6

Process Hazard Analysis

6.1. Overview

A Process Hazard Analysis (PHA) is an organized effort to identify and analyze the significance of hazardous scenarios associated with a process or activity. PHAs are used to pinpoint weaknesses in the design and operation of facilities that could lead to accidental chemical releases, fires, or explosions and to provide organizations with information to aid in making decisions for improving safety and managing the risk of operations.

Over the last several decades, the chemical process industry has developed a repertoire of techniques for performing PHA; other techniques have been adapted from the nuclear, aerospace, and electronics industries. This chapter briefly describes the more commonly used PHA techniques, many of which are described in greater detail in the CCPS book, Guidelines for Hazard Evaluation Procedures, Second Edition with Worked Examples.

6.1.1. Introduction

The PHA is the cornerstone of an organization's overall process safety management (PSM) program. By identifying the key design features, process conditions, and operating practices required for the safe operation of the facility, PHA serves as the basis for other PSM elements. Therefore, results of the PHA should be concisely and accurately documented in an organized manner that makes this information readily available to those responsible for implementing the other PSM elements.

This chapter briefly describes the results obtained from each technique and provides documentation guidance. Since one of the purposes of PHA is to identify needed changes, there is typically a considerable follow-up effort required to ensure the proper resolution of all proposed changes and recommendations. Follow-up systems intended to track and ensure the resolution of such recommendations are also described.
As with the other PSM elements, there is also a second documentation task required to ensure the consistent, effective implementation of the PHA element, that is, the description of the program defining just how the PHA element will be performed (e.g., who is responsible, how often it will be done, and in what manner). Suggested aspects of the program description that should be considered for documentation are also addressed.

6.1.2. Goals and Benefits

The major goals of performing PHA are to allow implementation and application of potentially hazardous chemical processes and facilities for manufacturing chemical products in a safe and cost effective manner. This is achieved by developing detailed knowledge of the actual hazards, and deriving design, construction, operation, and control approaches to minimize anticipated dangers.

Benefits to be gained include reducing all types of risks: human, property, financial, and legal (e.g., regulatory, litigation stemming from incidents) and providing management with a solid technical basis upon which to plan for long term, profitable business.

6.2. Description of Process Hazard Analysis

6.2.1. Objectives

Five intended objectives in conducting a PHA are to:

- identify the hazards inherent in the process or activity;
- identify the credible human and/or equipment failures likely to lead to accident scenarios;
- evaluate the consequences and likelihood of the various accident/incident scenarios, that is, assess the risk;
- propose changes where warranted, to equipment design, process conditions, and operating procedures, to mitigate the risk to a tolerable level; and
- document the PHA study in a sufficiently complete, accurate, and concise manner in order to:
  - provide a historical record of the results of the reviews;
  - establish adequacy and applicability of the PHA;
  - allow the use of the information learned from the review to further enhance the safety of the facility operation; and
  - provide a basis for future safety studies for that facility.

Each PHA technique has unique strengths and weaknesses. The logic underlying the decision of which PHA technique to select is complex and involves many factors, including those listed in Table 6-1. Detailed guidance on technique
TABLE 6-1. Factors That Could Influence the Selection of Hazard Evaluation Techniques

- motivation for the study;
- type of results needed;
- type of information available to perform the study;
- characteristics of the analysis problem;
- perceived risk associated with the subject process or activity;
- resource availability and analyst/management preference;
- amount of experience available with the technology involved; and
- organization and/or industry accident/incident experience.

Selection is provided in the CCPS book, *Guidelines for Hazard Evaluation Procedures, Second Edition with Worked Examples*, previously cited. The results derived from the application of the various techniques will vary somewhat in format and degree of detail, thus affecting documentation methods.

6.2.2. Method 1: Safety Reviews

*Description*—Safety Reviews appear under a variety of names, such as process safety review, design review, or loss prevention review. The safety review can be applied at any stage of a project or plant life cycle, before or after construction. When performed on existing facilities, the safety review typically involves a walk-through inspection that can vary from an informal routine visual examination to a formal examination, performed by a team, that takes several weeks.

Safety reviews are intended to identify plant conditions or operating procedures that could lead to an accident or incident and result in injuries, significant property damage, or environmental impacts. The review could include the following activities:

- a walk through the plant (or the design if the plant is not yet built);
- interviews with key people such as designers, operators, maintenance staff, and management;
- reviews of operating, maintenance, and emergency procedures;
- reviews of equipment test records; and
- reviews of plant design documents (e.g., drawings, and specifications).

Safety review inspections and interviews concentrate on significant process safety issues rather than just facility housekeeping. Safety reviews can be used to identify areas that require more detailed study, areas where some significant
change has made study necessary, or areas where some gradual progressive change in operating procedure or philosophy has occurred.

The objectives of the safety review are to:

- note and list safety issues requiring further examination or more detailed review;
- identify apparent departures from the original or current design or operating procedures;
- identify new issues;
- propose a course of action or a recommendation for follow-up; and
- document the results in a comprehensive report. There is no specific style required for this report.

Reference

6.2.3. Method 2: Checklist Analysis (CL)

Description—In a checklist analysis (CL), the hazard/risk analyst, or team, uses a list of specific items to identify known types of hazards, design deficiencies and potential accident scenarios associated with process equipment and operations. In effect, the traditional checklist represents a set of standardized design or operating practices against which the process or facility can be assessed. Other checklists are more general in scope and prompt the formulation of more original what-if type questions within the review, see Method 5: What-If Analysis (WI) and Method 6: What-If/Checklist Analysis (WICL). Many checklists of each type exist and have been published in the literature.

Example—Table 6-2 shows the use of a checklist and one method for recording answers; the first column repeats all the questions or prompts in the checklist, and the third column records the basic answer to the question as prompted. If necessary, additional columns can be used to record recommendations, actions completed, dates required for recommendation resolution, and/or responsibilities assigned. Some checklists, as published, do not have adequate space for questions/answers to appear alongside each other. Such checklists may need to be retyped, with the responses shown below or alongside the questions. If such lists are used regularly, they can be converted to word processor or computer files.

A traditional checklist generates a list of responses to the standard checklist questions, usually indicating compliance or noncompliance. The traditional checklist can also be used to develop a list of identified hazards and suggested corrective actions. More general checklists may produce lists of questions that require further evaluation before hazards can be assessed or recommendations proposed. A spreadsheet or a word processing program that permits columnar editing can be used for the record.
Specialist commercial software useful for this method includes:

- HAZSEC Plus (DNV-Technica, Temecula, CA);
- PHARA (Midwest Technologies, Inc., Kingsport, TN); and
- SAFEPLAN (DuPont, Westlake Village, CA).

