21
Analytical Methods in Process Safety Management and System Safety Engineering – Process Hazard Analysis

Paul Baybutt

21.1
Introduction

Various analytical methods are used to support different aspects of process safety management. Arguably, those used in process hazard analysis (PHA) are the most important and are the subject of this chapter. PHA is used to ensure process hazards are identified, evaluated, and controlled in an organized and systematic way. Generally, a hazard is a situation or intrinsic material property with the potential to cause harm, that is, injury to people, or damage to the environment, property, the process, the company, and so on. In process safety, the hazards of concern are usually those of highly hazardous chemicals, or the so-called *major hazards* of flammability, explosivity, toxicity, and reactivity. Their occurrence usually involves loss of containment. Chemicals posing reactive hazards, if not handled correctly, may react uncontrollably, causing the rapid release of large quantities of heat, energy, and gaseous by-products that may lead to explosions, fires, and toxic emissions.

Various PHA methods have been documented in the literature (Knowlton, 1992; Kletz, 1999; IEC, 2001; CCPS, 2008a; Crawley, Preston and Tyler, 2008). This chapter provides a step-by-step approach to using the principal methods. The methods addressed are as follows:

- preliminary hazard analysis (PrHA)
- checklist
- what-if (WI) and what-if/checklist (WIC)
- hazard and operability (HAZOP) studies
- failure modes and effects analysis (FMEA)
- major hazards analysis (MHA)
- process hazard review (PHR)
- fault tree analysis (FTA)
- event tree analysis (ETA)
- cause–consequence analysis (CCA)
- bow-tie analysis (BTA).

Handbook of Loss Prevention Engineering, First Edition. Edited by J. M. Haight.
© 2013 Wiley-VCH Verlag GmbH & Co. KGaA. Published 2013 by Wiley-VCH Verlag GmbH & Co. KGaA.

Brief descriptions and advantages/disadvantages of each method are provided in Appendices 21.A and 21.B, respectively.

Section 21.2 provides an overview of PHA and introduces key terms. The remaining sections explain how PHA is performed using the techniques described in Appendix 21.A.

21.2 Overview of PHA

PHA addresses the following issues:

- What can go wrong (hazard scenarios)?
- How bad could it be (consequence severity)?
- How often could it happen (consequence likelihood)?
- What is the risk (combination of severity and likelihood)?
- Is the risk tolerable considering existing safeguards?
- If not, what actions are needed to reduce the risk?

PHA focuses on identifying *hazard scenarios* which are specific, unplanned events, or sequences of events that have an undesirable consequence resulting from the realization of a hazard. They are also called *accident scenarios, accidents*, and *scenarios*. Sometimes the word *sequence* is used in place of scenario and *incident* in place of accident. The starting point of a hazard scenario is the *initiating event*, also called the *initiating cause* or often just *cause* (Figure 21.1). The initiating event is the minimum combination of failures necessary to start the propagation of a hazard scenario.

The initiating event may prompt automated process responses by control or safety systems and operator actions which are called *intermediate events*. They propagate or mitigate the initiating event and lead up to the scenario consequence. The actions of process *safeguards* are classed as intermediate events. Safeguards are means of protecting against hazard scenarios. They are also called *protection layers*.

Consequences are the direct impact of the hazard scenario in terms of its effects on *receptors* such as people, the environment, property, or equipment, the process, the company, and so on. The receptor is the entity that is harmed. Consequences can also include the impact of hazard scenarios on adjacent installations. They are characterized by their *type*, that is, impacts on people, property, and so on, and their *severity*, that is, their degree of impact, for example, single fatality versus multiple fatalities.

Enablers are events or conditions that must be present or active for the scenario to proceed, for example, an alarm that is bypassed. They do not by themselves initiate hazard scenarios, rather they make them possible. Enablers are sometimes called *contributing causes* or *contributing factors*.

At-risk factors and *conditional modifiers* are special types of enablers. At-risk factors account for the time period in which a process is at risk, for example, a runaway of

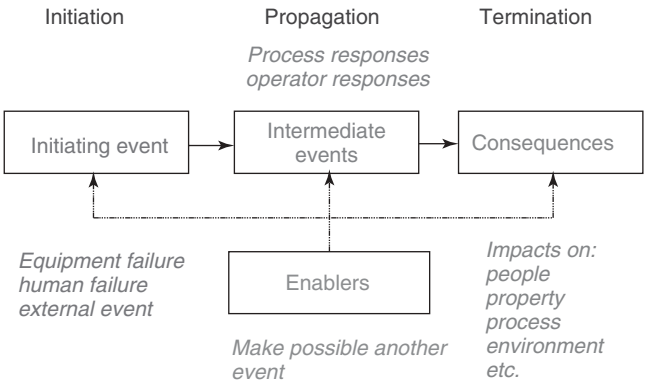


Figure 21.1 Elements of a hazard scenario.

a batch reaction can only occur when the reaction is being conducted. Conditional modifiers affect the scenario consequence, for example, the probability that a flammable or explosive material will be ignited, the probability that a person will be present to be exposed to a hazard (sometimes called the *occupancy factor*), the probability that harm will occur if an individual is exposed (sometimes called the *vulnerability*), or the probability of vessel rupture, failure of inerting, fire, or explosion.

Often, when problems are identified in a PHA, corrective actions will occur to the participants. These are called *recommendations*. They act to reduce the likelihood or mitigate the consequences of hazard scenarios. Traditionally, the primary objective of PHA has been the identification of hazard scenarios, not problem solution. However, ignoring solutions that occur to participants is not sensible and, therefore, they should be documented.

Sometimes the need for further information to complete the PHA will be recognized by participants. These are called *information needs*. For example, the potential for two-phase flow through a relief valve may be identified but it may not be known if it has been sized correctly.

All principal PHA methods identify initiating events (causes), consequences, safeguards, and recommendations (corrective actions) for hazard scenarios. Methods are distinguished mostly by the way in which they approach the identification of causes.

PHAs are typically performed by a team of people. The combined skills of a multi-disciplinary team are needed to identify hazards properly based on the premise that a group effort is better than the sum of individual efforts. Team interactions facilitate *brainstorming*, which is needed to stimulate creativity and generate new ideas. The team must be encouraged to look at the process in a different way and overcome mindsets in order to identify hazard scenarios fully. The team brainstorms in a series of meetings called *sessions* that may span days or weeks. A team leader or facilitator manages the brainstorming to ensure that steady progress is made. The leader guides the team systematically through the facility design applying the chosen PHA method. PHA methods are structured to help

provide consistency and completeness. Different PHA methods provide structure in different ways and to different extents.

