ The dock 8 HF supply system is designed to supply gaseous HF, under pressure, to a fluid bed reactor to produce uranium tetrafluoride. The gaseous HF is created by heating and vaporizing anhydrous liquid HF that is brought to the system in large portable cylinders. The vaporizer room is heated and has an exhaust fan in the wall near the roof. When the system is in operation, the nitrogen (N_2) pressurization system supplies 30-psig nitrogen to the top of the HF cylinder. The cylinder, which contains about 850 pounds of anhydrous HF when full, is on a calibrated scale and is connected to the nitrogen and HF piping systems by pigtail connectors. The nitrogen pressure forces liquid HF to the vaporizer, which is heated by a hot water blanket supplied by a water heater and circulating pump. The liquid HF is heated to its vaporization temperature at the desired pressure, and the resulting gaseous HF is directed to the fluid bed reactor, regulated at 25 psig.

The designed safety system components in the HF feed station are the nitrogen pressure regulator and the nitrogen overpressure relief valves. To provide overpressure protection for the vaporizer, relief valves are fitted to piping connected to the top of the vaporizer and supply cylinder. A rupture disc, with a rupture pressure rating somewhat higher than the relief valve setting, is provided upstream of each of the relief valves to protect the valves from continuous exposure to the corrosive HF environment. Between the rupture disc on the vaporizer and the relief valve is a pipe tee to a manual vent with a block valve near the discharge. This valve can be opened manually to relieve pressure between the rupture disc and relief valve or to vent the system during maintenance. A pressure gage is attached to the vent line upstream of the block valve. A plastic hose is connected to the vent line pipe to direct vent gas to a plastic collection bottle. The collection bottle normally contains water that covers the end of the vent line hose to absorb vent fumes/vapors.

5. This description is taken from Hummer, John J., et al., 1992.

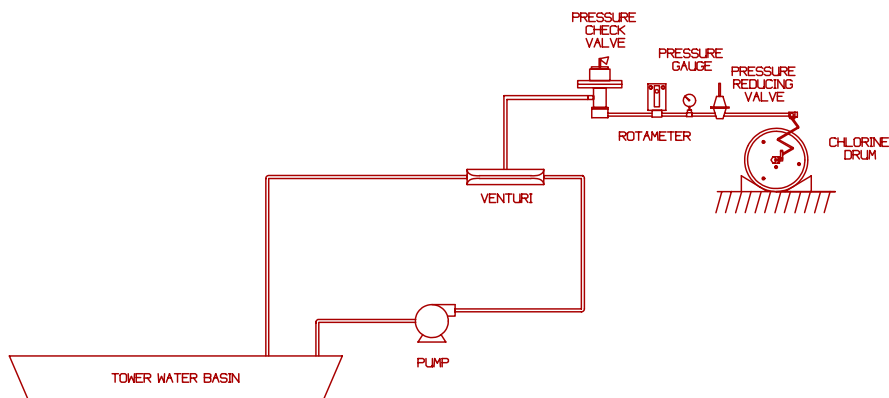


Figure 4.2. Cooling Water Chlorination System

EXAMPLE PROCESS 2: COOLING WATER CHLORINATION SYSTEM. The cooling water chlorination system is designed to provide chlorination to the basin of a cooling water system to prevent biological growth in the cooling water. Chlorine is provided from the vapor side of a 1-ton cylinder. Pressure is reduced from the cylinder (normally 80 psig at 70EF) to 15 psig at the rotameter. The rotameter is adjusted manually to provide an average flow rate of 2.5 to 3.0 pounds per hour to the pressure check valve. To operate properly, the chlorine gas supply must be reduced to zero so that the vacuum from a venturi may draw a controlled amount of chlorine into the water stream. A pressure check valve performs this function. Gas under pressure enters the pressure check valve. Its pressure is reduced to less than atmospheric as the gas passes through two valves which do not open unless a vacuum is present on the downstream side. If the first valve passes gas when a vacuum is not present, the second valve remains closed and contains the gas pressure in the unit. If the second valve also passes gas, the built-in pressure relief valve permits this gas to pass out of the vent. A small pump recirculates water through the venturi creating the vacuum for the chlorine and delivering chlorinated water to the basin. The pump's nominal flow rate is 30 gallons per hour.

development for entirely new processes to identify and eliminate hazards that have been recognized through operation and evaluation of similar systems. To be most useful, checklists should be tailored specifically for an individual facility, process, or product.

4.1.2 Analysis Procedure

Performing a checklist analysis requires access to engineering design procedures and operating practices manuals and must be performed by a team with appropriate expertise. An experienced manager or staff engineer should review the results and direct follow-up actions.

SELECTING OR DEVELOPING A CHECKLIST. A checklist is developed so that aspects of process design or operation that do not comply with standard industrial practices are discovered through responses to the questions in the list. A detailed checklist can be as extensive as necessary to satisfy the specific situation, but it should be applied conscientiously in order to identify problems that require further attention. Detailed checklists for particular processes should be augmented by generic checklists to help assure thoroughness. Generic checklists are often combined with other methods to evaluate hazardous situations.

Checklists are limited by their authors' experience. They should be developed by individuals who have extensive experience with the processes they are analyzing. Frequently, checklists are created simply by organizing information from current relevant codes, standards, and regulations. Checklists should be viewed as living documents and should be reviewed regularly and updated as required.

Sample checklists are shown in Tables 4.1, 4.2, and 4.3. A fairly exhaustive checklist appears in Guidelines for Hazard Evaluation Procedures, Appendix B (CCPS, 1992).

PERFORMING THE ANALYSIS. After a checklist is prepared, it can be applied by less experienced engineers if necessary. Team members should walkthrough and visually inspect the process areas to compare the process equipment and operations to the checklist items. The checklist can be reviewed in either hard copy or computer-based form. The analysts respond to the checklist items based on observations from their visual inspections, process documentation, interviews with operating personnel, and personal perceptions. If the process attributes or operating characteristics do not match the specific desired features on the checklist, the analysts note the deficiency.

A checklist analysis made prior to construction is usually performed during a PrHA team meeting. It focuses on review of the process drawings, completion of the checklist, and discussion of the deficiencies

Table 4.1 Simplified Process hazards Analysis Checklist Source: Burke, 1992

<u>STORAGE OF RAW MATERIALS, PRODUCTS, INTERMEDIATES</u>		<u>PERSONNEL PROTECTION</u>	
Storage Tanks	Design Separation, Inerting, Materials of Construction	Protection	Barricades, Personal, Shower, Escape Aids
Dikes	Capacity, Drainage	Ventilation	General, Local, Air intakes, Rate
Emergency Valves	Remote Control-Hazardous Materials	Exposures	Other Processes, Public, Environment
Inspections	Flash Arresters, Relief Devices	Utilities	Isolation: Air, Water, Inerts, Steam
Procedures	Contamination Prevention, Analysis	Hazards Manual	Toxicity, Flammability, Reactivity, Corrosion, Symptoms, First Aid
Specifications	Chemical, Physical, Quality, Stability	Environment	Sampling, Vapors, Dusts, Noise, Radiation
Limitations	Temperature, Time, Quantity		
<u>MATERIALS HANDLING</u>		<u>CONTROLS AND EMERGENCY DEVICES</u>	
Pumps	Relief, Reverse Rotation, Identification, Materials of Construction, Leaks, Cavitation	Controls	Ranges, Redundancy, Fail-Safe
Ducts	Explosion Relief, Fire Protection, Support	Calibration, Inspection	Frequency, Adequacy
Conveyors, Mills	Stop Devices, Coasting, Guards	Alarms	Adequacy, Limits, Fire, Fumes
Procedures	Spills, Leaks, Decontamination	Interlocks	Tests, Bypass Procedures
Piping	Rating, Codes, Cross-Connections, Materials of Construction, Corrosion/ Erosion Rates	Relief Devices	Adequacy, Vent Size, Discharge, Drain, Support
		Emergencies	Dump, Drown, Inhibit, Dilute
		Process Isolation	Block Valves, Fire-Safe Valves, Purging, Excess Flow Valves
		Instruments	Air Quality, Time Lag, Reset
			Windup, Materials of Construction
<u>PROCESS EQUIPMENT, FACILITIES AND PROCEDURES</u>		<u>WASTE DISPOSAL</u>	
Procedures	Startup, Normal, Shutdown, Emergency	Ditches	Flame Traps, Reactions, Exposures, Solids
Conformance	Job Audits, Shortcuts, Suggestions	Vents	Discharge, Dispersion, Radiation, Mists
Loss of Utilities	Electricity, Heating, Coolant Air, Inerts, Agitation	Characteristics	Sludges, Residues, Fouling
Vessels	Design, Materials, Codes, Access, Materials of Construction		Materials
Identification	Vessels, Piping, Switches, Valves	<u>SAMPLING FACILITIES</u>	
Relief Devices	Reactors, Exchangers, Glassware	Sampling Points	Accessibility, Ventilation, Valving
Review of Incidents	Plant, Company, Industry	Procedures	Pluggage, Purging
Inspections, Tests	Vessels, Relief Devices, Corrosion	Samples	Containers, Storage, Disposal
Hazards	Hang-fires, Runaways	Analysis	Procedures, Records, Feedback
Electrical	Area Classification, Conformance, Purging	<u>MAINTENANCE</u>	
Operating Ranges	Temperature, Pressure, Flows, Ratios, Concentrations, Densities, Levels, Time, Sequence	Decontamination	Solutions, Equipment, Procedures
Ignition Sources	Peroxides, Acetylides, Friction, Fouling, Compressors, Static	Vessel Openings	Size, Obstructions, Access
Compatibility	Electricity, Valves, Heaters	Procedures	Vessel Entry, Welding, Lockout
Safety Margins	Heating Media, Lubricants, Flushes, Packing	<u>FIRE PROTECTION</u>	
	Cooling, Contamination	Fixed Protection	Fire Areas, Water Demands, Distribution System, Sprinklers, Deluge, Monitors, Inspection, Testing, Procedures, Adequacy
		Extinguishers	Type, Location, Training
		Fire Walls	Adequacy, Condition, Doors, Ducts
		Drainage	Slope, Drain Rate
		Emergency Response	Fire Brigades, Staffing, Training, Equipment

Table 4.2. Main Headings of Well's Checklist

A	Basic process considerations
B	Some overall considerations
C	Operating limits
D	Modes of plant start-up, shutdown, construction, inspection and maintenance, trigger events and deviations of system
E	Hazardous conditions
F	Ways of changing hazardous events or the frequency of their occurrence
G	Corrective and contingency action
H	Controls, safeguards and analysis
I	Fire, layout and further precautions
J	Documentation and responsibilities

Source: King, 1990.

.DOCUMENTING THE RESULTS. Qualitative results of checklist analyses vary, but generally the analysis produces the answers "yes," "no," "not applicable," or "needs more information." The checklist should be included in the PrHA report. The PrHA team should summarize the deficiencies noted during the walkthroughs and/or meetings. Understanding these deficiencies usually leads to the development of a list of possible safety improvement alternatives for managers to consider, or a list of identified hazards and a set of suggested actions.

4.1.3 Staffing Needs and Time

Any engineer with knowledge of the subject process should be able to use a checklist. Because the PSM Rule requires a team approach, more than one analyst should be involved in preparing the checklist and applying it to the process. The results of the analysis should be reviewed by an independent analyst.

An estimate of the time required to perform a PrHA using the checklist analysis method is given in Table 4.4.