**References**


### 6.2.4. Method 3: Relative Ranking Analysis

**Description**—One of the challenges of a PHA program is that of establishing priorities to determine which parts of a large facility most urgently require attention. To address this problem, some chemical companies, such as Dow and ICI, have established review programs to determine the relative ranking of hazards. Other organizations have developed their own internal ranking systems or adapted existing systems to provide more options or to consider different aspects.
The Dow Fire and Explosion Index, the ICI Mond Index, and others are based on assigning quantitative values to various aspects of a plant's design features, operating conditions, and inventory. Using any of these index methods, it is possible to compare one plant with another, or one area of a plant with another. Also, since some general hazard scales are offered as guidance, individual facilities can be ranked in qualitative terms, for example, low, moderate, or severe risk.

Other indexes have been developed more recently, including:

- Dow, Chemical Exposure Index, (CEI);
- EPA, Threshold Planning Quantity, (TPQ); and
- OSHA, Substance Hazard Index, (SHI).

The last two indexes are less comprehensive in that they relate largely to the hazardous properties of individual substances. However, they are useful for general guidance and for regulatory compliance.

All relative ranking methods should result in an ordered list of processes, equipment, operations, or activities. Both the Dow and Mond Indexes incorporate calculation sheets on which ratings are applied to a wide variety of process and operating conditions. Other results, such as index scores, factor scores, graphs, etc., depend upon the particular technique used. Also, lists of recommendations intended to lower individual risk rankings may be produced, along with responsibility assignments and deadlines for recommendation implementation.

It is possible with both the Dow and Mond indexes to use computerized methods—either standard spreadsheets or special software. Available commercial software includes:

- MOND INDEX (ICI Pk, Northwich, UK)
- RISK*RANK (Battelle Columbus Division, Columbus, OH); and
- SPECTRUM/PC-F&E (Battelle Columbus Division, Columbus, OH).

References
Dow Chemical Company, Chemical Exposure Index (CEI), AIChE, 1994

6.2.5. Method 4: Preliminary Hazard Analysis

Description—The preliminary hazard analysis is a technique that was derived from the Military Standard System Safety Program Requirements. It can be used early in the design process and is generally followed by more in-depth studies. Facility characteristics considered in the analysis include:
• materials being handled and their properties;
• plant equipment;
• facility layout;
• operating environment;
• operational activities (e.g., testing, maintenance); and
• interfaces among system components.

The study is normally qualitative but can provide information to assist with prioritization of scenarios for further studies, either qualitative or quantitative.

The team assesses the importance of each plant characteristic listed above and identifies hazardous scenarios for each. These scenarios can then be assigned a criticality rating that can be used to address the scenarios in order of importance in later design work or safety studies. The results are usually in text format, but may include some tabular material. Available commercial software useful for this method includes HAZMAN (PLG, Inc., Newport Beach, CA).

References

6.2.6. Method 5: What-If Analysis (WI)

Description—The What-If (WI) analysis technique is a creative, brainstorming approach in which a team of experienced people familiar with the subject process or facility ask questions, voice concerns and develop scenarios for possible undesired events. The purpose is to identify hazardous situations, or specific accident scenarios that could produce an undesired hazardous event.

Results of a WI Analysis are most commonly recorded using a simple tabular form. Information entered on the form can include:

• headings detailing the section of the facility or subsystem being studied, relevant drawings, names of the individuals conducting the analysis, and the date;
• columns setting out the following:
  — the proposed what-if question or concern;
  — the identified scenario;
  — consequence/hazard for each scenario;
  — existing safeguards to prevent or mitigate the consequences;
  — recommendation, required action, including investigation outside the meeting;
  — names of individuals who are to execute action or follow up the question (optional, may be contained in subsequent documents); and
  — required completion dates for action plans (optional, may be contained in subsequent documents).
Such records can either be manually recorded, or recorded during the analysis on a personal computer (PC) using a simple form as described above. Commercially produced software is also available specifically for this type of analysis, although simple alternatives that include the above information are not difficult to create with spreadsheet or word processing software. An example of a WI worksheet is given in Table 6-3.

Some of the commercial software programs useable for WI are:

- **HAZSEC Plus** (DNV Technica Inc., Temecula, CA);
- **HAZPRO** (DiGraphics, Inc., Houston, TX);
- **PHARA** (Midwest Technologies, Inc., Kingsport, TN);
- **SAFEPLAN** (DuPont, Westlake Village, CA); and
- **WHAT IF-PC** (PrimaTech, Inc., Columbus, OH).

References


6.2.7. Method 6: What-If/Checklist Analysis (WICL)

**Description**—The What-If/Checklist (WICL) method is a hybrid of *What-If analysis (WI)* and *Checklist analysis (CL)*. It is used to capitalize on the best attributes of the two methods. The WI analysis is creative, and the CL analysis is systematic and experience based. In combination, the advantages of each method are synergized while the shortcomings are minimized.

The WICL analysis is normally approached in one of two ways. It may begin with a WI team review that allows a creative approach to the hazard analysis, followed by a CL review to ensure completeness. Alternatively, the CL and WI reviews may be reversed, where the CL is reviewed and used as a springboard for WI scenario creation by team members. In either approach, all the advantages of both the WI and CL methods can be realized.

The format for documentation can be in either text or tabular form as described for the individual CL or WI.

Currently available commercial software includes:

- **HAZSEC Plus** (DNV Technica, Inc., Temecula, CA);
- **HAZPRO** (DiGraphics, Inc., Houston, TX);
- **PHARA** (Midwest Technologies, Inc., Kingsport, TN);
- **SAFEPLAN** (DuPont, Westlake Village CA); and
- **WHAT IF-PC** (PrimaTech, Inc., Columbus, OH).
**TABLE 6-3**  
What If Worksheet Example (Page 1 of 3)