PHA studies are performed by subdividing the process into sections called *nodes or systems/subsystems*. They are used to focus the analysis and make the study manageable. PHA may be performed on virtually any aspect of a process, such as equipment, procedures, control systems, and/or management systems. It can be used throughout the process life-cycle. Simple techniques are used in the early stages and more sophisticated techniques are used in the later stages of the process life-cycle.

PHAs can be performed for new or existing processes, or processes at the design stage. The first PHA on a process is often referred to as an *initial* PHA. It is good engineering practice to update and revalidate PHAs periodically in what is usually termed a revalidation PHA. Such PHAs are often required by government regulations. Different PHA methods can be applied to different parts of a process according to their suitability (CCPS, 2008a).

21.3 PHA and Decision-Making

The primary objective of PHA is to provide information which will assist in making decisions on improving safety and reducing the consequences of unwanted or unplanned releases of hazardous chemicals. Thus, once hazard scenarios have been identified, their risks must be evaluated and their tolerability determined (Figure 21.2).

Risk is evaluated by estimating the *severity* and *likelihood* of harm occurring from a hazard scenario. The severity, S, is the degree of impact of the hazard scenario and the likelihood, L, is how often a hazard scenario is expected to occur. They may be expressed qualitatively or quantitatively and are combined to produce a risk estimate, R, usually by simple multiplication ($R = S \times L$). In most PHAs, a simple qualitative risk estimate is used. Frequently, risk ranking schemes that use severity and likelihood levels are employed. Levels are usually designated numerically as 1, 2, 3, ... and definitions of the levels are provided (Figures 21.3 and 21.4). Risk rankings (Figure 21.5) are used to:

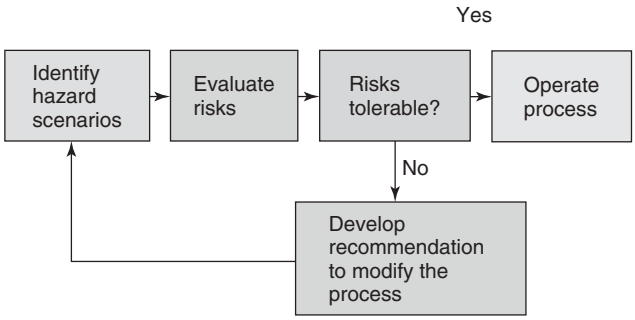


Figure 21.2 PHA and the decision process.

Severity level	Safety onsite	Safety offsite	Environ-mental	Property damage	Business interruption	Public relations
1 – Very high	Multiple fatalities	One or more fatalities	Remediation required	Extensive (>$ 5 M)	>60 days	National media attention
2 – High	Single fatality or hospitalization	Injuries or permanent health effects	Observable effects off flora and fauna	Major (above $ 1 M)	>30 days	Local media attention
3 – Medium	Lost time injury	Health effects requiring first aid	Exceed pemit conditions	Moderate (above $100,000)	>10 days	Complaints from neighbors
4 – Low	First-aid	Respiratory irritation etc.	Localized cleanup only	Minor (less than $100,000)	>1 day	Queries to plant only
5 – None / insignificant	None	None	None	None	None	None

Figure 21.3 Example of five-point severity level scale.

Level	Definition	Guideline
1 – Very high, Likely	Occurs at least once or more a year	Possibility of repeated incidents
2 – High, Possible	May occur about once every 10 years	Possibility of isolated incidents
3 – Medium, Occasional	May occur once in 100 years	Possibility of occurring some time
4 – Low, Unlikely	May occur once in 1000 years	Credible but unlikely. Never saw this or anything similar
5 – Insignificant, Rare	May occur once in 10,000 years	Conceivable but extremely unlikely, never occurred, speculative

Figure 21.4 Example of five-point likelihood level scale.

Severity

Likelihood	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

Figure 21.5 Example of a risk matrix.

- determine if further risk reduction is needed
- resolve differences of opinion on the need for recommendations
- prioritize recommendations
- determine how quickly recommendations should be addressed and implemented
- screen hazard scenarios for more detailed analysis
- comply with government regulations.

21.4 Stages and Steps in PHA

PHA entails several stages and steps:

- project initiation
- hazard identification (HAZID)
- getting ready:
  - selecting a PHA method
  - defining the purpose, scope, and objectives (PSO)
  - selecting a team
  - collecting and preparing reference information and data
  - estimating the effort involved and scheduling study sessions
  - briefing/training team members
  - arranging required facilities
  - other items
  - subdividing the process
  - performing an inherent safety review
- completing the worksheet:
  - first session
  - recording PHA studies
  - making worksheet entries
- special topics:
  - multiple failures
  - human factors
  - facility siting
  - utilities
  - modes of operation
  - process changes
  - procedures
  - non-steady-state processes
  - quality control
  - limitations and cautions
- revalidation
- report preparation
- follow-up.

Some companies have developed written procedures to govern their PHAs, in which case PHA team leaders must familiarize themselves with the procedures. If

company procedures are not available, team leaders will need to develop their own guidelines. Procedures are important as they help to ensure:

- PHA performance and documentation comply with regulatory and company requirements.
- PHA studies are conducted consistently for different processes.
- Appropriate teams are selected.
- Responsibilities are established.
- A consistent format is used to facilitate the use of PHAs by others.
- Schedules are established to ensure timely completion.
- Departures from established practices are avoided.

Companies should establish a system to manage the performance of PHA studies. Such a system needs to cover training of teams, team selection, scheduling sessions, tracking recommendations, and so on. Each of the stages and steps in conducting PHA is described in the following sections.

21.5 PHA Project Initiation

A PHA project begins when a responsible manager determines that a study is needed. The responsible manager must:

- Determine that a study is required.
- Ensure that it is performed when required.
- Specify the level of detail required.
- Appoint a study leader.
- Assist in the identification and assignment of team members and ensure their availability.
- Provide or arrange for necessary resources.
- Ensure that the study is planned and performed.
- Monitor the study and provide support.
- Resolve issues as the study progresses.
- Ensure that the study is completed and documented.
- Receive and act on the results of the study.
- Ensure any needed liaison with the process owner.