Table 4.3 Main Headings of Baleman's Check list

No. MAIN HEADING AND FIRST SUB-HEADING	No. MAIN HEADING AND FIRST SUB-HEADING
I. <i>Choice, situation and layout of site</i> 0. Choice and situation 1. Site layout II. <i>Process materials</i> 1. Physical properties 2. Chemical properties 3. Toxicological properties III. <i>Reactions, process conditions and disturbance analysis</i> 1. Reactions 2. Process conditions 3. Disturbance analysis 4. Causes of abnormal conditions 5. Abnormal conditions 6. Critical situations IV. <i>Equipment</i> 1. Introduction 2. Design 3. Choice of material 4. Construction 5. Location of equipment 6. Special provisions V. <i>The storage and handling of dangerous substances</i> 1. The storage of dangerous substances 2. The handling of dangerous substances services VI. <i>Handling and removal of hazardous waste products</i> 1. Introduction 2. Aspects of disposal 3. Reduction of disposal	VII. <i>Civil engineering aspects</i> 1. The ground 2. Foundations 3. Drainage systems 4. Roads 5. Buildings (see also section 9) 6. Additional points related to installations VIII. <i>Division of site into areas</i> (for hazards of igniting flammable vapors, etc.) IX. <i>Fire protection</i> 1. Introduction 2. Fire protection of buildings and plant 3. Fire-fighting organization 4. Fire detection and alarm 5. Classification of fires according to European Standard EN2 X. <i>General emergency planning</i> 1. Introduction 2. Operational emergency situations 3. Escape of liquids and gases 4. Fire and explosion 5. Personal protection 6. Training 7. Communication systems 8. Briefing and information

Source: King, 1990.

Table 4.4 Approximate Checklist Analysis Time Requirements

SCOPE	PREPARATION	EVALUATION	DOCUMENTATION
Simple/Small System	2 to 4 hours	4 to 8 hours	4 to 8 hours
Complex/Large Process	1 to 3 days	3 to 5 days	2 to 4 days

4.1.4 Limitations of Checklist Analysis

When derived from handbooks or similar sources, many entries in a checklist may not be applicable to the process being studied. In other cases, process hazards may be so unusual they are not in standard checklists. Thus, it may be difficult to assure that all hazards have been analyzed. Also, checklists may indicate that hazards exist, but not what accident scenarios are associated with them.

4.1.5 Example Checklist Analyses

Simplified checklist analyses for the two example processes in Section 4.0 are shown in Tables 4.5 and 4.6. The same checklist was used for both processes.

4.2 What-If Analysis

The purpose of a what-if analysis is to identify hazards, hazardous situations, or specific accident events that could produce an undesirable consequence. The what-if analysis is described in detail in Guidelines for Hazard Evaluation Procedures (CCPS, 1992).

What-if analysis involves the examination of possible deviations from the design, construction, modification, or operating intent of a process. It can be used to examine virtually any aspect of facility design or operation. Because it is so flexible, it can be performed at any stage in the life of a process using whatever process information and knowledge is available.

4.2.1 Description of the Method

The what-if analysis is a creative, brainstorming examination of a process or operation conducted by a group of experienced individuals able to ask questions or voice concerns about undesired events. It is not as inherently structured as some other methods, such as the hazard and operability (HAZOP) study or a failure mode and effects analysis (FMEA). Rather, it requires the analysts to adapt the basic concept to the specific application.

The what-if analysis encourages a PrHA team to think of questions that begin with "What-if." Through this questioning process, an experienced group of individuals identify possible accident events, their consequences, and existing safety levels, then suggest alternatives for risk reduction. The potential accidents identified are neither ranked nor given quantitative implications.

The what-if analysis method may simply generate a list of questions and answers about the process. However, it usually results in a tabular listing of hazardous situations, their consequences, safety levels, and possible options for risk reduction.

4.2.2 Analysis Procedure

PREPARING FOR THE ANALYSIS. The information needed for a what-if analysis includes process descriptions, operating parameters, drawings, and operating procedures. All information must be available to the PrHA team, if possible, in advance of the team meetings.

For analysis of an existing plant, the PrHA team may want to interview personnel responsible for operations, maintenance, utilities, or other services, if they are not on the PrHA team. In addition, if the analysis is performed offsite, the PrHA team should walk through the facility to better understand its layout, construction, and operation. Thus, visits and interviews should be scheduled before the analysis begins. Finally, some preliminary what-if questions should be prepared to "seed" the team meetings. If the analysis is an update of a previous PrHA, then questions listed in previous reports can be used. For a new process or a first-time application, preliminary questions should be developed by team members before the meetings, although additional questions formulated during the meetings are essential. The cause-and-effect thought process used in other types of analyses described in this section, such as HAZOP studies and FMEAs, can help formulate questions.

PERFORMING THE ANALYSIS. The scope of the study should be agreed upon by the team members. The analysis meetings should begin with a basic explanation of the process by operations staff who have overall facility and process knowledge, plus expertise relevant to the team's area of investigation. The presentation should also describe the facility's safety precautions, safety equipment, and health control procedures.

The meetings then revolve around potential safety issues identified by the analysts. The analysts are encouraged to voice any potential safety concern in terms of questions that begin with "what-if." However, any process safety concern can be voiced, even if it is not phrased as a question. For example:

"I wonder what would happen if the wrong material was delivered."

"What if Pump Y seals begin to leak?"

"What if valve X fails open?"

Table 4.5 Checklist Analysis of Dock 8 HF Supply System**MATERIAL**

- ☐ ***Do all raw materials continue to conform to original specifications?*** Yes. The cylinders are ordered with the same anhydrous HF specification used since startup.
- ☐ ***Is each receipt of material checked?*** No. There have been no problems with the supplier, so no such check has been considered. Investigate consequences of receiving material other than HF. Consider adding such checks on HF receipts.
- ☐ ***Does the operating staff have access to Material Safety Data Sheets?*** Yes. All staff are familiar with the process chemistry, including the hazards of HF.
- ☐ ***Is fire fighting and safety equipment properly located and maintained?*** Yes.

EQUIPMENT

- ☐ ***Has all equipment been inspected as scheduled?*** Yes. The maintenance personnel have inspected the equipment in the process area according to company inspection standards. Given the corrosivity of HF, inspections may have to be more frequent.
- ☐ ***Have pressure relief valves been inspected as scheduled?*** Yes.
- ☐ ***Have rupture discs been inspected (for having blown) as scheduled?*** Yes. Though none have failed, procedure calls for inspection of rupture disc and installation after maintenance.
- ☐ ***Are the proper maintenance materials (parts, etc.) available?*** Yes. They include spare pigtailed for the supply cylinders as well as properly rated rupture discs. Other items must be ordered.

PROCEDURES

- ☐ ***Are the operating procedures current?*** Yes.
- ☐ ***Are the operators following the operating procedures?*** Yes. No significant violations of procedures have been noted.
- ☐ ***Are new operating staff trained properly?*** Yes. Training includes a review of the PrHA for this process and familiarization with MSDSs.
- ☐ ***How are communications handled at shift change?*** If an HF cylinder needs to be changed out near a shift change, the change is scheduled to be performed by either, but not both, shifts.
- ☐ ***Is housekeeping acceptable?*** Yes.
- ☐ ***Are safe work permits being used?*** Yes.

Table 4.6 Checklist Analysis of Cooling Water Chlorination System**MATERIAL**

- ☐ ***Do all raw materials continue to conform to original specifications?*** Yes. The drums are ordered with the same chlorine specification used since startup.
- ☐ ***Is each receipt of material checked?*** Yes. The supplier once sent a cylinder of phosgene. Since then, a test is performed by the maintenance staff. In addition, the fusible plugs are inspected for evidence of leakage, before a cylinder is hooked up.
- ☐ ***Does the operating staff have access to Material Safety Data Sheets?*** Yes. All staff are familiar with the process chemistry, including the hazards of Cl₂.
- ☐ ***Is fire fighting and safety equipment properly located and maintained?*** Yes. This system is on a concrete building roof. Because there are no flammable materials involved in this system, if a fire occurs, there will be no special effort by fire fighting crews to concentrate on the roof area.

EQUIPMENT

- ☐ ***Has all equipment been inspected as scheduled?*** Yes. The maintenance personnel have inspected the equipment in the process area according to company inspection standards.
- ☐ ***Have pressure relief valves been inspected as scheduled?*** Yes.
- ☐ ***Have rupture disks been inspected (for having blown) as scheduled?*** Not applicable.
- ☐ ***Are the proper maintenance materials (parts, etc.) available?*** Yes. They include spare pigtails for the supply cylinders, as well as a rotameter and a pressure check valve. Other items must be ordered.
- ☐ ***Is there an emergency cylinder capping kit?*** Yes.

PROCEDURES

- ☐ ***Are the operating procedures current?*** Yes.
- ☐ ***Are the operators following the operating procedures?*** No. It is reported that some staff do not always check the cylinder's fusible plugs for leaks. Staff should be re-reminded of this procedural item and its importance.
- ☐ ***Are new operating staff trained properly?*** Yes. Training includes a review of the PrHA for this process and familiarization with MSDSs.
- ☐ ***How are communications handled at shift change?*** There are relatively few open items at the end of a shift. The chlorine cylinders need to be changed only about once every 45 days. If an empty chlorine cylinder needs replaced, it has proven to be easy to schedule the change during a shift.
- ☐ ***Is housekeeping acceptable?*** Yes.
- ☐ ***Are safe work permits being used?*** Yes.

The questions may address any off-normal condition related to the facility, not just component failures or process variations. The questions are formulated based on PrHA team member experience and applied to existing drawings and process descriptions. The team generally proceeds from the beginning of the process to its end, although the PrHA team leader can order the analysis in any logical way he or she sees fit, such as dividing the process into functional systems. Or the leader may direct the review to begin with the introduction of feed material and follow the flow until the end of the process. The questions, and eventually the answers (including hazards, consequences, engineered safety levels, and possible solutions to important issues), are recorded by the team member designated as "scribe," so that they can be viewed by all team members.

The questions may be divided into specific areas of investigation usually related to consequences of interest, such as electrical safety, fire protection, or personnel safety. Each area is subsequently addressed by a team of one or more knowledgeable individuals. The team answers each question and addresses each concern (or indicates a need for more information) and identifies the hazard, potential consequences, engineered safety levels, and possible solutions. During the process, any new what-if questions that become apparent are added. Sometimes the proposed answers are developed by individuals outside the initial meeting, and then presented to the team for endorsement or modification.

For example, given the question:

"What if the HF cylinder fails because of corrosion?",

the team would attempt to determine how the process would respond:

"A cylinder leak would release HF to the atmosphere and eventually result in a loss of HF feed to the vaporizer."

The team might then recommend checking with the supplier regarding cylinder inspection practices.

The team should not be rushed, and meetings should last no longer than 4 to 6 hours per day. What-if team meetings that last more than 5 consecutive days are not desirable. If a process is complex or large, it should be divided into smaller segments so that the team does not spend several consecutive days just listing questions.

DOCUMENTING THE RESULTS. The what-if analysis produces a tabular listing of narrative-style questions and answers that constitute potential accident scenarios; their qualitative consequences; and possible risk-reduction methods. Table 4.7 shows the format of a what-if analysis worksheet. Although some what-if analyses are documented in a narrative-style format, a table makes the documentation more organized and easier to use.

Table 4.7 Typical Format for a What-If Analysis Worksheet

LINE/VESSEL: _____ **Date:** _____ **PAGE:** _____ of _____

WHAT-IF	CONSEQUENCE	SAFETY LEVELS ^(a)	SCENARIO	COMMENTS

(a) This column is a recent improvement in documentation format.
Source: CCPS, 1992.

The comments column may contain additional descriptive information or actions/recommendations. The recommendations, sometimes with more detailed explanations, can be summarized in the report to produce a list of action items or suggestions for improving the safety of the process. These results should be reviewed with management to assure that the findings are transmitted to those ultimately responsible for any actions.

4.2.3 Staffing Needs and Time

The PSM Rule requires that a what-if analysis be performed by a team with expertise in engineering and process operations. It must include at least one employee experienced in the process, and one knowledgeable in the use of the analysis method. For simple processes, two or three people may be assigned to perform the analysis. However, larger teams may be required for more complex processes. When a large team is required, the process may be divided logically into smaller pieces, and a subset of the team may analyze each piece.