<table>
<thead>
<tr>
<th>What if . . .?</th>
<th>Consequence/Hazard</th>
<th>Recommendation</th>
<th>Responsible Individual</th>
<th>Initial and Date when Resolved</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Ethylene feed is contaminated</td>
<td>Typical contaminant in ethylene is oil. Oil will react energetically with chlorine. However, the amount of oil in ethylene is usually small, and the large quantity of ethylene dichloride (EDC) in the reactor should quench any oil/chlorine reaction. Water is also a trace contaminant</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
1.a Verify availability of high-purity ethylene and reliability of supply  
1.b Determine the reaction kinetics for oil/chlorine reactions. Examine the reaction kinetics for chlorine/water reactions |  
1.a Ethylene expert  
1.b Chemist |
<table>
<thead>
<tr>
<th>What if . . .?</th>
<th>Consequence/Hazard</th>
<th>Recommendation</th>
<th>Responsible Individual</th>
<th>Initial and Date when Resolved</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Cl₂ feed is contaminated</td>
<td>Typical contaminant in chlorine is water. Large quantities of water in chlorine would cause equipment damage in the chlorine plant and cause a shutdown well before it made it to the VCM plant. Small quantities of water should be no problem</td>
<td>2. Verify water content in chlorine supplies is very low</td>
<td>2. Chlorine expert</td>
<td></td>
</tr>
<tr>
<td>What if . . .?</td>
<td>Consequence/Hazard</td>
<td>Recommendation</td>
<td>Responsible Individual</td>
<td>Initial and Date when Resolved</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>-------------------------------</td>
</tr>
</tbody>
</table>
| 3. A feed pipeline breaks | 3. Chlorine — A large release of liquid chlorine would occur, which would create a large chlorine vapor cloud  
Ethylene — A large liquid ethylene release would occur, resulting in a large ethylene vapor cloud, which is a potential fire and explosion hazard | 3.a Consider supplying chlorine vapor to the VCM plant  
3.b Evaluate ABC’s abilities to handle highly flammable materials. Consider additional fire safety training and protection equipment  
3.c Consider remote-controlled feed | 3.a Chemist  
3.b Plant fire chief, corporate training officer  
3.c Engineer |                               |
| 4. The feed rates are out-of-balance | 4. A runaway reaction may be possible. An acceptable operating range is not yet known | 4.a Examine the reaction rates at various ethylene/chlorine feed ratios | 4.a Chemist (to communicate with research) |                               |
References

6.2.8. Method 7: Hazard and Operability Study (HAZOP)

Description—The Hazard and Operability Study (HAZOP) is a rigorous, systematic study into the consequences of process deviations from the design intent that may cause undesirable hazard or operability problems. The HAZOP was originally developed by ICI in the United Kingdom in the early 1970s from the application of method study techniques to design problems.

The basic format of the documentation for a HAZOP study is universal, but many variants exist. Whether the study is recorded manually on blank forms, on chart pads, or on a PC using special software, documentation requirements are similar.

The worksheet consists of two parts:

- headings detailing the study team and the precise design intent of the line, vessel, node, subsystem or subsection being studied; and
- a record, usually tabular, of potential deviations from the declared design intent, and the likely expected outcome.

A third section exists, sometimes separately, to record actions and responses for management control. A typical HAZOP worksheet is shown in Table 6-4 (the analysis was conducted on the process illustrated by the P&ID shown on Figure 5.3). The following features of Table 6-4 should be noted:

- **Part 1—Heading.** These items should be recorded:
  - who was on the study team and when (or use an attendance roster in the report);
  - project number/title;
  - area of facility being studied;
  - precise identification of the line or vessel subject to study in the table;
  - the design intent or objective of the line/vessel (e.g., liquid transfer, storage) flow rate, temperature, pressure, normal composition; and
  - other key parameters.

This information defines the normal or design intent from which the team will identify how deviations can occur.

- **Part 2—Deviations.** This section should list, in sequential order of questioning:
  - deviation from the design intent (parameter and guide word);
  - possible causes of deviation;
  - probable consequences of the deviation;
—safeguards or protection;
—required actions/investigations/questions—Note (a);
—response to actions/investigations/questions—Note (b);
—persons responsible for actions/investigations/questions—Note (c); and
—priority rating and/or hazard potential rating—Note (d).

Note (a) Required Actions/Investigations/Questions may also include serial numbers for future management reference.

Note (b) Responses may be recorded separately, along with the relevant question and reference to the study table, for subsequent follow-up.

Note (c) Persons Responsible should identify the individual who is to be responsible for the reply or action. It may also include a required completion date.

Note (d) Priority Ratings may include numbers or symbols for ratings for priority or hazard potential.

Storage and Retrieval—The worksheet record of a HAZOP study can extend from a few sheets for a small/simple facility to possibly 1,000 sheets or more for a large/complex installation. During the recording process, a system that provides a unique record of every sheet should be considered. One method is to number each study node, table or section, from 1 upward. Each of these nodes might contain one or more pages, which could be numbered, page 1 of 4, page 2 of 4, etc. The convention selected for naming computer files should allow for quick identification and retrieval, for example by incorporating the drawing number.

HAZOP studies can be performed with any of a variety of commercially prepared software for use on personal computers. These include:

- CAHAZOP (NUS Corporation, San Diego, CA);
- HAZOP (Lihou Technical & Software Services, Aston, UK);
- HAZOP-PC (PrimaTech, Inc., Columbus, OH);
- HAZOPtimizer (A.D. Little, Cambridge, MA);
- HAZSEC Plus (DNV Technica, Inc., Temecula, CA);
- HAZPRO (DiGraphics, Inc., Houston, TX);
- HAZTEK (Westinghouse Electric Corp, Pittsburgh, PA);
- LEADER (JBF Associates, Knoxville, TN); and
- SAFEPLAN (DuPont, Westlake Village, CA).

In addition, some organizations have adapted word processing or database software to provide their own customized worksheets for HAZOP recording.

References


**TABLE 6-4**

HAZOP Worksheet Example

**P&ID No:** E-250  
**Revision:** D  
**Meeting Date:** 9/5/90  
**Team:** Mr. Smart, Mr. Associate, Ms. Piper, Mr. Stedman, Mr. Volt (all from the ABC Anywhere Plant)