The project must be clearly defined by the responsible manager, including the facility, location, process, and chemicals to be addressed. This information is provided to the team leader.

21.6 Hazard Identification

Determining the presence and locations of process hazards that could produce undesirable consequences through the occurrence of an incident is the starting

point for hazard analysis. The identification of hazards can be addressed within some PHA methods such as HAZOP. However, a separate HAZID study can be performed and used to decide how hazards should be addressed. Hazards within each area of the process are identified using a hazards checklist, usually customized for each type of process, and the risks posed by the hazards are assessed using a ranking scheme. Possible means of eliminating the hazard or controlling the risk may also be identified where they are obvious.

A HAZID study is usually carried out by a team and a worksheet is completed (Figure 21.6). Various worksheet formats are employed, but typical columns include:

- hazards
- materials/situations
- criticality
- recommendations.

A HAZID study involves the following steps:

1) Review data sheets on process materials and other documents for hazard information.
2) Examine process parameters as indicators of possible hazards.
3) Compile a checklist of hazards present in the process.
4) List known hazards from process materials and characteristics.
5) Address all modes of process operation.
6) Conduct the HAZID review.

In the HAZID review, the team uses the prepared checklist of process hazards to identify which are present in each area of the process. The hazards may be categorized, for example, as process or occupational hazards, and the material or situation posing the hazard is identified. A ranking scheme is often used to provide an indication of the hazard severity. The ranking is used to help decide how the hazard should be addressed. An assignment of responsibility can also be made.

Once the hazards have been identified, it may be possible to address some of them before proceeding with the PHA. For those hazards which require further analysis, it must be decided which will be addressed using PHA, and which are better addressed by other approaches, for example, job safety analysis. A recommendation may also be made for the use of a specific PHA method suitable for the hazards identified.

System (1) TANK FARM

HAZARDS	CAT	MATERIALS / SITUATIONS	C	RECOMMENDATIONS	BY
1. Flammable	P	Hexane	3	1.1. Address in PHA	SAF
2. Toxic	P	Ammonia	4	2.1. Address in PHA	SAF
3. Simple asphyxiant	O	Nitrogen gas	2	3.1. Use checklist	ENG
4. Elevated work areas	O	Maintenance on tanks	1	4.1. Use checklist	ENG

Press F1 for Help

P – Process; O – Occupational; SAF – Safety; ENG – Engineering

Figure 21.6 Example of a HAZID worksheet.

Often a *hazards register* is maintained for a facility. The register documents the types and locations of hazards that are known to be present, sometimes with controls and a risk rating.

21.7 Selecting a PHA Method

Various PHA methods are available. The choice of method must comply with any applicable regulatory and company requirements. Selection guidelines may be provided in a company's PHA procedures. Considerations in selecting a method include:

- purpose of the PHA
- type of results needed
- level of detail required
- process size
- type of operations
- process type
- process complexity
- process age and condition
- process incident history
- phase of process development
- degree of process risk
- familiarity of team members with techniques
- opportunities for risk reduction
- information available
- resources available
- amount of existing knowledge about the process
- time and cost required.

For example, a simple process with significant risks may merit the use of the What-if checklist method when performed by an inexperienced team, although the team leader would need to be experienced. A new process with complex technology may merit the use of the HAZOP method even when performed by an experienced team. An existing complex process may merit the use of MHA when performed by either an experienced or inexperienced team.

21.8 Defining the Purpose, Scope, and Objectives of the Study

A vital aspect of study preparation is defining the PSO for the study. The PSO statement helps to ensure that the PHA is focused and complete and to avoid the inclusion of extraneous items in the study and digressions during the study sessions.

The purpose is why the study is performed. It must be defined as it affects the way in which the study is performed, for example, the types of hazards to be included and the types of consequences to be addressed. It helps to ensure that

the study outcome is consistent with the intention for the study. Scope specifies what is included in the study and it may also specify what is *not* included. Items to address in the scope statement include:

- process boundaries
- equipment, procedures, control systems, and so on
- utilities/services
- modes of operation
- external events
- level of detail
- level of causality
- design intent
- codes and standards
- exclusions
- assumptions.

Objectives define what is to be considered, specifically the types of hazards and the types of consequences.

Management is responsible for the PSO statement. However, the statement is often drafted by the PHA team leader for review and approval by management. The PSO statement will vary from one process to another, although there likely will be commonalities for processes at the same facility. They will likely share similar purposes and objectives but the scope statements will vary.

The PSO statement is used to help ensure that team members fully understand the study goals as expressed by management. It is also used during the performance of the PHA study to keep the team on track, ensure appropriate study content, ensure that the study is complete, and help avoid team members raising issues that are not relevant. It may be modified during the performance of a study, for example, if team members identify missing items. In such cases, management approval should be obtained for any changes made to it.

21.9 Selecting a Team

21.9.1 Team Members

PHAs are conducted by a multi-disciplinary team. The responsible manager and/or the team leader select the team members advised and approved by the other. Team members collectively should possess the knowledge and skills to identify hazard scenarios for the process being studied. They should have a sense of ownership and responsibility for the process to ensure their commitment and motivation for the study.

Suggested technical areas to be covered by PHA team members are:

- design engineering

- process engineering
- process controls engineering
- operations and maintenance
- safety engineering
- specialty technical areas, PHA facilitation and recording, quality control, and so on.

Team members should have personal attributes that result in positive team dynamics, which are very important for an effective and efficient study. Of course, the availability of personnel must also be taken into account. The various members of a PHA team have different responsibilities and qualifications (Table 21.1).

The team leader does not usually act as a technical resource on the process. Team members provide knowledge of the process. Ideally, the team leader should not have any day-to-day responsibilities for the process being studied to avoid bias, prejudice, and defensive behavior. Hence the team leader should not be the process engineer or the designer of the process. Team leaders must be impartial. The team leader does not need to be an expert on the process. Indeed, the team leader should *not* be an expert on the process. Experts will not be able to see the process from a fresh perspective and may suffer from mindsets (mindsets are one or more assumptions held by an individual which are so established that the individual cannot see beyond them and makes decisions without being consciously aware of the implicit assumptions being made). Management is responsible for ensuring that team leaders are appropriately qualified. Candidates should be screened according to suitable selection criteria. Key criteria are their technical understanding of PHA and their facilitation skills.