The time and cost of a what-if analysis are proportional to the number and complexity of the processes being analyzed. Table 4.8 presents estimates of the time needed to perform a PrHA using the what-if analysis method.

Table 4.8 Approximate Time Requirement for What-If Analyses

SCOPE	PREPARATION ^(a)	EVALUATION	DOCUMENTATION ^(a)
Simple/Small System	4 to 8 hours	4 to 8 hours	1 to 2 days
Complex/Large Process	1 to 3 days	3 to 5 days	1 to 3 weeks

(a) Primarily, team leader and scribe.
Source: CCPS, 1992.

4.2.4 Limitations of the What-If Analysis

The what-if analysis is a powerful PrHA method if the analysis team is experienced and well organized. Otherwise, because it is a relatively unstructured approach, the results are likely to be incomplete.

4.2.5 Example What-If Analyses

Partial what-if analyses for the two example processes described in Section 4.0 are shown in Tables 4.9 and 4.10. Although for actual, more complex analyses, the what-if tables for each line or vessel would be separate, for these examples, a single table was developed. A preliminary hazard analysis (PHA) would identify that the intrinsic hazards associated with HF are its reactivity (including reactivity with water, by solution), corrosivity (including carbon steel, if wet), toxicity via inhalation and skin contact, and environmental toxicity. The N₂ supply system pressure is not considered in this example. The specific effects of loss of containment could be explicitly stated in the "loss of HF containment" scenarios identified. Similarly, the effects of loss of chlorine containment, including the reactivity and toxicity of chlorine, could be specified for the second example.

4.3 What-If/Checklist Analysis

The purpose of a what-if/checklist analysis is to identify hazards, consider the types of accidents that can occur in a process or activity, evaluate in a qualitative manner the consequences of these accidents, and determine whether the safety levels against these potential accident scenarios appear adequate. The what-if/checklist analysis is described in detail in Guidelines for Hazard Evaluation Procedures (CCPS, 1992).

4.3.1 Description of the Method

The what-if/checklist analysis method combines the creative, brainstorming features of the what-if analysis with the systematic features of the checklist analysis. The PrHA team uses the what-if analysis method to brainstorm the types of accidents that can occur within a process. Then the team uses one or more checklists to help fill in any gaps. Finally, the team members suggest ways for reducing the risk of operating the process. The what-if analysis encourages the PrHA team to consider potential accident events and consequences that are beyond the experience of the authors of a good checklist and, thus, are not covered on the checklist. Conversely, the checklist lends a systematic nature to the what-if analysis.

Normally, a what-if/checklist analysis is used to examine the potential consequences of accident scenarios at a more general level than some of the more detailed PrHA methods. It can be used for any type of process at virtually any stage in its life cycle. However, this method is generally used to analyze the more common hazards that exist in a process.

4.3.2 Analysis Procedure

PREPARING FOR THE ANALYSIS. For a what-if/checklist analysis, the PrHA team leader assembles a qualified team and, if the process is large, divides it into functions, physical areas, or tasks to provide some order to the review. The important aspects of preparing for a what-if analysis, which also apply to the what-if/checklist analysis, are discussed in Section 4.2 and are not repeated here.

For the checklist portion of the analysis, the PrHA team leader obtains or develops an appropriate checklist for the team to use. This list need not be as detailed as those used for a standard checklist analysis. Rather than focusing on a specific list of design or operating features, the checklist used here should focus on general hazardous characteristics of the process.

DEVELOPING WHAT-IF QUESTIONS. Section 4.2 describes the approach the PrHA team uses to develop questions about potential accident scenarios.

USING A CHECKLIST TO COVER THE GAPS. After the team members have identified all of the questions in a particular area or step of the process, they apply the previously-obtained or prepared checklist. The team considers each checklist item to determine whether any other potential accident scenarios exist. If so, these scenarios are added to the what-if list and evaluated in the same way. The checklist is reviewed for each area or step in the process.

EVALUATING THE QUESTIONS. After developing questions involving potential accident scenarios, the PrHA team considers each one; qualitatively determines the possible effects of the potential accident; and lists existing safety levels to prevent, mitigate, or contain the effects of the accident. The team then evaluates the significance of each accident and determines whether a safety improvement should be recommended. This process is repeated for each area or step of the process or activity. The evaluation may be performed by specific team members outside the team meeting but must be subsequently reviewed by the team.

DOCUMENTING THE RESULTS. The results of a what-if/checklist analysis are documented like the results for a what-if analysis (see Section 4.2). The what-if/checklist analysis method usually generates a table of potential accident scenarios, consequences, safety levels, and action items. The results may also include a completed checklist or a narrative. The PrHA team may also document the completion of the checklist to help illustrate the completeness of the analysis. For compliance with the PSM Rule, detailed explanations of the analysis action items and recommendations should be provided to management for review, and transmitted to those responsible for their resolution.

4.3.3 Limitations of the What-If/Checklist Analysis

Combining the what-if and checklist analysis methods emphasizes their main positive features (i.e., the creativity of what-if analysis and the experience-based thoroughness of a checklist analysis) while at the same time compensating for their shortcomings when used separately. For

Table 4.9. What-If Analysis of Dock 8 HF Supply System**LINE/VESSEL: Dock 8 HF Supply System DATE: December 22, 1992 PAGE: of**

WHAT IF	CONSEQUENCES	SAFETY LEVELS	SCEN- ARIO	COMMENTS
... the HF cylinder corrodes through?	Cylinder leak, HF release to atmosphere, possible worker exposure via inhalation and skin, possibly fatal.	None.	1	Check with supplier regarding cylinder inspection practices.
... the dock and this equipment is involved in a fire?	HF release to atmosphere via vent	None.	2a	
	OR cylinder rupture, with possible worker exposure via inhalation and skin, possibly fatal.	Relief valves, rupture discs.	2b	
... the hot water jacket on the HF corrodes through	Heat of solution, HF release via vent, possible worker exposure via inhalation and skin, possibly fatal.	None.	3a	
	Possible large pipe and pipe component failures due to corrosion. Possible vaporizer rupture with further release and blast effects, worker injured by blast or scalded.	Relief valve, rupture disc.	3b	
... moisture is introduced into the HF cylinder via the N ₂ supply?	Heat of solution, HF release via vent, possible worker exposure via inhalation and skin, possibly fatal.	None.	4a	Prevention is procedures for monitoring N ₂ supply.
	HF solution attacks carbon steel, corrosion, leak or rupture, possible worker exposure via inhalation and skin, possibly fatal.		4b	

Table 4.9. What-If Analysis of Dock 8 HF Supply System (continued)**LINE/VESSEL: Dock 8 HF Supply System DATE: December 22, 1992 PAGE: of**

WHAT IF	CONSEQUENCES	SAFETY LEVELS	SCEN- ARIO	COMMENTS
... N ₂ supply lost	N ₂ supply contaminated with HF ...	Check valves in N ₂ supply line.	5	
... Water pump fails	Liquid HF not vaporized, passed to fluidized bed reactor, off-spec or no product.	None.	6	Consider adding a low temperature interlock on HF (N ₂) flow.
... Piping or pigtail failure	Loss of containment, HF release, possible worker exposure via inhalation and skin, possibly fatal.	None.	7	
... Material other than HF received in cylinders	Unknown (see Comments).	Procedure: sampling of contents on receipt.	8	Prevention includes supplier's shipping procedures. Investigate consequences of receiving material other than HF.

Table 4.10. What-If Analysis of Cooling Water Chlorination System**LINE/VESSEL: Cooling Water Chlorination System DATE: December 22, 1992 PAGE: of**

WHAT IF	CONSEQUENCES	SAFETY LEVELS	SCEN- ARIO	COMMENTS
... the system is involved in a fire?	High pressure in chlorine cylinder, fusible plugs melt, chlorine release into fire ...	Ignition source control.	1	Verify that area is free from unnecessary fuel.
... the wrong material is received in the cylinder and hooked up? - Oil	Water contaminated, not sterilized	None.	2	Prevention: supplier's procedures.
... the cylinder's fusible plugs prematurely fail?	Chlorine release.	None.	3	Purchase and train personnel in the use of a Cl ₂ cylinder leak capping kit.
... the pressure check valve fails open (both pass chlorine gas)?	Built-in relief valve opens, releasing chlorine to atmosphere.	None.	4	
... the basin corrodes through?	Chlorinated water release.	Periodic inspection.	5	
... the recirculation pump fails OR power is lost?	Eventually low chlorine in water, biological growth.	None.	6a	
	Release of undissolved chlorine to atmosphere if pressure check valve fails.	Pressure check valve.	6b	
... the chlorine cylinder is run dry and not replaced?	Eventually low chlorine in water, biological growth.	None.	7	

example, a traditional checklist is, by definition, based on the process experience the author accumulates from various sources. The checklist is likely to provide incomplete insights into the design, procedural, and operating features necessary for a safe process. The what-if part of the analysis uses a team's creativity and experience to brainstorm potential accident scenarios. However, because the what-if analysis method is usually not as detailed, systematic, or thorough as some of the more regimented approaches (e.g., HAZOP study, FMEA), use of a checklist permits the PrHA team to fill in any gaps in their thought process.

4.3.4 Staffing Needs and Time

The number of individuals needed depends upon the complexity of the process and, to some extent, the stage at which the process is being evaluated. Normally, a PrHA using this method requires fewer people and shorter meetings than does a more structured method such as a HAZOP study. Estimates of the time needed to perform a PrHA using the what-if/checklist analysis method are shown in Table 4.11.

Table 4.11 Approximate What-If/Checklist Analysis Time Requirements

SCOPE	PREPARATION ^(a)	EVALUATION	DOCUMENTATION ^(a)
Simple/Small System	6 to 12 hours	6 to 12 hours	4 to 8 hours
Complex/Large Process	1 to 3 days	4 to 7 days	1 to 3 weeks

(a) Primarily, team leader and scribe.
Source: CCPS, 1992.

4.3.5 Example What-If/Checklist Analyses

To fill in the gaps in the standard what-if analyses given as examples in Section 4.2, the checklists used for the examples in Section 4.1 were used here. The resulting what-if/checklist analyses for the two example processes are shown in Tables 4.12 and 4.13. The tables show only *additional* scenarios identified by applying the checklist.

4.4 Hazard and Operability Study

The HAZOP study was developed to identify hazards in process plants and to identify operability problems that, although not hazardous, could compromise a plant's productivity. The basic concept behind HAZOP studies is that processes work well when operating under design conditions. When deviations from the process design conditions occur, operability problems and accidents can occur. The HAZOP study method uses guide words to assist the analysis team in considering the causes and consequences of

Table 4.12. What-If/Checklist Analysis of Dock 8 HF Supply System**LINE/VESSEL: Dock 8 HF Supply System****DATE: December 22, 1992****PAGE: of**

WHAT IF	CONSEQUENCES	SAFETY LEVELS	SCEN- ARIO	COMMENTS
... the pressure relief valve fails closed?	Possible rupture of HF cylinder with personnel exposure to HF and blast effect, possibly fatal.	None.	1	Add pressure alarm on operator console.
... the operator does not valve off the empty cylinder before removing it?	HF release with personnel exposure, possibly fatal.	None.	2	Review training records to make sure all staff have been trained in current procedures.

Table 4.13. What-If/Checklist Analysis of Cooling Water Chlorination System**LINE/VESSEL: Cooling Water Chlorination System DATE: December 22, 1992 PAGE: of**

WHAT IF	CONSEQUENCES	SAFETY LEVELS	SCEN- ARIO	COMMENTS
... a chlorine cylinder which is not empty is removed?	If the operator does not expect it to contain chlorine, then possible Cl ₂ exposure via skin and inhalation.	None.	1	Review training records and operating procedures to minimize possibility of this occurring.
... the venturi is clogged with residue from the water basin?	No sterilization will occur.	Periodic checks of water quality.	2	
	High pressure in recirculation line, with	None.	3	
	• possible rupture, release of water • release of Cl₂ if pressure check valve fails.	Pressure check valve.	4	

deviations. These guide words are applied at specific points or sections in a process and are combined with specific process parameters to identify potential deviations from intended operation.