<table>
<thead>
<tr>
<th>Item Number</th>
<th>Deviation</th>
<th>Causes</th>
<th>Consequences</th>
<th>Safeguards</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 LINE — AIR SUPPLY LINE TO INCINERATOR (INTENTION: SUPPLY 15,000 SCFM OF AIR TO INCINERATOR AT AMBIENT TEMPERATURE AND 3 IN. WC)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>No flow</td>
<td>1 — Air fan #1 fails off</td>
<td>A — Incinerator shuts down. Possible release out the scrubber stack. Potential incinerator explosion if shutdown interlocks fail</td>
<td>1 — Redundant fan on standby with autostart</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 — FCV-1 fails closed</td>
<td></td>
<td>A — Low-low air pressure (PSLL-I) shutdown interlock</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 — FT-1 fails — high signal</td>
<td>A — Incinerator shuts down. Possible release out the scrubber stack. Potential incinerator explosion if shutdown interlocks fail</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 — FT-2 fails — low signal</td>
<td>1,2,3,4,6 — Multiple incinerator shutdown interlocks (temperature, flame)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 — Loss of electric power</td>
<td>1,5 — Automatic shutdown upon loss of electric power</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>6 — Plugged air screen</td>
<td>6 — Air screen cleaned weekly</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5 — FCV-1 fails open on loss of electric power</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2,3,4 — Mechanical stop on FCV-1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2</td>
<td>Low flow</td>
<td>1 — FCV-1 fails — partially closed</td>
<td>A — Incinerator shuts down. Possible release out the scrubber stack. Potential incinerator explosion if shutdown interlocks fail</td>
<td>1,2,3 — Mechanical stop on FCV-1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 — FT-1 fails — high signal</td>
<td></td>
<td>4 — Air screen cleaned weekly</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 — FT-2 fails — low signal</td>
<td>A — Low-low air pressure (PSLL-1) shutdown interlock</td>
<td>A — Multiple incinerator shutdown interlocks (temperature, flame)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 — Plugged air screen</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| 1.3 | High flow | 1 — FCV-1 fails open               | A — Poor combustion, with potential release of flammable gas out the scrubber stack. Excessively high air flow may blow flame out causing a shutdown | A — Multiple incinerator shutdown interlocks (temperature, flame) |
|     |           | 2 — FT-2 fails — high signal       |                                                                          | 2 — FT-1 closing to reduce air flow |
|     |           | 3 — FT-1 fails — low signal        |                                                                          | 3 — Operator inadvertently starts fan #2 (fan #1 still running) |
|     |           | 4 — Operator inadvertently starts fan #2 (fan #1 still running) |                                                                 |                                      |

| 1.4 | Low temperature | No consequences of interest |
| 1.5 | High temperature | No consequences of interest |

*The consequences and safeguard numbers correspond to the numbered causes. The letter "A" indicates that the respective consequences and safeguards apply to all of the listed causes.*
6.2.9. Method 8: Failure Modes and Effects Analysis (FMEA)

Description—Failure Modes and Effects Analysis (FMEA), sometimes extended to Failure Modes, Effects and Criticality Analysis (FMECA), is used to examine the way each item of equipment can fail and the effect the failure could have on the plant or system. In addition, a criticality rating for each failure can be developed, if required, leading to prioritization of necessary actions.

An FMEA analysis generates an itemized list of equipment pieces and an associated list of failure modes appropriate to each. For each failure mode for each equipment item, the analyst or team identifies the effects (consequences) of the failure, as well as any existing safeguards. Recommendation for further safeguards are proposed, where warranted. Additionally, in a FMECA, a semiquantitative evaluation is proposed for the frequency of the failure and the significance or severity of its consequence.

Text or a multicolumn analysis form may be used to display the results. The heading of the analysis table should adequately identify the study team and date, and the equipment or system being studied. An example of a FMEA worksheet is given in Table 6-5 (the analysis was conducted on the process illustrated by the P&ID shown on Figure 5.3).

Available commercial software includes:

- CARA (DNV Technica, Inc., Temecula, CA);
- FIABEX (Institution of Quality Assurance, London, UK);
- FMEA-PC (PrimaTech, Columbus, OH);
- HAZOPtimizer (A.D. Little, Cambridge, MA);
- HAZSEC Plus (DNV Technica, Inc., Temecula, CA); and
- SAFEPLAN (DuPont, Westlake Village, CA).

References


International Organization for Standardization, Failure Mode and Effects Analysis, ISO CEI/812: 1985, Geneva, Switzerland

6.2.10. Method 9: Fault Tree Analysis (FTA)

Description—A fault tree is a graphical model that illustrates combinations of failures that will cause one specific failure scenario of interest, called a top event. FTA is a deductive technique that uses Boolean logic symbols—that is, AND gates and OR gates—to break down the causes of a top event into basic events involving equipment failures and human errors. The analyst begins with an accident or undesirable event that is to be avoided and identifies the immediate causes of that event. Each of the immediate causes, called fault events, is further examined in the same manner until the analyst has identified the basic causes of each fault event.
<table>
<thead>
<tr>
<th>Item Number</th>
<th>Component</th>
<th>Failure Mode</th>
<th>Effects</th>
<th>Safeguards</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Flame scanner UVL-1B</td>
<td>No signal change</td>
<td>Loss of capability to initiate an incinerator shutdown upon loss of flame. Potential incinerator fire or explosion if flame extinguished</td>
<td>Redundant UVL</td>
<td>Verify the reliability of the UVLs</td>
</tr>
<tr>
<td>False flameout signal</td>
<td></td>
<td></td>
<td></td>
<td>Multiple incinerator interlocks (temperature, fuel, and air)</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>Shutdown is alarmed. Operators verify shutdown actions</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>False flameout signal</td>
<td>Inadvertent incinerator shutdown. Potential incinerator explosion if incinerator fuel not shut off</td>
<td></td>
<td>Double block and bleed valves in fuel lines</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Three-way shutoff valve in vent line</td>
</tr>
</tbody>
</table>
or reaches the boundary established for the analysis. The resulting fault tree model displays the logical relationships between basic events and the selected top event. The advantage of the schematic nature of FTA is that it clearly shows what the causal events are, which can lead to developing means to control or eliminate those events.

Top events are specific hazard scenarios that are typically identified through the use of other hazard scenario identification techniques, e.g., WICL, HAZOP, FMEA. A fault tree model can be used to generate a list of the combinations of failure modes that can cause the top event of interest. These failure mode combinations are known as cut sets. A minimal cut set (MCS) is a smallest combination of component failures which, if they all occur or exist simultaneously, will cause the top event to occur. These are the smallest combinations in that all of the failures in a MCS must occur if the top event is to occur as a result of that particular MCS. A list of minimal cut sets represents the known ways the undesired event can occur, stated in terms of equipment failures, human errors, and associated circumstances.

Special symbols are used, and International Organization for Standards (ISO) symbology should be used in the preparation of an FTA diagram. An example of one of the various types of FTA diagrams is given in Figure 6-1 (the FTA was conducted on the process illustrated by the P&ID shown on Figure 5.3).

There is usually no single ultimate event of interest in a plant, but rather several, perhaps of different types or locations. Hence, no single fault tree normally represents a plant; instead, many fault trees are usually required. It is important that the selection of the scope of the FTA be fully documented.

The FTA diagram can grow, and often single events will themselves develop into smaller fault trees. The recording system chosen should be able to accommodate this evolutionary progress.