Good technical secretaries or scribes are able to start typing as soon as a team consensus emerges without waiting for instruction or dictation by the team leader, although some team leaders prefer to instruct the scribe to make entries. Recording by the scribe should not slow the progress of the study or interfere with the creative flow of discussion. Scribes can assist team leaders by noting suggestions made by team members and reminding the team leader. They can also help with quality control and act as a keeper of checklists used to facilitate the study. Experienced team leaders often act as their own scribe.

Technical team members fall into two groups: core team members and specialty team members. Core team members participate in the PHA on a full-time basis. Their involvement is critical to the success of the study. Their full-time participation helps to achieve consistency across PHA sessions and their presence may be necessary to satisfy regulatory requirements. Typical core team members may include the following:

- design engineer
- process engineer
- operator(s) (covering inside and outside activities)
- maintenance technician(s) or engineer(s)
- controls engineer
- safety engineer.

Table 21.1 Responsibilities and qualifications for PHA team members.

Team member	Responsibilities	Qualifications
Team leader/facilitator	Coordinates with management Prepares and organizes the study Manages and guides the team Quality control May record the PHA sessions Prepares the study report	Formal PHA leader training Leadership/facilitation skills Motivational/interpersonal skills Communications skills Project management skills Understands processes and their operation quickly Reads engineering drawings easily
Scribe/technical secretary	Records PHA sessions	Technically-oriented Understands PHA Familiar with terms and acronyms used Competent with the means used to record PHA sessions Good working relationship with the team leader
Technical team members	Brainstorm hazard scenarios Identify process safeguards Perform risk ranking Identify recommendations	Work with the process being studied Detailed technical knowledge of some aspect(s) of the process being studied Ability to read P&IDs and understand other process documentation Knowledge of PHA method being used is desirable but not required
Other technical team members	Provide information on equipment design, maintenance, operation, and so on	Similar to core and specialty technical team members
Interpreter	Ensures that team members communicate effectively	High level of ability Knows technical terms in languages used
Site coordinator	Liaison between team and local facility Ensures adequate facilities, such as a meeting room, and other team needs	Available for the duration of the study Well connected

More than one person from the same technical discipline, for example, operations, may be needed to reflect different levels of experience, ways of performing the job, attitudes, and so on.

Specialty team members are individuals with a particular expertise who attend only certain sessions where their expertise is needed. These people may be better called team advisors since they are not present at every session. Typical specialty team members may include the following:

- instrumentation/electrical engineer
- mechanical engineer
- programmer
- inspection/materials engineer
- research scientist/chemist
- environmental engineer/regulatory specialist
- quality assurance/quality control specialist
- industrial hygienist
- industrial engineer.

Some specialty team members may be core team members and vice versa according to the particular PHA study being conducted. Other technical team members include vendors of licensed technology, contractors who perform activities such as maintenance, and design and engineering company representatives. PHAs may be conducted by teams who are unable to communicate in a common language or cannot communicate well enough to perform the study properly and an interpreter will be needed to help ensure that team members communicate effectively. Such interpreters must be familiar with technical terms in the languages used.

Team member qualifications, including education and experience, should be documented as part of the PHA records.

21.9.2 Team Size and Composition

A large enough team is needed for effective brainstorming, but the team should not be so large that brainstorming is hindered. The typical size is five to nine people. Experience shows that fewer than three or more than 10 can create problems. Factors that influence team size are the complexity of the process and the expertise of individual team members. Ideally, team members are needed who together can provide the information required to define the design intent completely for the process, including operations and maintenance intents. Team members may cover more than one technical area if their expertise allows.

The team should not consist entirely of people who know the process since the phenomenon of *groupthink* can be a problem. This phenomenon usually occurs where people have worked together for some time in the same environment and results in everyone unwittingly making the same assumptions, some of which may be unfounded. Consequently, it is a good idea to have an independent individual

on the team. This person should be a senior engineer who will have the credibility to challenge the views of other team members and be able to contribute knowledge that may not be possessed by them. This role can be played by an independent experienced team leader.

21.9.3 Leadership and Facilitation Skills

Team leaders must ensure that the study is completed within the allotted time by maintaining a suitable study pace and keeping the study focused. They must also keep team members involved and energized. In particular, team leaders should focus on important and relevant scenarios and not waste team brainstorming on routine hazard scenarios. The Pareto principle (also known as the 80–20 rule) may apply such that roughly 80% of the significant consequences may be expected to come from 20% of the causes. The repetitive nature of PHA must also be managed. Hazard scenarios may be distinct but often they have similarities; for example, scenario causes may be different but consequences and safeguards may be the same. Such scenarios must still be documented as their risk rankings and recommendations may vary. Teams may become frustrated by the apparent repetition.

Team leaders must also motivate team members and ensure that they work together effectively as a team. Leaders should model the behaviors they expect of team members and seek to understand personalities, which can provide insights into how team members may interact with each other. The team must be managed and challenges anticipated so that preparations can be made to deal with them. Team leaders should develop leadership and facilitation skills through training and practice.

21.10 Collecting and Preparing Reference Information and Data

Information on the hazardous chemicals, technology, and equipment in the process, often called *process safety information*, is needed to perform a PHA (Table 21.2).

Information gathering may involve:

- administering questionnaires
- collecting and reviewing written documents
- conducting surveys
- touring the facility and making observations
- interviewing facility personnel.

PHA team members also contribute their knowledge of the facility during the performance of a study.

The compilation of needed information should begin well in advance of the first PHA session as some of the information may require a significant amount

Table 21.2 Information and data needed for PHA.