4.4.1 Description of the Method

A HAZOP study requires considerable knowledge of the process, its instrumentation, and its operation. This information is usually provided by expert team members. The team should include individuals with a variety of experience, including design, engineering, operations, and maintenance.

The primary advantages of a HAZOP study are creativity and new ideas. Creativity is the result of interactions among team members with diverse backgrounds. Such interactions often generate new ideas. The success of a HAZOP study depends on the freedom of members to freely express their views. Combining this approach with a systematic protocol for examining hazards promotes thoroughness and accuracy.

4.4.2 Analysis Procedure

A HAZOP study has three steps: (1) defining the process, (2) performing the study, and (3) documenting the results. Defining the process and documenting the results can be performed by a single person. The study itself must be performed by a team.

DEFINING THE PROCESS TO BE STUDIED. This step identifies the specific vessels, equipment, and instrumentation to be included in the HAZOP study and the conditions under which they are analyzed. Defining the problem involves defining the boundaries of the analysis and establishing an appropriate level of resolution for the study. For most HAZOP studies, the causes of deviations are identified at the component level (i.e., control valve CV101 fails open).

PERFORMING THE STUDY. A HAZOP study focuses on specific points of a process called "study nodes," process sections, or operating steps. Depending on the experience of the study leader, the portion of a process included in a single study node can vary. In the most conservative studies, every line and vessel are considered separately. If the HAZOP study leader is experienced, he or she may elect to combine two or more lines into a single study node. For example, the cooling water chlorination system (Example Process 2) could be separated into three study nodes (chlorine supply to venturi, recirculation loop, and tower water basin), two study nodes (recirculation loop and tower water basin combined as a single study node), or one study node (the entire process).

If too much of a process is included in a single study node, deviations may be missed. If too little of a process is included, the study can become tedious. In addition, root causes of deviations and their potential consequences can become separated. Too many study nodes is common for novice HAZOP study leaders. On the positive side, a study with too many nodes is less likely to miss scenarios than one with too few nodes.

The HAZOP team examines each study node for potentially hazardous process deviations. First, the design intent is defined to delineate the purpose of the equipment and the process

parameters. Process deviations are determined by combining guide words with the important process parameters. The established set of guide words is shown in Table 4.14.

Table 4.14 Guide Words for HAZOP Studies

GUIDE WORD	MEANING	EXAMPLES
None of	Negation of Intention	No forward flow when there should be. Sequential process step omitted.
More of	Quantitative Increase	More of any relevant physical parameter than there should be, such as more flow (rate, quantity), more pressure, higher temperature, or higher viscosity. Batch step allowed to proceed for too long.
Less of	Quantitative Decrease	Opposite of "MORE OF"
Part of	Qualitative Decrease	System composition different from what it should be (in multi-component stream).
As well as	Qualitative Increase	More things present than should be (extra phases, impurities). Transfer from more than one source or to more than one destination.
Reverse	Logical Opposite	Reverse flow. Sequential process steps performed in reverse order.
Other than	Complete Substitution	What may happen other than normal continuous operation (start-up, normal shutdown, emergency shutdown, maintenance, testing, sampling). Transfer from wrong source or to wrong destination.

The process parameters and example deviations typically used in a HAZOP study are shown in Table 4.15. Additional process parameters can be added if warranted. One purpose of the guide words is to assure that all relevant deviations of process parameters are evaluated.

The following are examples of deviations created using guide words and process parameters.

<u>Guide Word</u>		<u>Parameter</u>		<u>Deviation</u>
No	+	Flow	=	No flow
More	+	Temperature	=	High temperature
Other than	+	Location	=	Wrong location

Table 4.15 Example HAZOP Study Process Parameters and Deviations

PROCESS PARAMETER	DEVIATION	PROCESS PARAMETER	DEVIATION
Flow (rate)	No flow High flow Low flow Reverse flow	Time	Too long Too short Too late Too soon
Flow (quantity)	Too much Too little	Sequence	Omit a step Steps reversed Extra step
Pressure	High pressure Low pressure	pH	High pH Low pH
Temperature	High temperature Low temperature	Viscosity	High viscosity Low viscosity
Level	High level/overflow Low level/empty	Heat Value	High heat value Low heat value
Mixing	Too much mixing Not enough mixing Loss of agitation Reverse mixing	Phases	Extra phase Phase missing
Composition	Component missing High concentration Low concentration	Location	Additional source Additional destination Wrong source Wrong destination
Purity	Impurities present Catalyst deactivated/inhibited	Reaction	No reaction Too little reaction Too much reaction Reaction too slow Reaction too fast

In the first example, the guide word "No" combined with the process parameter "Flow" results in the deviation "No flow." Considering this deviation, the study team agrees on its possible causes (e.g., operator error causes block in pump), the consequences of the deviation (e.g., line rupture due to high pressure), and the safety levels which prevent the cause from leading to the consequence (e.g., pressure relief valve on pump discharge line). The consequence specified presupposes the failure of active protection systems (e.g., relief valves, process trip signals). If the causes and consequences are significant, and the safety levels are inadequate, the team may recommend a follow-up action. In some cases, the team may identify a deviation with a realistic cause but unknown consequences (e.g., an unknown reaction product) and recommend follow-up studies to determine the potential consequences.

The HAZOP study should be performed in a deliberate, systematic manner to reduce the possibility of omissions. Within a study node, all deviations associated with a given process parameter should be analyzed before the next process parameter is considered. All of the deviations for a given study node should be analyzed before the team proceeds to the next node.

DOCUMENTING THE RESULTS. The documentation of a HAZOP study is a systematic and consistent tabulation of the effects of process deviations. The study generates narratives about the normal operating conditions and analysis boundary conditions for each equipment item. In addition, it provides a list of potential actions that should be evaluated. Table 4.16 is an example of a HAZOP study worksheet. A typical HAZOP study report should include a brief system description, a list of drawings or equipment analyzed, the design intents, the HAZOP study tables, and a list of actions items.

4.4.3 Staffing Needs and Time

Staff requirements for HAZOP studies vary with the size and complexity of the process. Time and cost are proportional to the size of the process being analyzed and the experience of the study leader and team members. Table 4.17 presents estimates of the time needed to perform a PrHA using the HAZOP study method (CCPS, 1992). Study sessions should be limited to 3 consecutive days.

4.4.4 Limitations of the Hazard and Operability Study

The primary limitation of a HAZOP study is the length of time required to perform it. Because the study is designed to provide a complete analysis, study sessions can be intensive and tiring. HAZOP studies typically do not look at occupational hazards (e.g., electrical equipment, rotating equipment, hot surfaces) or chronic hazards (e.g., chronic chemical exposure, noise, heat stress).

Table 4.16 Typical Format for a HAZOP Study Worksheet**LINE/VESSEL: DATE: PAGE: of**

GUIDE WORD	DEVIATION	CAUSE	CONSEQUENCE	SAFETY LEVELS	SCENARIO	COMMENTS/ACTIONS

Table 4.17 Time Estimates for Using the HAZOP Study Method

SCOPE	PREPARATION^(a)	EVALUATION	DOCUMENTATION
Simple/Small System	8 to 12 hours	1 to 3 days	2 to 6 days ^(b)
Complex/Large Process	2 to 4 days	1 to 4 weeks	2 to 6 weeks

(a) Primarily team leader and scribe, although others may work during this phase.

(b) Team leader and scribe only. May be shorter for experienced scribes using computer software in the HAZOP study meetings.

Source: CCPS, 1992.

4.4.5 Example Hazard and Operability Studies

Partial HAZOP studies for the example processes described in Section 4.0 are shown in Tables 4.18 and 4.19. A complete example of a HAZOP study can be found in Reference 10.

4.5 Failure Mode and Effects Analysis

4.5.1 Description of the Method

A FMEA is used to examine each potential failure mode of a process to determine the effects of the failure on the system. A failure mode is the symptom, condition, or fashion in which hardware fails. It may be identified as a loss of function, a premature function (function without demand), an out-of-tolerance condition, or a physical characteristic, such as a leak, observed during inspection. The effect of a failure mode is determined by the system's response to the failure.

4.5.2 Analysis Procedure

A FMEA has three steps: (1) defining the process, (2) performing the analysis, and (3) documenting the results. Defining the process for study and documenting the results can be performed by a single person. The analysis itself must be performed by a team.

Table 4.18. Example HAZOP Study for the Dock 8 HF Supply System**LINE/VESSEL: HF Supply Line To Vaporizer****DATE: December 28, 1992****PAGE: 1 of 1**

GUIDE WORD	DEVIATION	CAUSE	CONSEQUENCE	SAFETY LEVELS	SCENARIO	COMMENTS/ ACTION
No	No flow	Valve V-19 closed HF Vaporizer inlet header plugged/frozen	Loss of HF to B-1 process; consequences unknown.	No known protection.	1	Action Item: Determine the level of protection available and potential consequences in B-1 Wing.
		Line rupture	HF release in area; possible injuries/fatalities.	None	2	No Action: Unlikely event; piping protected against external impact.
Less	Low flow	Valve V-19 partially closed HF Vaporizer inlet header partially plugged/frozen	Insufficient HF supply to B-1 process; consequence unknown.	No known protection.	3	Same as #1
			Local rapid flashing, rupture disc/relief valve inadvertently opens, release to stack.	Stack height designed to dissipate release.	4	
			Release HF into storage area; potential injuries/fatalities if people in area.	Valve V-28 closed, forcing release to stack.	5	Action Item: Consider administrative controls or actions to ensure V-28 is closed when operating.
More	High flow	None			6	
	High temperature	Fire; hot weather	Over-pressure; HF release; possible injuries/fatalities.	Local temperature indication on water heating loop.	7	No action: Unlikely event.
	Low temperature	Cold weather	Possible plugging of lines; insufficient vaporization (see consequences of no/less flow scenarios #1-5).		8	
Reverse	Backflow to HF inlet line	None			9	

Table 4.19. Example HAZOP Study for the Cooling Water Chlorination System**LINE/VESSEL: Cooling Water Chlorination System** **DATE: December 28, 1992** **PAGE: of**

GUIDE WORD	DEVIATION	CAUSE	CONSEQUENCE	SAFETY LEVELS	SCENARIO	ACTION
None	No flow - chlorination loop	Pump failure. Loss of electric power to pump.	No chlorine flow to tower basin. Low chlorine concentration in tower basin.	Chlorination pump malfunction alarm.	1	
		Low water level in tower basin.	Potential pump damage. No chlorine flow to tower basin. Low chlorine concentration in tower basin.	Tower basin low water level alarm. Tower basin water level indication.	2	
Less	Low flow - chlorination loop	None identified			3	
More	High flow - chlorination loop	None identified			4	Note: Pump normally runs at full speed.
Reverse	Backflow - in chlorination loop	None identified			5	
None	No flow - chlorine to chlorination loop	No/low level in chlorine drum. Pressure reducing valve fails closed.	No chlorine flow to tower basin. Low chlorine concentration in tower basin.	Local pressure indication on chlorine injection line. Local flow indication on chlorine injection line (rotameter).	6	

DEFINING THE PROCESS. This step identifies the specific vessels, equipment, and instrumentation to be included in the FMEA and the conditions under which they are analyzed. Defining the problem involves establishing an appropriate level of resolution for the study and defining the boundary conditions for the analysis.