The FTA diagram can be created and documented in several ways:

- manual drawings (in this case, the use of a template for FTA symbols can be helpful; see Berol: RapiDesign R-555 Fault Tree);
- CAD drawings or other computer-based drafting systems;
- word processor or spreadsheet graphics (which may have limitations); and
- specialized software written for FTA.

In addition, a summary report may be prepared with drawings and statements identifying sources of data. The report will also typically contain a ranked list of minimal cut sets for the system under study.

Available commercial software includes:

- AFTQM (University of New Mexico, Las Cruces, NM);
- AFTP3 (S.I.A.I, Paris, France);
- BRAVO (JBF Associates Inc., Knoxville, TN);
- CAFTA+/SAIPLOT/SAICUT (SAIC, Los Altos, CA);
- CARA (DNV Technica, Inc., Temecula, CA);
FIGURE 6-1. Example FTA Diagram.
• CAT (EPRI NP-705);
• FaultrEASE (A.D. Little, Cambridge, MA);
• FIABEX (Institution of Quality Assurance, London, UK);
• FTL (a reliability data collection, used in risk and availability assessment), Springer-Verlag, NY;
• IRRAS-PC (Idaho National Engineering Laboratory, Idaho Falls, ID);
• ISOGRAPH (Isograph Ltd, Manchester, UK);
• LOGAN/GRAAFT (RM Consultants, Abingdon, UK);
• MOCUS, ANCR-1156, (Idaho National Engineering Laboratory, Idaho Falls, ID);
• NUSSAR-PC (NUS Corp., San Diego, CA);
• PC-RISA (RISA GmbH, Berlin, Germany);
• PHARA (Midwest Technical, Inc., Kingsport, TN); and
• RISKMAN (PLG Inc., Newport Beach CA).

References
International Organization for Standardization, Symbols, ISO CEI/IEC 617: Geneva, Switzerland

6.2.11. Method 10: Event Tree Analysis (ETA)

Description—Fault Tree Analysis (see Section 6.2.10) is a deductive reasoning method; after identifying the ultimate or top event, the analyst deduces the sequence of events that can lead to the top event. In contrast, Event Tree Analysis uses inductive reasoning. After identifying an event, the possible outcomes of the event are developed. Sometimes this method is referred to as the bottom-up approach, in contrast to FTA's top-down approach.

Event trees are important because they can help in developing the sequence of events that can occur following a primary accident or event. They can help in the writing of emergency preparedness plans, since many of the possible secondary outcomes may not be within the experience of facility management, and these may not be anticipated during an actual accident situation.

ETA can be used when examining in detail the performance of plant protective systems. Using the structure of ETA, it is easy to evaluate and, if necessary, quantify the potential failures of equipment and their likely consequences. With the results, it is then possible to evaluate potential improvements to such systems. Basic steps in conducting an ETA are as follows:
• identify the need for ETA, define its scope, assemble the available information, and determine what additional information is required;
• identify the primary or initiating events;
• construct the event tree (diagram);
• describe the resulting accident sequence (text);
• determine the accident minimal cuts sets (MCS); and
• document the results, to include:
  — diagrams of ETAs performed;
  — lists of accident sequence MCSs;
  — a discussion of consequences of various accident sequences; and
  — recommendations for action;

ETA diagrams are normally represented either sequentially from left to right, or sometimes vertically, with the initial event below the sequential event. The diagrams can be drawn manually, or constructed with simple word processing or graphics programs on PCs or with specialty software. An example of an ETA diagram is given in Figure 6-2 (the ETA was conducted on the process illustrated by the P&ID shown on Figure 5.3).

Available commercial software includes:
• CARA (DNV Technica, Inc., Temecula, CA);
• CHEM-RISK (NUS Corp. San Diego, CA);
• ETA-11 (SAIC, Los Altos, CA);
• IRRAS-PC (Idaho National Engineering Laboratory, Idaho Falls, ID);
• METEOR (RM Consultants, Abingdon, UK); and
• RISKMAN (PLG Inc., Newport Beach, CA).

References

6.2.12. Method 11: Cause–Consequence Analysis (CCA)

Description—Cause–consequence analysis (CCA) is basically a combination of FTA and ETA. The CCA can benefit from the deductive and inductive reasoning used in the separate application of these methods. Unfortunately, because the diagrams produced can be extensive, there is a limit to their practical application.

As with FTA and ETA, the outlines of the CCA can be sketched on a large sheet of paper, and the completed diagram can be transferred to a manually prepared drawing or to a computer recording system. As with FTA and ETA, the recording system must accommodate the evolutionary progress of the study.
### FIGURE 6-2. Example ETA Diagram.

<table>
<thead>
<tr>
<th>SIGNIFICANT UNIT UPSET</th>
<th>FIREBOX FLAME NOT EXTINGUISHED (F)</th>
<th>INCINERATOR SHUTDOWN (I)</th>
<th>QUENCH SYSTEM WORKS (Q)</th>
<th>SCRUBBER WORKS (S)</th>
<th>SEQUENCE ACRONYMS</th>
<th>IDENTIFIER</th>
<th>CONSEQUENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IE-1</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>FQS</td>
<td>1-1</td>
<td>SAFE RELEASE</td>
</tr>
<tr>
<td><strong>IE-1</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>FQ5</td>
<td>1-2</td>
<td>MODERATE TOXIC RELEASE</td>
</tr>
<tr>
<td><strong>IE-1</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>FiO</td>
<td>1-3</td>
<td>LARGE TOXIC RELEASE, SCRUBBER DAMAGE</td>
</tr>
<tr>
<td><strong>IE-1</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>FiQS</td>
<td>1-4</td>
<td>MODERATE FLAMMABLE RELEASE</td>
</tr>
<tr>
<td><strong>IE-1</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>FiQs</td>
<td>1-5</td>
<td>MODERATE FLAMMABLE AND TOXIC RELEASE</td>
</tr>
<tr>
<td><strong>IE-1</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>FiO</td>
<td>1-6</td>
<td>MODERATE FLAMMABLE AND LARGE TOXIC RELEASE, MINOR SCRUBBER DAMAGE</td>
</tr>
<tr>
<td><strong>IE-1</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Fi</td>
<td>1-7</td>
<td>EXPLOSION, TOXIC RELEASE</td>
</tr>
</tbody>
</table>

F = FAILURE OF EVENT F  
E = SUCCESS OF EVENT F
Documentation requirements parallel these for FTA and ETA and use can be made of software that handles and quantifies FTA and ETA (see earlier sections). CCA-specific software includes CARA (DNV Technica, Inc., Temecula, CA).