Process safety information (PSI)		
Hazardous chemicals	**Process technology**	**Process equipment**
Toxicity information Permissible exposure limits Physical data Reactivity data Corrosivity data Thermal and chemical stability data Hazardous effects of inadvertent mixing of different materials that could foreseeably occur	Block flow diagram or simplified process flow diagram Process chemistry Maximum intended inventory Safe upper and lower limits for process parameters Consequences of deviations, including those affecting the safety and health of employees	Materials of construction Piping and instrument diagrams Electrical classifications Relief system design and design basis Ventilation system design Design codes and standards employed Material and energy balances Safety systems
Other information		
Process description Information on vendor-packaged units Plot plan Critical actions list Critical operating parameters list Procedures Information on previous incidents including near misses Instrumentation and controls Operating modes Critical equipment list Equipment data Critical safety systems list Vessel, piping, and equipment chemical inventories Services and utilities	Vulnerable locations on-site and off-site Electrical one-line diagrams Schematic wiring diagrams Mechanical drawings General arrangement and elevation drawings Drainage layout drawings List of car sealed valves (open/closed) Fire protection design philosophy and basis Emergency action plan/emergency response plan Operating history and condition of equipment Corrosion control information and corrosion rates	Compatibility matrix (materials of construction versus list of process chemicals) Maintenance, test, and inspection records Relevant codes, standards, and practices HAZID study Off-site consequence analyses, if available Quantitative Risk Analysis (QRA) studies, if available Staffing strategy (attended/unattended) Applicable warnings and safety alerts Local area maps showing off-site receptors Meteorological conditions Process Safety Management (PSM) audit reports

of time to develop, update, or assemble. It is useful to employ a checklist to keep track of information and identify its location. The validity of the PHA depends on the quality of the information on which it is based, so it is important to confirm that the information is accurate, complete, and clear. In particular, piping and instrumentation drawings (P&IDs) must be up-to-date. Despite these efforts, inaccuracies may be discovered in drawings or documents during the performance of the PHA. Corrections should be marked and a set of the marked-up drawings and documents kept with the PHA report. If the changes are extensive, the documents may need to be updated before the PHA can proceed.

21.11 Estimating the Effort Involved and Scheduling Study Sessions

Estimates of the effort required for a PHA are usually based on the number of nodes or systems/subsystems for the process. As a rule of thumb, it may require 2–6 h (or more) per node or system, depending on how nodes or systems/subsystems are defined. However, the actual time required will depend on the skill and experience level of the team and the leader, the complexity of the node or system/subsystem and process, team dynamics, and the fluency of team members in a common language. Novice teams typically will take longer for the first few sessions and, even with an experienced team, the first few nodes or systems will take longer. For batch processes, or the inclusion of other operating modes for continuous processes, the estimate should be increased by 10–100% per batch step or operating mode. Estimates should be conservative and account for breaks during sessions, team member substitutions, the possibility of plant distractions, and missing documents or lack of ready availability of needed information.

A PHA may take from a few hours to several months to complete depending on the size and complexity of the process and the scope and objectives of the PHA. Team member burnout must be avoided while maintaining momentum by avoiding long gaps between meetings. Many practitioners schedule one 4–6 h session per day to provide some time each day for team members to follow up on study items and attend to their regular duties. Alternatively, if the study must be performed with urgency or full team days are required, two 3 h sessions can be scheduled, although they should be separated by a lengthy break. For single sessions, mornings are preferred when personnel are fresher, more alert, and better able to brainstorm.

Consecutive daily sessions are best for studies estimated at 1 week or less. For multi-week PHAs, scheduling three to four sessions per week is preferable to provide at least a full day each week for team members to attend to their normal duties. However, flexibility is needed to accommodate a variety of situations. For example, alternating days and/or weeks can be scheduled. Team member commitments, both business and personal, should be considered.

Team leaders must be made aware of possible constraints such as working hours and breaks for team members who are union members. Management and team

members should be advised of the anticipated schedule and management approval obtained for the time each team member will need to participate.

The schedule should be prepared early so that:

- Team members can plan for the time commitment required.
- Management is aware of the total time required.
- Time required can be factored into project schedules.
- Progress checks can be made against the projected schedule.
- Logistical issues, such as the availability of a meeting room, can be addressed as soon as possible.

21.12 Briefing/Training Team Members

Team members should be briefed on the PHA procedure that will be followed and reviews should be provided of the study PSO, the process and its hazards, and available information to support the study.

Novice teams will benefit from a short training session on PHA. Practice in the PHA technique to be used is beneficial. This briefing can be conducted shortly before the PHA begins or as part of the first session.

21.13 Arranging Required Facilities

A meeting room is required to conduct the study sessions. Ideally, it should be away from the facility, for example, at a neighborhood hotel, to provide fewer distractions and disturbances. However, an on-site meeting room provides access to the facility, proximity to reference materials, and availability of office equipment. Sufficient wall and table space is needed to display drawings and documents and team members must be able to enter, exit, and move around the room without obstructions.

A means is required to record the PHA. Typically, computer software is used so a computer and computer projector are needed. The latter is used so that all team members can see entries as they are being made in the PHA worksheet. A white board or flip chart should also be provided for impromptu use.

The room environment and lighting must be controllable and suitable. Temperature, humidity, ventilation, air quality, noise, and so on should not interfere with the study. Variable lighting is needed to optimize viewing of the PHA worksheet by computer projection and the reading of documents. Window blinds are needed to control sunlight. Of course, office supplies and refreshments should be provided.

Video or web conferencing for PHA sessions is not recommended. Efficiencies and synergistic benefits of in-person meetings are lost and facilitation is harder. Personal interactions of team members are very important. However, video or web conferencing may be acceptable in some cases, for example, when team members

are separated geographically, when team members know each other well, or when consulting with a subject matter expert.

21.14 Other Items

The team leader should prepare a project plan for the study to help ensure an efficient and effective study. Typically, the plan will include such items as:

- identification of the chosen PHA technique
- reference to PHA procedures to be used
- PSO of the study
- names and roles of team members
- list of reference information to be used
- schedule (dates and times) and locations of PHA sessions.

The plan should be reviewed with the responsible manager, who should approve it and provide authorization to proceed with the PHA. The team leader and the responsible manager must agree on the authority of the team leader before the PHA study begins, for example, the freedom to postpone a PHA session if core team members are absent or if needed information is not available.

The team leader should formally notify team members, and their supervisors or managers, of their selection for participation in a study and their role and responsibilities. The intent is to ensure their availability and attendance. Team leaders should also provide an information package to team members so that they can prepare for participation in the study. The package should contain such information as the study PSO; reference data to be used; and the dates, times, and locations of sessions. The team leader may prepare session aids such as checklists to assist team members during PHA sessions and also configure recording software for the study. Thorough preparation is vital for a smooth-running and high-quality study.

21.15 Subdividing the Process

The process must be divided into sections that are consistent with the scope of the study for detailed review. Either nodes or systems and subsystems are used. Node or system selection defines, in part, the level of resolution for the study and the amount of detail that is recorded in the PHA. Different process subdivisions may be needed for different modes of operation.