The required level of resolution determines the extent of detail needed in a FMEA. The choices for the level of resolution range from the subcomponent level to the system level. To satisfy PSM Rule requirements, most FMEAs should be performed at the major component level. This level provides the best trade-off between the time necessary to perform the analysis and the usefulness of the information gained from it.

Defining the analysis boundary conditions requires the following.

1. Identifying the system or process to be analyzed.
2. Establishing the physical boundaries of the system or process.
3. Establishing the analytical boundaries of the system or process.
4. Documenting the internal and interface functions.
5. Documenting the expected performance of the system, process, or equipment item; the system or process restraints; and the failure definitions of the equipment items, the process, or the system.
6. Collecting up-to-date information identifying the process equipment and its functional relationship to the system.

Functional narratives about the system or process should include descriptions of the expected behavior of the system or process and the equipment components for each operational mode. Narratives should describe the operational profiles of the components and the functions and outputs of each.

To assist in the review, block diagrams should be constructed which illustrate the operation, interrelationships, and interdependencies of functional components for each equipment item. All interfaces should be indicated in these block diagrams.

PERFORMING THE ANALYSIS. The FMEA should be performed in a deliberate, systematic manner to reduce the possibility of omissions and to enhance completeness. All failure modes for one component should be addressed before proceeding to the next component. A tabular format is recommended for recording results. A FMEA worksheet is produced by beginning at a system boundary on a reference drawing and systematically evaluating the components in the order in which they appear in the process flow path. A worksheet such as that shown in Table 4.20 should be completed for each equipment item, as follows.

Failure Mode. The PrHA team should list all of the equipment item and interface failure modes. Given the equipment's normal operating condition, the team should consider all conceivable malfunctions.

Cause(s). If desired, the root causes of the failure mode should be identified. Identification of root causes provides information helpful for ranking hazards.

Operational Mode. If the equipment being analyzed is subject to different modes of operation, each operational mode should be identified and analyzed separately.

Effects. For each identified failure mode, the PrHA team should describe the anticipated effects of the failure on the overall system or process. The key to performing a consistent FMEA is to assure that all equipment failures are analyzed using a common basis. Typically, analysts evaluate effects on a worst-case basis, assuming that existing safety levels do not work. However, more optimistic assumptions may be satisfactory as long as all equipment failure modes are analyzed on the same basis.

Failure Detection Method. The means of failure detection should be identified, such as visual or warning devices, automatic sensing devices, sensing instrumentation, or other indicators. The main purpose of identifying failure detection methods is to determine whether the failure mode is "hidden," i.e., not detectable for some period of time. If there is no means to detect failure, "none" should be entered into the worksheet.

Compensating Provisions. For each identified failure mode, the PrHA team should describe any design provisions, safety or relief devices, or operator actions that can reduce the likelihood of a specific failure or mitigate the consequences.

Severity Class. The severity of the worst consequence should be specified as follows.

Category I	Catastrophic	May cause death or loss of system or process.
Category II	Critical	May cause severe injury, major property damage, or major system damage.
Category III	Marginal	May cause minor injury, minor property damage, or minor system damage.
Category IV	Minor	Is not serious enough to cause injury, property damage, or system damage, but may result in unscheduled maintenance or repair.

Remarks/Actions. For each identified failure mode, the PrHA team should suggest actions for reducing its likelihood or mitigating its effects. The actions suggested for a particular piece of equipment may focus on the causes or effects of specific failure modes or may apply to all of the failure modes collectively.

If the team discovers that a single item failure is not detectable, the FMEA should be extended to determine if the effects of a second failure in combination with the first could have

catastrophic consequences. When a safety, redundant, or back-up component is evaluated, the analysis should consider the conditions that generated the need for the component.

DOCUMENTING THE RESULTS. A FMEA generates a qualitative, systematic reference list of equipment, failure modes, and effects. The results of a FMEA are usually listed in tabular format, by equipment item. Table 4.20 shows a typical worksheet used in performing a FMEA. For each equipment item, the failure modes for that item and, if desired, the root causes for that failure mode are identified. For each failure mode, a worst-case estimate of the consequences is identified. This worst-case estimate assumes the failure of all protection against both the failure itself and the undesired consequences of the failure. The method by which the failure is detected is specified along with any compensating provisions. Finally, any suggestions for improving safety are listed in the table.

The PSM Rule requires that a FMEA be performed by a team, all of whose members participate in the analysis. The most practical means of performing the FMEA is to prepare blank worksheets on viewgraphs or on a large display screen. For each equipment item, the PrHA team reaches a consensus on its failure modes and their causes, effects, detection methods, compensating provisions, severity (if desired), and any remarks or action items.

Staff requirements for a FMEA vary with the size and complexity of equipment items being analyzed. The time and cost of a FMEA is proportional to the size of the process and number of components analyzed. On average, an hour is sufficient to analyze two to four equipment items. For processes or systems in which similar equipment items perform similar functions, the time requirements for completing a FMEA are reduced. Table 4.21 presents estimates of the time needed to perform a PrHA using the FMEA method (CCPS, 1992).

4.5.3 Limitations of Failure Mode and Effects Analysis

Human operator errors are not usually examined in a FMEA, but the effects of human error are indicated by an equipment failure mode. FMEAs rarely investigate damage or injury that could arise if the system or process operated successfully. Because FMEAs focus on single event failures, they are not efficient for identifying an exhaustive list of combinations of equipment failures that lead to accidents.

4.5.4 Example Failure Mode and Effects Analyses

Partial FMEAs for the example processes described in Section 4.0 are shown in Tables 4.22 and 4.23.

4.6 Fault Tree Analysis

4.6.1 Description of the Method

FTA is a systematic, deductive failure analysis that focuses on a particular accident or undesired event called the "top event" and develops the underlying sequence of events leading to the top event. A separate FTA must be performed for each top event.

The FTA method was originally developed to supplement a FMEA. Fault trees, in their original usage, were diagrams indicating how the data developed by FMEAs interact to cause a specific event. The FTA method is most effective in analyzing complex systems with a limited number of well-identified hazards. In most cases, FTAs are used to perform in-depth analyses of hazardous events identified by another hazard evaluation method.

FTA is a deductive method that uses Boolean logic symbols (i.e., AND gates, OR gates) to break down the causes of the top event into basic equipment failures and human errors. The analysts begin with the top event and identify the causes and the logical relationships between the causes and the top event. Each of the causes, called intermediate events, is examined in the same manner until the basic causes for every intermediate event have been identified. The fault tree is a graphic representation of the relationships between basic events and the selected top event. Table 4.24 presents the standard symbols used in fault tree construction to show these relationships.

A fault tree is, itself, a Boolean equation relating basic events to the top event. The equation can be analyzed quantitatively or qualitatively by hand or by using computer code(s). If it is analyzed quantitatively, the probabilities or frequencies of the intermediate events and the top event are calculated. If it is analyzed qualitatively, a list of the failure combinations that can cause the top event is generated. These combinations are known as cut sets. A minimal cut set (MCS) is the smallest combination of basic events that, if they occur or exist simultaneously, cause the top event. These combinations are termed "minimal" because all of the basic events in a MCS must occur if the top event is to occur. Thus, a list of MCSs represents the known ways the top event can occur, stated in terms of equipment failures, human errors, and associated circumstances.

4.6.2 Analysis Procedure

A FTA has four steps: (1) defining the system or process, (2) constructing the fault trees, (3) analyzing the fault trees, and (4) documenting the results. To meet PSM Rule requirements, defining the process for study, performing the analysis, and documenting the results can be performed by a single person. The construction of the fault trees must be performed by a team.

DEFINING THE PROCESS. This step identifies the specific top event or events to be evaluated and the boundary conditions under which they are analyzed. Boundary conditions include the following.

- System Physical Boundaries
- Level of Resolution
- Initial Equipment Configuration
- Initial Operating Condition
- Unallowed Events
- Existing Conditions
- Other Assumptions

Table 4.20. Example FMEA Worksheet

[illegible]

Table 4.21 Time Estimates for Using the Failure Mode and Effects Analysis Method

SCOPE	PREPARATION	EVALUATION	DOCUMENTATION
Simple/Small System	2 to 6 hours	1 to 3 days	1 to 3 days
Complex/Large Process	1 to 3 days	1 to 3 weeks	2 to 4 weeks

Source: CCPS, 1992

Physical system boundaries encompass the equipment, the interfaces with other processes, and the utility/support systems to be analyzed. Along with the physical system boundaries, analysts should specify the *levels of resolution* for fault tree events reflecting failures of both equipment and support systems (i.e., major component level, subcomponent level, system level, and subsystem level). For example, analysts may set the level of resolution at the subsystem level (electrical bus, cooling loop) for support systems.

Other boundary conditions are the *initial equipment configuration* or the *initial operating conditions*. Initial conditions reflect the initial state of all components and support systems that are included in the FTA. This boundary condition describes the system in its normal, unfailed state.

Unallowed events are those that are considered to be incredible or that, for some other reason, are not to be considered in the analysis. For example, wiring failures might be excluded from the analysis of an instrument system. *Existing conditions* are, for the purposes of the FTA, events or conditions considered certain to occur. The unallowed and existing conditions do not appear in the fault tree, but their effects must be considered in developing other fault events as the fault tree is constructed.

Because a broadly scoped or poorly defined top event can lead to an inefficient analysis, the top event should be precisely defined to show the "what," "when," and "where" of the accident. Accordingly, analysts may specify *other assumptions*, as necessary, to define the system or process to be analyzed. For example, analysts may assume that the process is operating at 100 percent of normal capacity.

CONSTRUCTING THE FAULT TREE. Fault tree construction begins at the top event and proceeds, level by level, until all fault events have been traced to their basic contributing

Table 4.22. Partial FMEA for the Dock 8 HF Supply System

DATE:		<u>12/30/92</u>		PAGE:		<u>1</u> of <u>1</u>	
PLANT:		<u>Y-12 Plant</u>		SYSTEM:		<u>Dock 8 HF Supply System</u>	
ITEM:		<u>Pressure Reducing Valve V-13</u>		REFERENCE:		<u></u>	
FAILURE MODE	CAUSE(S)	OPERATIONAL MODE	FAILURE EFFECTS	FAILURE DETECTION METHOD	COMPENSATING PROVISIONS	SEVERITY CLASS	REMARKS/ ACTIONS
Valve open too far	Internal valve malfunction. Operator error. Calibration error.	Operation	High N ₂ pressure at HF cylinders, HF vaporizer - HF vaporizer vessel rupture - HF released to environment. High HF flow to HF vaporizer - high HF flow to B-1 wing - potential liquid HF to B-1 wing.	Local pressure indication on N ₂ line. Local pressure indication between rupture disk and PRV-4 at vaporizer.	PRV-3 at V-13 outlet. PRVs on N ₂ feed lines to HF cylinders. PRV-4 at HF vaporizer.	II	If N ₂ line relief valves lift, vaporizer relief valve should not lift. Relief valve discharges piped to D-wing stack.
Valve closed too far	Internal valve malfunction. Operator error. Calibration error.	Operation	No N ₂ pressure to HF cylinder - no HF flow to HF vaporizer, B-1 wing.	Local pressure indication on N ₂ line.	None	IV	
External leakage	Valve seal leakage.	Operation	Waste on N ₂ . If severe, same as "valve closed too far."	Audible Local pressure indication on N ₂ line, if severe.	None	IV	

Table 4.23. Partial FMEA for the Cooling Water Chlorination System

DATE: <u>1/4/93</u> PAGE: <u>1</u> of <u>1</u> PLANT: _____ SYSTEM: <u>Cooling Water Chlorination System</u> ITEM: <u>Pressure Check Valve</u> REFERENCE: _____							
FAILURE MODE	CAUSE(S)	OPERATIONAL MODE	FAILURE EFFECTS	FAILURE DETECTION METHOD	COMPENSATING PROVISIONS	SEVERITY CLASS	REMARKS/ ACTIONS
Too much flow through valve	Both internal pressure valves fail open	Operation	Excessive chlorine flow to Tower Water Basin - high chlorine level in cooling water - potential for excessive corrosion in cooling water system	Rotameter Daily testing of cooling water chemistry	Relief valve on Pressure check valve outlet	III	None
Too little flow through valve	One or both internal pressure valves fail closed	Operation	No/low chlorine flow to Tower Water Basin - low chlorine level in cooling water - potential for excessive biological growth in cooling water system - reduction in heat transfer	Rotameter Daily testing of cooling water chemistry	Automatic temperature controllers at most heat exchangers	IV	None
Chlorine flow to environment	Internal relief valve sticks open Both internal pressure valves fail open and relief valve opens	Operation	Potential low chlorine flow to Tower Water Basin - see above Chlorine released to environment - potential personnel injury due to exposure	Distinctive odor	Pressure check valve located outdoors - unlikely to accumulate significant concentration	III	Action Item: Consider venting relief valve above ground level

events or basic events. The analysis starts with a review of system requirements, function, design, environment, and other factors to determine the conditions, events, and failures that could contribute to an occurrence of the undesired top event. The top event is then defined in terms of sub-top events, i.e., events that describe the specific "whens and wheres" of the hazard in the top event. Next, the analysts examine the sub-top events and determine the immediate, necessary, and sufficient causes that result in each of these events. Normally, these are not basic causes, but are intermediate faults that require further development. For each intermediate fault, the causes are determined and shown on the fault tree with the appropriate logic gate. The analysts follow this process until all intermediate faults have been developed to their fault causes. The fault causes, or basic events, include equipment failures, human response errors, and initiating events.