As with FTA and ETA, the completed graphic documentation is typically accompanied by a text summary report.

References


6.2.13. Method 12: Human Factors Analysis (HFA)

Description—Virtually every aspect of process engineering, plant operations and maintenance is directly associated with the performance of human beings. People are known to be fallible and also to be influenced in their performance by a wide variety of performance influencing factors (PIFs), also known as performance shaping factors (PSFs). Some of these ergonomic factors such as lighting, heating, noise, etc., can be optimized to minimize errors, but others are very personal and include such aspects as emotional state, stress, training level, and experience.

Considerable research has gone into improving human reliability and to the removal of adverse PIFs, but the possibility of error remains. Techniques for Human Factors Analysis (HFA), also known as human reliability analysis (HRA), are applied to the identification of PIFs and ways in which they can be improved.

An HFA should be considered whenever human error is known or expected to be a potentially significant contributor to process risk. HFA may be performed separately after other hazard evaluation procedures have been conducted, or at the same time as any other PHA study method discussed earlier.

The HFA typically follows these steps:

- describe the personnel, their tasks and their work environment;
- evaluate the man/machine interface using HFA;
- perform a task analysis of operator functions;
- perform a human error analysis of operator functions; and
- develop recommendations to reduce human error;
- document the results.

Different levels of human reliability analysis and use of different techniques result in various work products. The HFA typically should produce a list of corrective actions that will reduce the likelihood of specific human errors. The HFA should also produce a detailed description of operator tasks, in list or graph
form, which can be used to establish or improve procedures, training or policies. In addition, the analysis may generate a set of combinations of human errors that may be ranked using human error data. HFA event trees, such as illustrated in Figure 6-3, may also be included. Thus, the documentation may include text, tables, charts, and graphic representations of the analysis results.

For a more detailed description of the documentation of the application of Human Factors in PSM, see Chapter 9 of this book. The CCPS book *Guidelines for Preventing Human Error in Chemical Process Safety* provides details of a large number of different methodologies for Human Factors Analysis (HFA), with examples of their application.

Available commercial software includes SHERI (Battelle Columbus Laboratory, Columbus, OH) which can handle the construction of diagrams and their analysis. Help can also be obtained by using FTA and ETA drawing packages and software.

**References**


### 6.3. Process Hazard Analysis Documentation

In the preceding sections, the more commonly used PHA techniques and the types of results that come from their application were briefly described. Where PHA is appropriate, guidelines should be followed to ensure that PHA is performed and documented in a consistent and effective manner. This Section includes issues relative to documentation of the PHA element itself, and to documentation of the program describing how the organization will implement PHA.

#### 6.3.1. PHA Program Documentation

Organizations implementing PHA should include in their PSM program documentation a discussion of the goals of PHA as well as any general procedures that outline how PHA will be implemented. The PHA program documentation should set the standard of performance and demonstrate the support of upper management for what can be a resource-consuming endeavor. Without the visible support of upper management, there is a risk of perfunctory efforts from those responsible for the actual implementation of PHA. Some organizations may issue
FIGURE 6-3. Example HFA Event Tree.
broader, more general policy statements at the corporate level, with the development of more specific interpretations of these goals at the operating unit (e.g., plant or site level). In either case, management support should be evident.

There are a wide variety of factors that should be considered when establishing detailed procedures intended to achieve the established goals of PHA. The more significant factors will be discussed in the following paragraphs. Some of these are prescriptively addressed in current and proposed government regulations.

**When to Perform PHA**—PHAs should be conducted on a proportional-to-need basis. In other words, some portions of a facility may require more frequent and rigorous review based upon either their demonstrated or perceived hazard potential. Similarly, some operations may be appreciably more subject to change in operating conditions or equipment design (see Chapter 10, *Management Of Change*). Consequently, a PHA schedule should be established for each facility to ensure that reviews are conducted at appropriate frequencies. The facility, and possibly individual processes, may be subdivided with each subdivision given a specific review frequency based upon its particular needs. For example, a powerhouse may require less frequent review than a polymerization reactor.

Another advantage to establishing such a schedule is that it permits planning and scheduling reviews in a manner that balances the PHA effort over an entire review cycle. An organization initially implementing a PHA program should establish a prioritized schedule of which operations to review in what order, along with a schedule for updating or revalidating previous reviews. Such schedule guidelines must be capable of addressing the changing needs of a process (e.g., in response to changes in the nature of the hazards present or marked changes in safety experience for that operation or similar operations). A statement on the derivation of the schedule may be included in the documentation record.

**Technique Selection**—As discussed briefly above, and covered in more detail in the CCPS book, *Guidelines for Hazard Evaluation Procedures, Second Edition with Worked Examples*, the various PHA techniques differ in approach and work product. Some are more rigorous and detailed, and some approach the PHA task from very different perspectives (e.g., contrast the difference in detail between WI and FTA techniques, or the inductive versus deductive approaches used by ETA and FTA analyses). Consequently, some organizations may want to establish guidelines for technique selection to ensure that a specific high-hazard operation receives a sufficiently rigorous review or that a too-rigorous technique is not wastefully applied to a low hazard process. Such guidelines should be just that—guidance rather than mandatory edicts. Often, the best judge of the most appropriate technique is the trained, experienced analyst who is responsible for the review. Such guidelines would form part of the documentation record.

**Training and Qualifications**—Some techniques like FTA and HRA require more detailed, specific training and practice in their application than is the case with a technique such as the CL review. An organization may wish to establish minimum
levels of demonstrated competency for those responsible for the application of such techniques. An organization may consider documenting training requirements for the various personnel who participate in the reviews. Obviously, a team leader will need more training than someone who is merely participating in the review.

**Team Make-up**—For team-based techniques, it is important to get a proper mix of training, background, and expertise in the team make-up. Similarly, a proper mix of supervisory and nonsupervisory personnel helps ensure a balance of backgrounds and perspectives and contributes to more meaningful results. Organizations may wish to prepare guidelines for team composition to ensure that a proper mix of functional responsibilities (e.g., manufacturing, maintenance, technical, engineering, and R&D), background and training are provided on PHA teams.

**PHA Results Documentation**—Documentation of the results of the PHA will be discussed in Section 6.3.2. In the documentation of the PHA program, minimum standards for the form and content of PHA results documentation should be established. For example, what goes into the final, formal report? How is supporting information documented? Who is responsible for signing the final report? What degree of review is appropriate for the report before it is issued?