Nodes are used in HAZOP. Generally, they are defined as pipe sections and major vessels in which process chemicals are, or may be, present. This is the ''line-by-line'' HAZOP method. They may also be steps in a procedure, or process functions such as control loops. Some companies use combinations of lines and vessels as ''super-nodes'' to speed up the study. While the study may take less time,

and provide a bigger picture, it does so at the expense of complicating the analysis and likely missing hazard scenarios. Early design stage HAZOP studies may use this approach when the disadvantages are not so significant.

Systems and subsystems are used in other PHA methods, such as WI analysis. They are simply a convenient way to divide the process into sections. They may be process areas, buildings, units, unit operations, major vessels and associated piping, and so on. Typically, the facility will already have a way of looking at the process as a number of separate parts. This is often a useful point of departure for subdividing the process, for example, 100 area, 200 area, and so on. Generally, each system will have multiple subsystems. For example, a tank farm (system) may have several different product storage areas (subsystems). The study is performed at the lowest level defined, usually subsystems. The size of systems and subsystems depends on how detailed a study is desired. Manageable parts must be selected so they cannot be too big. However, subsystems are usually larger than nodes.

Process subdivision is partly an art. There is no unique or ''correct'' choice of nodes or systems and subsystems for a process. However, equivalent PHA results can be expected with alternative subdivisions of similar complexity. The procedure for assigning nodes using the line-by-line method is as follows:

1) Start at the beginning of the process.
2) Identify each major vessel within the study scope such as reactors and storage tanks.
3) Starting with the first major vessel.
   a. Designate each inlet line in the main process flow path to the vessel as a node beginning with the main inlet line.
   b. Designate the vessel as a node.
   c. Designate each outlet line in the main process flow path as a node.
4) Repeat Step 3 for all vessels in the primary process flow path.
5) Designate vessels and lines in side streams and other process flow paths as nodes at any time that makes sense in the noding process.
6) Designate a global node (see definition below).

The procedure for assigning systems and subsystems is as follows:

1) Decide on the basis for subdivision.
2) Start at the beginning of the process.
3) Designate systems throughout the process according to the basis selected.
4) For each system, designate subsystems according to the basis selected.
5) Designate a global system (see definition below).

The goal of process subdivision is to choose the optimum number of nodes or systems/subsystems so that hazard scenarios can be identified as completely as possible while performing the study within a reasonable amount of time.

As the PHA study progresses, changes to the nodes or systems and subsystems may be needed. A node, system, or subsystem may be too complicated for the team to handle or may have been omitted inadvertently. The scope of the study

may change or the team's understanding of the process may increase as the study progresses and a different breakdown of the nodes, systems, and subsystems may be appropriate.

Global nodes or systems are used to represent the whole process, or certain aspects of it. They can be used to address initiating events that affect more than one node or system such as some external events, for example, flooding, and the process-wide loss of utilities, for example, electric power. They can also be used to address specific issues that arise in more than one node or system, such as those relating to facility siting and human factors. They also facilitate viewing hazards from the perspective of the overall process and can help to avoid the omission of hazard scenarios that may not be identified by focusing on individual nodes or systems such as multiple failure scenarios that may involve causes originating from within more than one node or system. Multiple global nodes or systems may be used for different purposes.

The team leader usually prepares the node or system and subsystem list prior to commencement of the study. Usually, a master set of P&IDs is marked up to show the process subdivision for reference during the study, for example, using colored highlighters.

21.16
Performing an Inherent Safety Review

Good engineering practice suggests that inherent safety principles be applied to processes. Such practice involves looking for changes to the process that eliminate the need for elaborate safety systems and procedures by either eliminating the hazard completely, or reducing its magnitude sufficiently, using means that are permanent and inseparable from the process. The application of inherent safety principles is best done at the design stage but it can also be done for existing processes. Consequently, the performance of an inherent safety review before a PHA study is conducted can be worthwhile to ensure that inherent safety methods are not overlooked as solutions to risk reduction or elimination.

Various inherent safety approaches are possible (CCPS, 2008b) and an inherent safety review involves a discussion of their applicability to a process. The entire PHA team can participate or a smaller or different group of people can conduct the review.

21.17
First Session

A number of important orientation and training issues should be addressed in the first session of a study. The team is briefed on the study and informed of what to expect in the PHA sessions. The process of establishing the group as a functional team should begin as quickly as possible. Items to address include:

- team member introductions
- PHA orientation
- explanation of PHA procedure
- review of study PSO
- process overview briefing
- review of process hazards
- review of available process safety information (PSI)/study data
- review of initial process subdivision
- review of guidelines for behavior by team members and rules to govern how the PHA will be conducted
- explanation of how recommendations will be handled
- viewing of the process.

The foundation should be laid for a constructive study. The team should be informed that it is normal for PHA studies to find areas of needed improvement, even when processes are designed and operated by the most highly regarded people, and that no-one should feel threatened by critique of the process design, operation, and so on. Participants should be asked to help to ensure that the PHA is performed on the process as it is actually constructed and operated. Hence operators must be willing to describe operating practices that are actually followed rather assuming that written procedures are always followed. Similarly, participants must flag any inaccuracies they observe in process drawings or other information used in the study. There is little point in performing a PHA assuming procedures are followed and documentation is correct if that is not the case. The PHA performed may be of high technical quality but it would not correspond to any existing process and the time and effort invested in performing the study would be wasted.

A practice PHA session may be conducted, especially with inexperienced teams. Such a session can help teach the PHA method and, in particular, assist team members with their calibration of the risk ranking scheme to be used. Team members may have questions. They must be answered to their satisfaction to ensure that the entire team has an understanding of PHA and the process and is ready to begin the study.

A checklist can help to ensure that each PHA session proceeds smoothly. Items to address include:

- Check that facilities are O.K. prior to the session start time.
- Record session participants.
- Remind the team of expected behavior and rules for how the PHA will be conducted.
- Address information needs.
- Address any issues identified by team leader QC or by team member review of worksheets.
- Briefly review the study PSO.
- Briefly review where the team left off at the end of the previous session.
- Review the design intention for the parts of the process to be considered in the session.

- As each node/system/subsystem is studied, review the design intention for the node/system/subsystem.