EVALUATING THE FAULT TREE. After a fault tree is constructed, it can be input to a fault tree analysis computer program, such as FTAP, IRRAS, or WAM. The output from the computer program is a list of MCSs which cause the top event to occur. For each of the MCSs, the analysts describe the consequences associated with that cut set. Table 4.25 shows a typical worksheet used to document the consequences associated with MCSs.

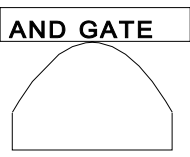
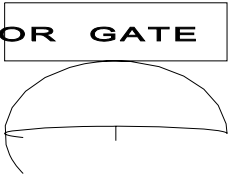
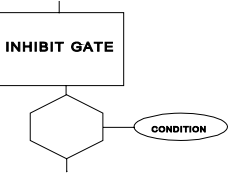
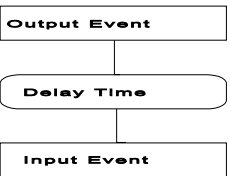
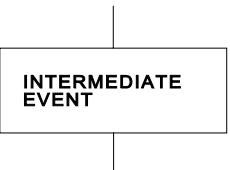
DOCUMENTING THE RESULTS. A ranked list of MCSs for a system, along with the consequence of each cut set, is the ultimate product of a qualitative FTA. Based on the number and type of failures in the MCSs, the PrHA team may recommend improvements to make the top event less likely. The fault tree model itself is often used as a communication tool with both technical and nontechnical decision makers.

4.6.3 Staffing Needs and Time

Although the construction of fault trees is not typically done by team approach, to meet the PSM Rule requirement, all members of a PrHA team should provide input during the construction of fault trees. The PrHA team can meet in a room with a large chalkboard or roll of paper and assign one person to draw the fault trees. The team can come to a consensus on the type (AND, OR) and inputs for each fault-tree gate, and the gates can then be added to the fault tree drawing. However, because FTA develops a model of a system, it is fundamentally not a consensus method. If there is disagreement in the tree construction, then it is likely that the process is not well understood.

Using FTA requires a detailed understanding of how a process or system functions, detailed drawings and procedures, and knowledge of component failure modes and effects. The team leader should be well trained and experienced in constructing fault trees.

Table 4.24. Fault Tree Symbols

	AND Gate	The output event occurs if and only if all input events occur.
	OR Gate	The output event occurs if any of the input events occur.
	INHIBIT Gate	The output event occurs when the input event occurs and the inhibit condition or restriction is satisfied.
	DELAY Gate	The output event occurs when the input event has occurred and the specified time delay has expired.
	INTERMEDIATE Event	A fault event that results from the interactions of other fault events that are developed through logic gates such as those defined above.

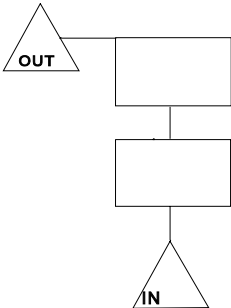
	BASIC Event	A fault event representing a component failure or human error that requires no further development. A basic event is the lowest level of resolution in a fault tree.
	UNDEVELOPED Event	A fault event representing a failure or error which is not examined further because information is not available or because further development is beyond the scope of the study.
	EXTERNAL or HOUSE Event	A fault event representing a condition or event that is assumed to exist either as a boundary condition for the fault tree or because the event always occurs unless a failure takes place.
	TRANSFER IN/OUT Symbols	The TRANSFER IN symbol indicates that the fault tree is developed further at a corresponding TRANSFER OUT symbol. Transfer symbols are used to transfer off-page or to avoid repeating identical logic (with identical events) in several places in a fault tree.

Table 4.25 Minimal Cutset Documentation

TOP EVENT:		Date:	Page:
CUTSET	CONSEQUENCE	SCENARIO #	COMMENTS

Time and cost requirements for a FTA depend on the complexity of the process being analyzed and the level of resolution. With an experienced team, modelling a single top event involving a simple process could require one day or less. Complex processes or large systems with many potential accident events could require many weeks or months, even with an experienced analysis team. Table 4.26 presents estimates of the time needed to perform a PrHA using the FTA method.

Table 4.26 Time Estimates for Using the Fault Tree Analysis Method

SCOPE	PREPARATION	MODEL CONSTRUCTION	QUALITATIVE EVALUATION	DOCUMENTATION
Simple/Small System	1 to 3 days	3 to 6 days	2 to 4 days	3 to 5 days
Complex/Large Process	4 to 6 days	2 to 3 weeks	1 to 4 weeks	3 to 5 weeks

Source: CCPS, 1992.

4.6.4 Limitations of Fault Tree Analyses

FTA is designed to develop the logical combinations of failures required to cause a given event to occur. It is not an efficient, straightforward, practical method for identifying the hazards present in most systems or processes, nor does it necessarily promote a more practical understanding of the hazards, which is the intent of the PSM Rule.

4.6.5 Example Fault Tree Analyses

Partial FTAs for the example processes described in Section 4.0 are shown in Figures 4.3 and 4.4.