**Recommendations and Their Resolutions**—An important function of PHA is either to validate the safety of current equipment design and operating procedures or to propose necessary and sufficient corrective actions to ensure an appropriate level of process safety within the operation. Most PHA efforts result in a number of recommendations that may either define a specific course of action (do this . . .) or define the need for further evaluation (study this . . .). A documented system for tracking the status of these recommendations, and obtaining documentation of the implementation or resolution of each one, will help to ensure that the organization complies with its ethical responsibilities in this matter and achieves the full value of the effort that it has devoted to the PHA program.

**Records Management**—Retention and purge schedules for PHA reports and supporting documentation should be clearly established, documented, and followed. Legal and regulatory requirements should be considered. See Section 6.4 and Chapter 4, Records Management.

**Communication of PHA Results**—It was mentioned in the introduction to this chapter that PHA serves as the cornerstone to virtually all of the other PSM elements. The necessity of appropriately communicating the results of the PHA to other members of the organization must be carefully considered in establishing distribution lists for reports. Similarly, suitable storage locations for copies of the reports should be identified so that those not receiving a copy, yet having a need-to-know, can have access to this information. Suitable controls should be applied to ensure that these general access copies remain secure, accurate, and up to date.
PHA Program Responsibility—An organization should document the functional responsibility and accountability for implementation of the PHA program. Ultimate responsibility may reside with the site manager, but accountability for the actual implementation can be delegated. It is the responsibility of the program manager to interpret policy, establish frequency and scope of reviews, and examine reports for uniformity and quality of the reviews. In addition, members of the line organization will have their own responsibilities and roles in the implementation of the overall PHA program. These responsibilities, from the top of the organization to its lower levels, should be clearly established, documented, and communicated to all those involved.

6.3.2. Documentation Of PHA Results

A brief description of the type of results and documentation requirements specific to the more commonly used individual techniques was provided in the first part of this chapter. The following summary provides a more general perspective on broader issues related to documentation of the PHA effort, independent of which technique was used for the PHA.

The primary objective of PHA is to address the following basic needs:

- identify the hazards inherent in the process or activity;
- identify the credible human and/or equipment failures likely to lead to accident scenarios;
- evaluate the consequences and likelihood of the various accident/incident scenarios, that is, assess the risk;
- propose changes, where warranted, to equipment design, process conditions, operating procedures, etc. to mitigate risk to a tolerable level; and
- document the PHA study appropriately.

Unless a PHA is properly documented, there can be no assurance that the information gained from the PHA review will actually be applied to enhancing operational safety. Furthermore, future efforts may be less productive in that additional resources may be expended in relearning the same lessons. Finally, the results should be communicated in a way that allows for adequate scrutiny of the technical quality of the review.

The results of a PHA are typically documented and communicated to those affected via a formal summary report. The content of the report will vary somewhat based upon the scope of the review and the technique used, but the basic structure of the report typically can, and should, be standardized for the organization. Table 6-6 shows one suggested outline for such a summary report.

As shown in the table, the report typically contains the following information:

- a clear, concise identification or description of the facility or process under review including a brief description of the process chemistry and the hazardous properties of the materials involved;
TABLE 6-6
Items to Consider Including in PHA Study Reports

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Study objectives</td>
<td>Primary purpose and ancillary needs</td>
</tr>
<tr>
<td>Physical and analytical scope</td>
<td>Specific process areas, systems, and equipment covered. Hazards analyzed along with situations beyond the study's scope</td>
</tr>
<tr>
<td>Analysis team composition</td>
<td>Participants in the review (categorized by organization and job/experience)</td>
</tr>
<tr>
<td>Meeting dates and duration</td>
<td>When, where, for how long the team met and attendance lists</td>
</tr>
<tr>
<td>PHA technique description</td>
<td>Rationale for selection of the PHA techniques. Description of the techniques employed</td>
</tr>
<tr>
<td>Process/activity description</td>
<td>Description of the system analyzed. Explanation of the procedure steps used in batch operations. Listing of important process conditions. Descriptions of safety systems. Listing of materials and hazards.</td>
</tr>
<tr>
<td>Drawing, specification, and procedures list</td>
<td>Documents (with dates and revision numbers) used as the basis for the analysis</td>
</tr>
<tr>
<td>Conclusions</td>
<td>Team consensus as to the safety of the facility or operation</td>
</tr>
<tr>
<td>Action items/suggestions</td>
<td>Recommendations made to management for risk reduction with clear delineation of responsibilities and required timing</td>
</tr>
<tr>
<td>Detailed documentation of any review meeting</td>
<td>Minutes of meetings, summaries of topics covered</td>
</tr>
<tr>
<td>Technique-specific lists, forms, or graphical models</td>
<td>Checklists, lists of What-If questions, worksheets, FMEA or HAZOP tables, fault trees, event trees, cause–consequence diagrams, HFA event treesa</td>
</tr>
</tbody>
</table>

• careful definition of the scope and limitations of the review (e.g., was only off-site risk considered, does the review address environmental damage as well as personnel injuries);
• clear statements defining, and justifying, the need for recommendations, namely, what specifically must be done and what is to be achieved, recognizing that some recommendations may merely define the need for additional study before a course of action can be proposed;
• clear statements defining responsibilities and required timing for resolution of recommendations;
• documentation of actions that were taken immediately to enhance operational safety, along with explanations of why they were necessary;
• identification in the report of those parties that participated in the review and their affiliations, attendance rosters for each meeting, where multiple meetings were required;
6.3. Process Hazard Analysis Documentation

- documentation of the technical content, including the identification of the PHA technique used (which may be described in either the PHA report or a PHA methodology/protocol, or other referenced documents) with some explanation as to the rationale for its choice.
- key results and conclusions of the review should be clearly, unambiguously, and concisely summarized and documented and should be reviewed by all participants in the review, as an affirmation of their concurrence with the published conclusions.
- reference documents used during the review should be listed (e.g., drawing and/or procedure numbers along with the then current revision number or date, previous PHA reports or technical studies). Working papers, if retained, should be filed together in a secure location and indexed in the report.

The main body of the report will usually be comprised of output generated during the PHA. Typical outputs of the individual techniques were described earlier in Section 6.2. In general, however, there are two broad categories of information that would typically be documented. The first is primarily text, which may or may not be presented in a tabular (or columnar) format. This sort of output typically results from techniques such as WI, CL, HAZOP, or WICL.

The second common type of information will be diagrams, e.g., process flow diagrams, simplified piping and instrument diagrams, FTA and ETA charts, HFA charts, facility layout diagrams. These diagrams are usually accompanied by some text describing their content.