21.18 Recording PHA Studies

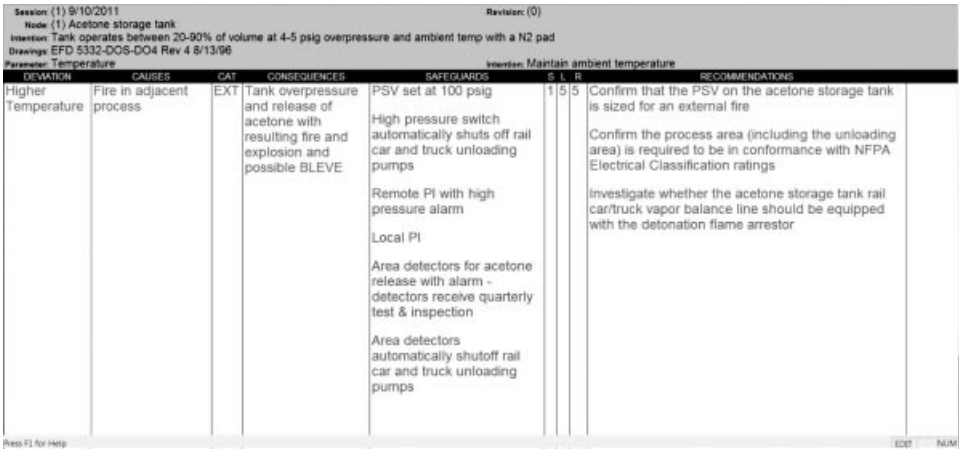
PHA study sessions are recorded in worksheets. Worksheet formats vary according to the PHA method, although most formats are similar (Figure 21.7). In addition to PHA worksheets, a report is also prepared to ensure that the PHA is properly documented.

The worksheet consists of two parts. In the banner or header, information such as the node name and intention is recorded (Figure 21.7). The main part of the worksheet contains information documenting the hazard scenarios identified by the team which are displayed in a column format showing their elements. It is useful to include in the banner the name and number of the drawing or document on which the node is shown. Other documents referenced or used to complete entries in the worksheet can also be recorded in the banner.

PHA worksheets are used in various ways:

- review by the team leader and team members after each session
- generation of actions on information needs
- reference by team members during the study
- quality control review by peers and/or third parties
- generation of actions on recommendations on completion of the study
- review by interested parties on completion of the study, for example, regulators
- revalidating PHAs.

There are two approaches to recording hazard scenarios in the HAZOP method: deviation-by-deviation (DBD) and cause-by-cause (CBC). In the DBD method,



Session: (1) 9/10/2011 Revision: (0)
Node: (1) Acetone storage tank
Intention: Tank operates between 20-90% of volume at 4-5 psig overpressure and ambient temp with a N2 pad
Drawings: EFD 5332-DOS-DO4 Rev 4 8/13/96
Parameter: Temperature Intention: Maintain ambient temperature

DEVIATION	CAUSES	CAT	CONSEQUENCES	SAFEGUARDS	S	L	R	RECOMMENDATIONS
Higher Temperature	Fire in adjacent process	EXT	Tank overpressure and release of acetone with resulting fire and explosion and possible BLEVE	PSV set at 100 psig High pressure switch automatically shuts off rail car and truck unloading pumps Remote PI with high pressure alarm Local PI Area detectors for acetone release with alarm - detectors receive quarterly test & inspection Area detectors automatically shutoff rail car and truck unloading pumps	1	5	5	Confirm that the PSV on the acetone storage tank is sized for an external fire Confirm the process area (including the unloading area) is required to be in conformance with NFPA Electrical Classification ratings Investigate whether the acetone storage tank rail car/truck vapor balance line should be equipped with the detonation flame arrestor

Press F1 for Help EDIT NUM

Figure 21.7 Example of a HAZOP worksheet.

causes, consequences, safeguards, and recommendations are related only to the HAZOP deviation. Specific cause–consequence–safeguard–recommendation relationships are not explicitly identified. Hence, all causes listed for a deviation do not necessarily result in all of the listed consequences. It is assumed that reviewers of the study can infer the correlations. This approach requires less time and documentation than the CBC approach. In the CBC method, consequences, safeguards, and recommendations are explicitly correlated with each particular cause of a deviation. Each cause has an independent set of consequences, safeguards, and recommendations relating to it. The CBC approach is more precise than the DBD approach. It avoids the ambiguity of the DBD approach, but it requires more time to document and produces lengthier documentation. The DBD approach cannot be recommended. Indeed, the Center for Chemical Process Safety (CCPS) emphasizes the use of the CBC approach (CCPS, 2008a) as it lessens the likelihood of overestimating scenario risks or crediting safeguards that do not apply.

PHAs can be recorded at different levels of detail. In ''by exception'' recording, a scenario is recorded only when the team develops a recommendation for it. This makes for shorter meetings and simpler reports while providing a basis for implementation of recommendations. However, it is of little value for subsequent uses, peer review and auditing are difficult, and some regulators have rejected the approach. Consequently, it is not recommended for general use. It may be appropriate for some non-regulatory uses of PHA.

In intermediate recording, hazard scenario entries are made even if there are no recommendations, for example, when existing safeguards are judged adequate. Entries are not made if there are no credible causes or significant consequences. This approach facilitates PHA of modifications at a later date, its coverage is clearer to auditors or reviewers, and there is an increased likelihood that all needed safeguards will be maintained during the life of the process as their purpose is made clear.

In full recording, entries are made for every deviation considered by the team, even when no credible causes or significant consequences are found, unless it is immediately obvious that it is unimportant. This approach permits a full audit and better withstands regulatory scrutiny, although at the expense of a lengthier worksheet. It is used if there is a need to demonstrate a high standard of process safety management, for example, for regulatory compliance. The level of recording must be determined by companies for each PHA to ensure that applicable regulatory requirements and expectations are met.

Some team leaders complete PHA worksheets before meeting with the team so that team members can prepare comments in advance of the PHA sessions and/or review the completed worksheets during the PHA sessions. Usually, this practice is not accepted by regulators. Moreover, it is not good engineering practice as the brainstorming that is such a vital part of PHA is mostly bypassed (Baybutt, 2012a).

Most PHA studies today are recorded using custom software packages such as PHAWorks. Some people use word processing, spreadsheet, or database software packages. PHA software improves the efficiency and effectiveness of recording studies. Software use speeds up the study, helps guide and control the team, avoids

the need for team review, comments, and editing, and facilitates sharing of PHA worksheets.