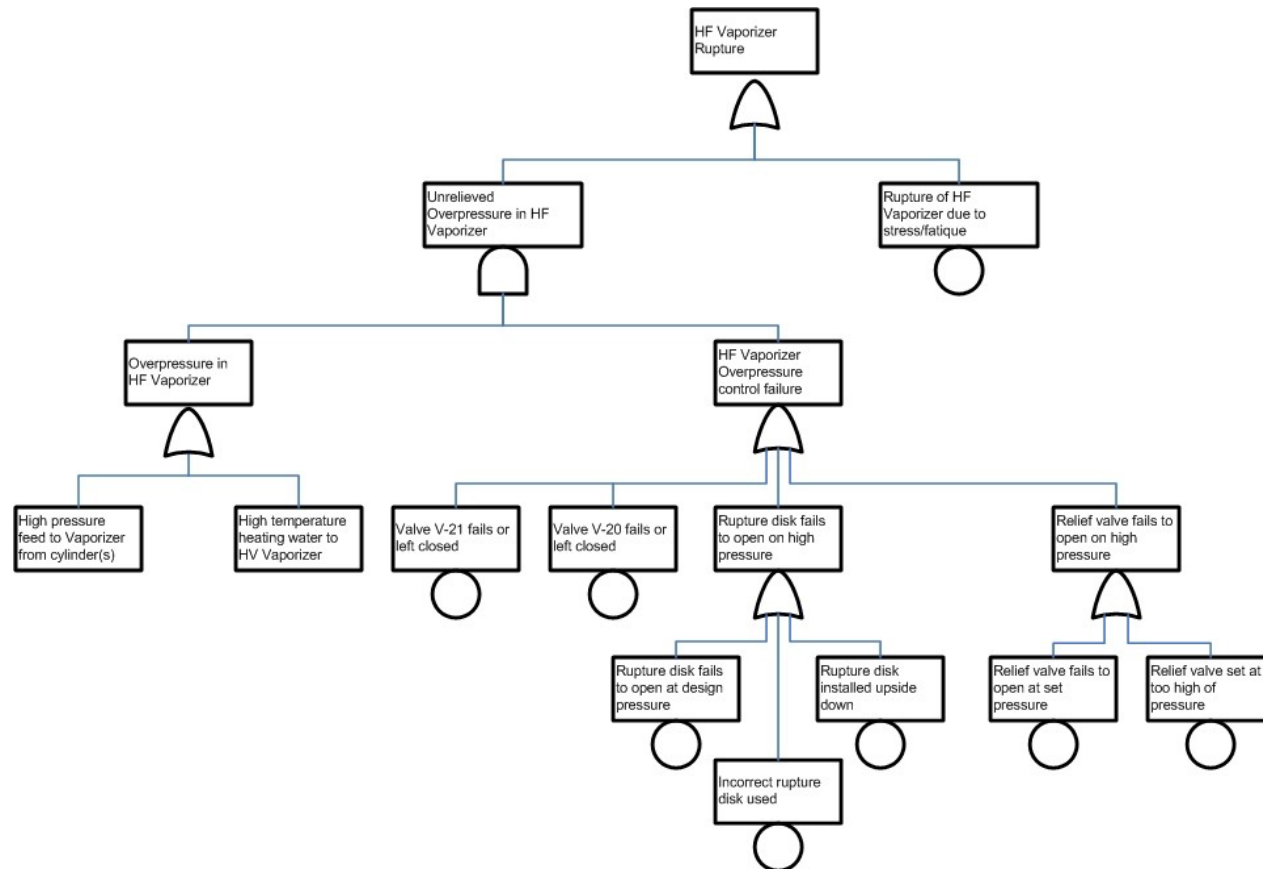


Figure 4.3 Example FTA for the Dock 8 HF Supply System

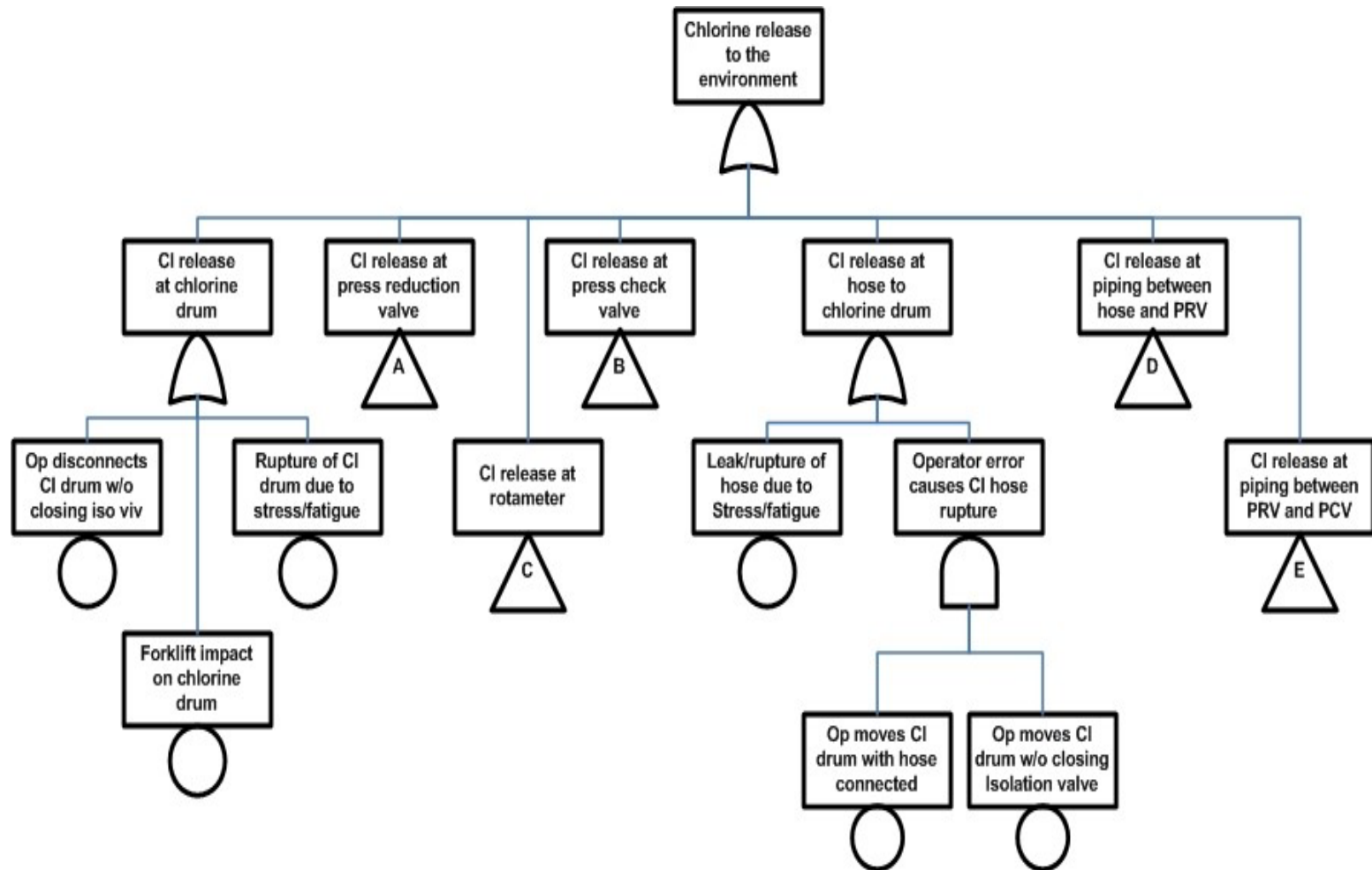


Figure 4.4 Example FTA for the Cooling Water Chlorination System

5.0 REPORTING AND REVIEW OF ANALYSES

5.1 Reporting the Process Hazard Analysis

The format of PrHA documents must conform to the requirements of the PSM Rule and existing guidance for DOE documentation. Two documents are required by the PSM Rule. The first, the PrHA report, contains all necessary information except for a "...system to promptly address the team's findings and recommendations; assure that the recommendations are resolved in a timely manner and that the resolution is documented;..." That information is separately documented, as discussed in Section 6.0 of this handbook. Two useful references on the documentation of PrHAs are Freeman, 1991 and Hendershot, 1992.

TITLE PAGE AND TABLE OF CONTENTS. Because the PrHA must be updated at least every 5 years, the initial and all subsequent analysis dates should be recorded on the report's title page and table of contents. The title page should show the date of the latest revision and reflect the authenticity of the revision by signature(s). The table of contents should show the revision number and the effective date of the revision. The DOE contractor may wish to make the PrHA report a controlled document so that users may verify that they have the latest version.

SUMMARY OF RECOMMENDATIONS. Recommended changes to reduce risk are recorded in the PrHA as action items. This section should report the action items and safety improvement recommendations from the analysis. These action items and recommendations are used to resolve safety issues and to implement corrective actions and safety improvements (see Section 6.0).

PROCESS DESCRIPTION. A separate element of the PSM Rule (paragraph [d] *Process Safety Information*) requires documentation of process details. These details need not be repeated in the process description. However, this section of the report should provide a brief working description of the process, perhaps with a block diagram. It should also describe the location of the process and the potential for exposure of workers. The discussion should consider workers working directly on the process and those that are "co-located" but not directly involved in the process. This section should also discuss the relationship between the location or "siting" of the process and the accident potential.

SCOPE OF ANALYSIS. According to the PSM Rule, the scope of any analysis should include receiving, storage, processing, and loading for delivery of any hazardous chemical covered under the rule. The scope section of the report explains the extent of the treatment of each part of the process. It may or may not include support systems, depending on their inherent hazards and/or interactions with the process.

REVIEW OF PREVIOUS INCIDENTS. This section discusses any incidents relevant to the process. Incidents include releases and "near misses." Incidents should be presented in the

context of related accident scenarios. Recommendations from related scenarios should reflect the incidents.

IDENTIFIED HAZARDS. The identification of hazards is discussed in Section 3.0. This section should present the hazards as identified. It may consist of or include the MSDSs for the chemicals involved (see Section 2.1.1).

ANALYSIS METHODOLOGY. The PrHA method and the justification for selecting it are presented here. It is not necessary to describe the method if it is listed in the PSM Rule (e.g., what-if, checklist, HAZOP study, FMEA, FTA). If any other method is used, it must be described, and the reason for its selection must be presented.

ANALYSIS TEAM. A list of the team members, their roles, and brief biographical sketches are included here. Because the PSM Rule requires a team approach, this section should demonstrate that the PSM team requirements were met. These requirements include expertise in engineering and process operations, experience and knowledge specific to the process being analyzed, and knowledge of the specific hazard analysis method.

SUMMARY OF FINDINGS. The PSM Rule requires a qualitative evaluation of the consequences of engineering and/or administrative control failures, to show the range of possible safety and health effects on workers and offsite populations. This information can be obtained from the PrHA by selecting those scenarios that cover the range of possible health effects, and then discussing the existing *protection* (see Section 3.2). It may be necessary to conduct a rudimentary, quantitative consequence evaluation in order to provide the qualitative information required.

In addition to describing *protection*, the summary should point out any mitigation systems at the facility which were not included in the PrHA (*Mitigation* is not normally included in a PrHA. See Section 3.2). Mitigation systems have the potential to reduce accident impact levels. They include spray systems to reduce release quantities and early warning systems.

The following is an example of information that should be included in the "Summary of Findings."

One scenario from the PrHA results in a release of chlorine from a storage cylinder through an improperly installed fitting. The quantity of chlorine that could leak is limited only by the diameter of the tubing, assuming the connection comes completely loose. Based on a rudimentary evaluation of the release of this quantity of chlorine, it was found that the chlorine concentration that would be dangerous to workers (lung tissue damage) extends to about 50 meters from the fitting, with no concern beyond this distance. Workers are not generally in the area, except for a walk-around inspection once per shift. The worker conducting the walk-around would probably smell the leak before any health effect could occur. Administrative protection includes a leak check of the fittings that the installer performs before leaving the site. Mitigation includes chaining off and clearly marking the area to minimize casual entry.

ANALYSIS DOCUMENTATION. PrHA report documentation should include the PrHA worksheets, checklists, logic diagrams, human reliability analyses, and any other analysis made to better understand the scenarios. The PSM Rule requires that human factors that impact scenarios as *cause* or *protection* be expanded to analyze the basic cause of errors or response failures. For example, a *cause* may identify that an operator can turn the wrong valve to initiate an accident. The PSM Rule requires that basic causes also be identified. For example, valve is not labeled; the operator has not been trained on the operation; or the operator forgot the step. There may be more than one basic cause. (See also Section 3.2, paragraph on Human Factors.)

PROCESS SAFETY INFORMATION. This section need not replicate data stored in other locations, but should provide a list of the drawing numbers, including revision numbers, and other basic data used in the PrHA. The location of these data should be provided.

5.2 Review of the Process Hazard Analysis

After completion, the PrHA report should be reviewed internally. The review starts with an assessment of the team and its credentials. A technical review follows, focusing on the completeness of the analyses and the traceability and understandability of the documentation.

OVERALL APPROACH TO THE PROCESS. Completeness of a PrHA depends on how methodical the PrHA team is in its approach. Reviewers should ask the following.

- Did the PrHA work its way through the process systematically, or did it "jump around," overlooking important scenarios. Scenarios are harder to find if the PrHA does not move methodically from one part of the process to the next.
- Were all parts of the system considered? All hardware and procedures should be considered, from the receipt of hazardous chemicals through their use in the process. In addition, if process connections exist, material flowing into systems where it is not designed to be should also be considered.
- Were all stages and operating modes of the process considered? Review should include analysis of procedures for material receipt and unloading, startup, shutdown (emergency and normal), and transitioning to partial operation (e.g., 100 percent to 500 percent production).
- How long did it take to perform the PrHA? Too short a time could indicate lack of thoroughness. Or the PrHA may have been dominated by one person. Alternatively, the leader might have prepared the PrHA ahead of time and used the meetings to confirm his work.

PROCESS DEVIATIONS. Not all PrHA methods specifically identify process deviations. However, to review the PrHA scenarios for completeness, a reviewer can use process deviations such as those listed in Table 5.1, combined with process parameters.

Table 5.1 Deviations Guide

	NO/NONE	MORE OF	LESS OF
Apply each guide word to relevant parameters/operations to create deviations	Containment lost Procedure step skipped No [Function] No transfer No agitation No reaction	Procedure started too late Procedure done too long Too much [Function] Too much transferred Too much agitation High [controlled variable] High reaction rate High flow rate High pressure or dP (different pressure) High temperature High level; overflow High concentration High pH, viscosity, ...	Procedure started too soon Procedure stopped too soon Not enough [Function] Not enough transferred Not enough agitation Low [Controlled Variable] Low reaction rate Low flow rate Low pressure or dP; Vacuum Low temperature Low level; empty Low concentration Low pH, viscosity, ...
PART OF	AS WELL AS	REVERSE	OTHER THAN
Containment leak/spill Part of procedure step omitted Part of [Function] achieved Part of [Composition] Component missing Phase missing Catalyst deactivated	Extra step performed Extra [Function] Transfer from more than one source Transfer to more than one destination Extra [Composition] Extra species present Extra phase present Impurities; dilution Previous heel present	Steps done in wrong order Reverse [Function] Reverse flow Reverse mixing	Wrong procedure performed Wrong [Function] achieved Transfer from wrong source Transfer to wrong destination Maintenance/test/sampling at wrong time or location Start-up/shutdown of continuous process

INCIDENT CAUSES. Incident *causes* or initiating events should be readily identifiable in any PrHA method. Reviewers should use their experience to assure that all initiating events, including hardware failure modes, operator errors, administrative errors, and loss of utilities, are considered. If the process is in a location subject to external events, the PrHA should include relevant events such as earthquakes, traffic, weather, or accidents at an adjacent process.

CONSEQUENCE EVALUATION. Anomalies are most often found in the *consequence* section of the PrHA. A common mistake is to use the successful actuation of a *protection* device as a consequence, thus omitting the true consequence. For example, if a pressure vessel can be over-pressured due to a system failure, the *consequence* is damage/destruction of the vessel, not opening of the relief valve. It is also necessary to assure that all consequences are listed for every *cause*. For example, a pipe break and spill of vessel contents could result in a runaway reaction due to loss of the chemical and a fire if the chemical is flammable. Finally, the *consequence* must be developed assuming all protection fails. A common mistake is to assume "No Consequences," if *protection* was successful.

IDENTIFICATION OF PROTECTION. Protection reduces the probability of the consequence occurring given that the cause has occurred. There are two key questions to ask when reviewing the *protection* portion of a PrHA. First, is the *protection* capable of preventing the consequence if it functions correctly? Second, will the *protection* function, given the *cause*? For example, a normally open electric solenoid valve will not close after loss of electrical power and, therefore, cannot function as protection under that circumstance. A motor-operated valve also will not operate after loss of electrical power. However, a normally closed electric solenoid valve will automatically close upon loss of power.