Some techniques, such as relative ranking, produce a variety of output including charts, graphs, tables, and standardized forms.

Readers wishing a broader background may find further descriptions of many of the concepts discussed in this section by referring to Chapters 2 and 7 of the CCPS book, *Guidelines for Hazard Evaluation Procedures, Second Edition with Worked Examples*.

6.3.3. Resolution of PHA Recommendations

The final decision with regard to adoption of PHA recommendations is typically a management responsibility and the status of PHA recommendations may not be determined before the PHA summary report is issued. Once a recommendation has been made, it must be resolved and documentation of the final resolution of all recommendations is the last task in documenting a PHA. Dates by which the recommendations should be implemented, or otherwise resolved, should be clearly communicated and documented in the PHA summary report. Responsibility for recommendation follow-up should be clearly assigned.

Resolution is not synonymous with adoption; not all recommendations will eventually be implemented as originally proposed. Circumstances change, some recommendations may ultimately be seen to be inappropriate, or a better means
of achieving the same results may become known. In summary, the various ways that a recommendation could be resolved include:

- Accepted and implemented;
- Rejected for cause:
  - would have introduced a greater hazard; or
  - change in circumstances, no longer required.
- Accepted in principle:
  - equivalent protection obtained via another route.

In any event, the method of final resolution of all recommendations should be documented, either in the summary report, in an addendum to the report, or in a separate follow-up report. The rationale for not implementing the recommendation as originally proposed, as well as any alternative course of action intended to achieve the objective, should be clearly documented. The date of resolution, as well as the name of the person accountable should also be documented.

6.4. Records Management

6.4.1. Records Management Program

In addition to the description of the PHA program given in Section 6.3.1, the organization’s PSM program documentation should define PHA records management practices. This should address documentation gathered, generated, and utilized during reviews as well as the reports, recommendations, and documents relating to follow-up activity stemming from the PHA reviews. The records management practices should provide access by the PHA team members to the information required for their evaluation and reviews, while at the same time ensuring that appropriate control and retention procedures exist to preserve historical or sensitive data, and to gather, store, and disseminate documentation of pertinent interim and final reports.

6.4.2. Media and Methods

Depending on the size of the organization or facility, the nature and scope of the review, and PHA technique chosen, the media used to document meetings and results can range from text information recorded by a meeting scribe on a notepad, to computer-based records. Since many of the techniques are team-based, a media visible to the team as a whole would be an appropriate choice. In its simplest form, this could be large chart pads displayed on meeting room walls, to permit the entire team to refer to information discussed or conclusions previously reached. Similarly, worksheet transparencies shown on overhead projectors, could permit team members to view, revise, and record data during meetings. Alternatively, the scribe might utilize a personal computer, commercial software and a wall
screen projection system to show the data, allowing editing or reformatting as the analysis is being performed and results formulated.

Electronic media is attractive for records management since it is versatile in displaying, recording, and rapidly producing hard copies, if needed. It is easily updated and increasingly economical to implement.

Specialized software exists for generating some of the records that are presented in diagram form (especially for FTA, ETA, and HFA diagrams). Alternatively, CAD programs or simply desktop publishing, drafting, or presentation graphics can be used. Even the simplest drafting programs offer specialized clip art features for addition to drawings, as needed, thus allowing creation of specialized FTA templates.

6.4.3. Responsibility and Accountability

Someone in the organization, by job title, should be identified as having the responsibility and accountability for managing PHA related documentation within the organization’s normal records management function. Someone on each PHA team should be designated to ensure that this PHA documentation is properly completed and entered into the records management system.

6.4.4. Distribution, Access, and Retention

Storage locations, access controls, and revision and purge schedules should be in accordance with the organization’s established PSM records management procedures. It should be remembered that PHA serves as the foundation for many other PSM elements. Thus, it is important that ready access to PHA documentation be provided to personnel implementing other PSM functions. Documentation should be retained at least until the PHA is next updated. Note, however, that current regulatory requirements dictate that PHA reports for covered processes be retained for the life of the facility. See Chapter 4, Records Management for additional guidance.

6.5. Auditing

The PSM program should establish the requirements for auditing PHA. The first step in auditing PHA is to verify that a documented program exists for implementing PHA throughout the facility life cycle. This program would include elements outlined in Sections 6.3.1 and 6.4 that are pertinent to the needs of the organization or facility.

The second step in auditing PHA is to verify that the results of implementing PHA have been documented in the manner prescribed by the program. Particular emphasis should be placed on auditing the documentation of the resolution of recommendations.
Any deficiencies identified during the audit must be documented and promptly resolved. See Chapter 14 and the CCPS book *Guidelines for Auditing Process Safety Management Systems* for more guidance on auditing PSM.

### 6.6. Examples

#### 6.6.1. Runaway Reaction in a Polymerization Reactor

A severe cooling problem in a polymerization reactor was believed to be due to fouling from polymer deposits in the cooling system. The operations management team decided to empty the reactor, refill it with refined reactant and circulate this in the reactor cooling system to dissolve the polymer deposits and thus restore efficient heat transfer. This operation had been in progress for more than an hour when an incident occurred:

- the emergency high pressure alarm went off;
- the relief valve began to discharge into the blowdown system;
- the pressure recorder in the control room went off scale;
- a loud noise was heard from outside;
- the unit gas detection alarm sounded; and
- a field report came in of hydrocarbon vapors escaping from a ruptured blowdown drum.

Emergency procedures were immediately implemented and response teams set up water curtains to disperse the hydrocarbon vapor cloud. Fortunately the damaged drum was safely isolated from the flare and no further consequences occurred.

Investigation revealed that residual catalyst in the reactor had apparently initiated a polymerization reaction. Since heat removal from the reactor was impeded, the bulk temperature of the reactants had exceeded the acceleration temperature, producing a runaway reaction and rapid pressure buildup. This pressure exceeded the relief valve design basis and capabilities, and rose too fast to allow a built-in reaction kill system to respond.

Fundamental process changes had been introduced by the revised cleaning procedure:

- changing the polymerization conditions; and
- changing the reactant concentration for the cleaning operation.

No formal, systematic, or critical process hazard analysis (PHA) had been done to enable operations personnel to manage and understand the potential hazards associated with these process changes. In fact, the plant's technology group was not contacted about the modifications.

Performance of a timely and well documented PHA, based on known and documented plant experience on cooling system fouling and known data on the
probability of increased hazards of runaway reactions at the changed operating conditions, would have informed the operations team of the hazards and could have prevented this incident.