DECISION FOR ACTION. A PrHA reviewer needs to know the team's criteria for determining if additional effort is warranted to review a specific scenario or provide risk reduction. After reviewing the criteria, the reviewer should spot check the PrHA to see how the criteria were applied to several scenarios.

This Page Intentionally Left Blank

6.0 ESTABLISHING A SYSTEM FOR RESOLVING ACTION ITEMS AND IMPLEMENTING CORRECTIVE ACTIONS

Activities documenting and tracking implementation of corrective actions or safety improvements are not part of a PrHA report. However, the PSM Rule requires a documented, integrated system for managing and monitoring action items. This system must assure that action items and recommendations are addressed and documented in a timely manner. Implementation schedules for corrective actions or safety improvements must be tracked. Finally, the system must assure that all affected operating and maintenance personnel and other affected employees are notified of planned actions.

In addition to these requirements, if a PrHA is conducted to satisfy safety analysis requirements of 10 CFR 830 Subpart B NUCLEAR SAFETY MANAGEMENT, SAFETY BASIS REQUIREMENTS, the resolution of action items must be documented to obtain approval of the safety analysis and the startup of the facility. In this case, the contractor may be required to satisfy specific safety criteria before an action item is considered resolved.

6.1 Process Hazard Analysis Action Items and Recommendations

The critical result of a PrHA is the list of action items developed by the PrHA team. Action items are written any time the team thinks that additional effort is warranted to review further a specific scenario, to eliminate a hazard, or to reduce risks. Usually, action items do not recommend specific corrective actions. They are meant to alert management to potential problems. Sometimes, action items may suggest alternatives to be considered. However, if a problem is simple, if a PrHA team is quite experienced, or if there is only one obvious solution, an action item may be written to recommend a specific corrective action.

The action items from a PrHA are presented to management for review and evaluation, and for determination of what, if any, corrective actions should be taken to eliminate hazards or to reduce risks through preventative, protective, or mitigative measures. Because many action items may be generated during a PrHA, the team may choose to rank the action items according to the probability of occurrence of their corresponding accident scenarios or the severity of their consequences or both. If the PrHA team is quite experienced, it may also choose to rank the action items based on the anticipated time and resources required to implement changes.

6.2 Criteria for Corrective Actions and Safety Improvements

Management can use a variety of criteria to select and prioritize corrective actions and safety improvements. They include costs, other competing priorities, implementation schedules, the effectiveness of risk reduction, and technical feasibility. These criteria, as well as management decisions about corrective actions, must be documented. If after evaluating an action item, management chooses to take no further action, that decision must also be documented. In addition to requiring documentation of management decisions, the PSM Rule requires a system to track implementation of corrective actions to be made.

6.3 The Corrective Actions System

Implementation of corrective actions is the responsibility of management. In assigning corrective actions, management may consult with the PrHA team to assure full understanding of the hazards identified in the PrHA before corrective actions are taken.

If an action item appears in a PrHA report and management chooses not to implement a corrective action, then the justification for not doing so must be documented and made part of the PrHA records. If management approves a particular corrective action and it is not implemented, justification must also be documented as part of the PrHA records.

Management review of the action items from a PrHA of a large or complex process may result in many corrective actions and safety improvement activities. These actions should be prioritized to facilitate timely implementation.

After approving a prioritized list of corrective actions and safety improvements, management must maintain a system for managing, monitoring, and tracking their implementation. This system must also track delegation of authority for monitoring and reporting.

Monitoring corrective action plans and schedules can be done manually. However, a computerized database can also be used to track all corrective actions. A computerized tracking system is of particular benefit when a large number of activities must be monitored. As a minimum, the system for tracking the status of corrective actions should:

- list and describe the corrective actions;
- provide schedules for completing the corrective actions;
- name the individuals responsible for tracking and reporting on the corrective actions;
- identify the organizations and name the individuals responsible for completing the corrective actions;
- state completion dates.

All documentation and tracking information must be up to date, readily available, and easy to audit.

Because all corrective actions and safety improvements are management decisions, they should be implemented according to DOE Order 5480.19, "Conduct of Operations Requirements for DOE Facilities."

7.0 UPDATING THE PROCESS HAZARD ANALYSIS

Each PrHA must be updated and revalidated at least every 5 years to make sure it accurately reflects current processes and operating experiences.

7.1 Update Team

The PrHA update is performed by a team with expertise in engineering and process operations. The team must include at least one member who has experience and knowledge specific to the process, and one member who is knowledgeable in the PrHA method being used. The team need not include the original PrHA team members, although it may be helpful, for consistency, to include at least one original member. New team members, however, may bring different perspectives to the update.

7.2 Approach

Members of the update team should review a copy of the initial PrHA and check completion of action items. The team should thoroughly review current PSI and descriptions of all process modifications made since the last PrHA report. A thorough review of the PSI is necessary to make sure that the PrHA incorporates any new hazardous materials, process technologies, equipment, and/or operating procedures. Finally, the team should review all findings and resolutions from the last PrHA to assure that they have been adequately addressed.

If the process has changed extensively, it should undergo a new analysis using a PrHA method appropriate to its new configuration. If the process has not changed much, the PrHA is updated considering the changes that were made. Any hazards that were overlooked in the previous analysis or that resulted from process modifications are added to the PrHA. In addition, "lessons learned" from other PrHAs should be incorporated where applicable. In some cases, scenarios may be omitted as a result of risk reduction measures. Updating a PrHA typically takes a third to a half of the time of the original analysis.

7.3 Documentation

The update team must develop a new PrHA report to document the scope and approach of its analysis as well as any new hazards, scenarios, and action items. Justification must be provided for removing any scenarios from the last PrHA. The report should receive close scrutiny, both for compliance with the PSM Rule and for explanations of new action items. Guidance for reporting the PrHA results is given in Section 5.1. The updated report is submitted to management for review and approval, following the same procedure as an initial PrHA.

The PSM Rule requires that PrHAs for all covered processes, along with documentation of resolutions of recommendations, be retained for the life of the process.

8.0 RELATIONSHIPS OF PROCESS HAZARD ANALYSES TO OTHER DOE REQUIRED HAZARD ANALYSES

Because a PrHA can require a substantial investment, it is important to identify potential overlap with other DOE hazard analysis requirements. This section provides a recommended approach for satisfying the PSM Rule and the related requirements of a nuclear safety analysis report (SAR).

10 CFR 830 Subpart B specifies that hazard and accident analyses be included in safety analyses for nuclear facilities. Two nuclear SAR topics overlap with the PrHA.

- Topic 5: Hazard Analysis and Categorization
- Topic 11: Analysis of Accident Conditions

These topics are the subject of DOE Standard DOE-STD-1027-92 (CH-1), "Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Nuclear Safety Analysis Reports," which provides guidance for facility managers. They are also discussed in the DOE Standard DOE-STD-3009-94, "Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports," which describes a SAR preparation method that is acceptable to DOE.

The requirements of DOE-STD-1027-92 (CH-1) are used as the basis for identifying the overlap of nuclear facility safety analysis requirements with the requirements of the PSM Rule. According to DOE-STD-1027-92 (CH-1), the level of hazard analysis required for a nuclear facility SAR is determined by the facility's nuclear hazard classification as follows:

NUCLEAR HAZARD CATEGORY 3 FACILITIES. Minimal hazard and accident analyses are required. The PrHA should provide information to the safety analysis on release mechanisms, engineering analysis, and consequence analysis.

NUCLEAR HAZARD CATEGORY 2 FACILITIES. This category requires use of one of several analytical methods for developing qualitative accident scenarios. The choices are generally⁶ compatible with the requirements of the PSM Rule. If the PSM Rule requirements for PrHAs

6. Event Tree Analysis (ETA) is suggested by the DOE-STD-1027-92 (CH-1), but not included in the PSM Rule. However, the PSM Rule does allow the use of "an appropriate equivalent methodology." Hence, if ETA is to be used as the PrHA, the PrHA report must justify that the ETA method is appropriate and equivalent to the methods listed in the rule.

are met, the resulting analysis should significantly contribute to the analysis required under the DOE-STD-1027-92 (CH-1) for release mechanisms. However, analyses beyond PSM Rule requirements may be needed to comply with other SAR requirements for Nuclear Hazard Category 2 Facilities.

NUCLEAR HAZARD CATEGORY 1 FACILITIES. Fault tree/event tree analyses are required if the facility is a large reactor. If the facility is not a reactor and a PSM Rule PrHA is required, the analyses can be conducted as described for Nuclear Hazard Category 2 Facilities. Different systems or processes within the facility may be analyzed using different methods. For example, HAZOP studies may be used as the PrHA method for processes that contain chemical hazards. Fault tree/event tree analyses may be used to analyze systems that do not need to comply with the PSM Rule.

All documents required by the PSM Rule should be referenced and their significant findings summarized in the SAR. References and summaries should include not only the results of the PrHA, but also all documents concerning the resolution of the PrHA team's findings.

9.0 REFERENCES

Burk, Arthur F., 1992. "Strengthen Process Hazards Reviews," Chemical Engineering Progress, June 1992, pp. 90-94.

Center for Chemical Process Safety (CCPS), 1992. Guidelines for Hazard Evaluation Procedures, Second Edition with Worked Examples; Publication G18; American Institute of Chemical Engineers, New York.⁷

Freeman, Raymond A., 1991. "Documentation of Hazard and Operability Studies," Plant/Operations Progress, July 1991, Vol. 10, No.3.

Hendershot, Dennis C., 1992. "Documentation and Utilization of the Results of Hazard Evaluation Studies," prepared for presentation at the AIChE 1992 Spring National Meeting, New Orleans, LA. Rohm and Haas Company, Bristol, PA.

Hummer, John J., John M. Googin, Ph.D, Michael W. Knazovich, Paul R. Wasilko, and Janice West, 1992. "Report of Investigation of Accidental Release of Hydrogen Fluoride from the Y-12 Plant Oak Ridge, Tennessee, January 24, 1992," Martin Marietta Energy Systems, Inc., Oak Ridge, TN, March 1992.

King, Ralph, 1990. "Safety in the Process Industries," Butterworth-Heinemann, Ltd., 1990.

U.S. Department of Defense, MIL-STD-882-C, "Military Standard System Safety Program Requirements," Washington, DC, January 1993.

U.S. Department of Energy, DOE Order 5480.19 (Chg 2), "Conduct of Operations Requirements for DOE Facilities," Washington, DC, July 1990.

7. Publications by the CCPS may be obtained from:
American Institute of Chemical Engineers
Publication Sales
3 Park Avenue
New York, NY 10016-5991
Tel. (212) 591-7319 or (800) 242-4363

U.S. Department of Energy, DOE Standard, DOE-STD-1027-92 (CH-1), "Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23 Nuclear Safety Analysis Reports," Washington, DC, September, 1997 .

U.S. Department of Energy, DOE Standard, DOE-STD-3009-94 CN2, "Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports," Washington, DC, July 1994.

U.S. Department of Energy, DOE Handbook, DOE-HDBK-1101-2004, "Process Safety Management for Highly Hazardous Chemicals," Washington, DC, August 2004.

U.S. Department of Energy, "Example Process Hazard Analysis of a Department of Energy Water Chlorination Process," DOE/EH-0340, September 1993.

Title 29 Code of Federal Regulations (CFR) Part 1910, "Process Safety Management of Highly Hazardous Chemicals; Explosives and Blasting Agents; Final Rule," February 24, 1992.

Title 10 Code of Federal Regulations (CFR) Part 830, Nuclear Safety Management; Final Rule, April 10, 2001.

CONCLUDING MATERIAL

Review Activities:

DOE HQ

DP
EH
EM
ER
NE
SS

FIELD OFFICES

AL
ID
NV
Oakland
NV
RF
SR

Preparing Activity:

DOE-EH-52

Project Number:

SAFT-0096

PROJECT OFFICES

GJ