21.19
Making Worksheet Entries

21.19.1
Initiating Events (Causes)

The initiating event for a hazard scenario may be a single initiating cause, multiple simultaneous causes, or initiating cause(s) in the presence of enabling events or conditions. Initiating events may be equipment failures, human failures, or external events. Equipment failures may include:

- mechanical, for example, pumps, valves, piping, vessels, instrumentation
- structural, for example, foundations, supports, hangers
- electrical, for example, switches, motors, wiring
- electronic, for example, circuit boards
- programmable (i.e., computers, including software failures)

Several types of human failures are possible (Table 21.3). Such failures may be made by anyone who interfaces with a process, including designers, construction personnel, operators, mechanics, engineers, managers, and so on. While people have the ability to recognize their failures and correct them, recovery by people is usually not considered in PHA in order to be conservative.

External events originate outside the process but have an adverse impact on it (Table 21.4). They are also called *external factors*. External events can impact the entire plant or process, parts of the process, or specific pieces of equipment.

Causes may be defined at various levels, for example, immediate, basic, enabling, and root causes. There is a hierarchy of causality. Hierarchies with more levels

Table 21.3 Types of human failures.

Type	Meaning	Example
Omission error	Action is not performed	Operator fails to close a valve
Commission error	Action is performed incorrectly (wrong equipment, location, sequence, time, etc.)	Operator starts the wrong pump
Extraneous act	Non-required action is performed instead of or in addition to required action	Mechanic isolates two systems instead of one
Violations (deliberate acts)	Action that is prohibited, or different from that prescribed	Operator disables an alarm

can be defined, but four levels are sufficient for the purposes of PHA. Each immediate cause may have multiple basic causes and each basic cause may have various enabling and root causes. The immediate cause is the direct cause of the scenario, that is, the event that precipitates it, for example, pump fails off. It does not provide detail on why the failure occurred. The basic cause is the underlying reason for the immediate cause. It directly and proximately results in the immediate cause. For example, a pump can fail off for various reasons such as mechanical failure, switched off by an operator, and power supply failure. Enabling causes are contributing causes for basic causes. For example, pump mechanical failure could be caused by lack of preventive maintenance, incorrect maintenance, environmental stress, and so on. Often they are called *enablers*. Root causes are the fundamental underlying reasons for failure; for example, no-one is held accountable for performing preventive maintenance, responsibility is not clearly assigned, no-one checks maintenance work. Often, they are not identified in PHA unless they are known and important.

Detailed causes are needed for several reasons. Scenario risk estimates require that scenario severities and likelihoods be estimated. Likelihood estimates depend on the underlying reasons for the scenario cause. Scenario consequences and safeguards may vary according to the underlying causes for the same immediate cause. Also, recommendations for corrective action are most likely to address the level of causality used for the scenario causes. The deeper causes are explored, the more directly recommendations can address their prevention.

Ideally, PHA should identify at least basic causes, although initially teams may identify only immediate causes until it is determined if they result in scenarios within the study objectives. However, that determination requires careful consideration of possible basic causes. Obvious basic causes may not result in relevant scenarios, for example, pump power failure resulting in no feed, but less obvious basic causes may result in relevant scenarios, for example, pump mechanical seal failure resulting in a release.

Basic causes may have multiple underlying contributors, for example, a pump may fail off in a variety of mechanical ways. The focus should be on those

Table 21.4 Types of external events.

Type	Example
Natural events	Flooding, lightning, tornadoes, hurricanes, earthquakes
Human induced	Vehicle impacts, dropped objects from lifting devices
Utility failures	Electricity, instrument air, plant nitrogen, cooling water, steam
Knock-on or domino effects	Propagation of an incident to affect adjacent equipment, processes, or plants, for example, fires or explosions in adjacent facilities

underlying causes that result in scenarios within the study objectives, for example, when examining causes of low flow in a line, a mechanical valve failure that results in a leak of fluid from the valve should be recorded in preference to a mechanical valve failure that just reduces fluid flow if only safety scenarios are of concern and not operability scenarios.

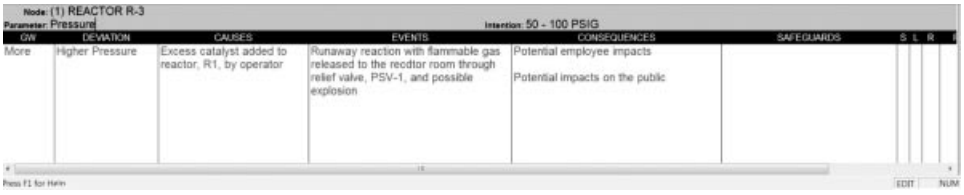
Only as much detail should be provided as is necessary to identify unique hazard scenarios, risk rank hazard scenarios, identify distinct consequences, and develop a full set of recommendations. Additional criteria for deciding on recording contributors to basic causes include dominance, that is, the most important contributors, and credibility, that is, they could occur.

Credible causes are included in the PHA whereas non-credible causes are not. Team judgment is used to decide whether causes are sufficiently probable to be considered credible. The inclusion of events with a low probability of occurrence is prudent as the catastrophic events that are the focus of PHA will be in a probability domain that is naturally low.

The causes of previous incidents must be captured in the worksheet. Not only is it a regulatory requirement in some parts of the world but also it makes sense to ensure that lessons from the past have been learned. Near-misses as well as actual incidents should be included.

21.19.2 Intermediate Events

The initiating event for a hazard scenario leads directly to intermediate events that precede the scenario consequences. Historically, many PHA worksheets have not captured intermediate events in a separate column. To the extent that they have been captured at all, information on intermediate events has been combined with entries in the consequences column of the worksheet. Consequently, their details have often been glossed over. A separate column for intermediate events is a valuable addition to the PHA worksheet (Figure 21.8), particularly when layers of protection analysis (LOPA) studies are planned for which such details are needed. It also helps to avoid confusion over entries in the consequences column and provides a cleaner worksheet. This is a recent innovation and is not yet common.


Node: (1) REACTOR R-3
Parameter: Pressure
Intention: 50 - 100 PSIG

GW	DEVIATION	CAUSES	EVENTS	CONSEQUENCES	SAFEGUARDS	S	L	R	I
More	Higher Pressure	Excess catalyst added to reactor, R1, by operator	Runaway reaction with flammable gas released to the reodtor room through relief valve, PSV-1, and possible explosion	Potential employee impacts Potential impacts on the public					

Press F1 for Help
EDIT NUM

Figure 21.8 Example of a HAZOP worksheet with an events column.

21.19.3 Consequences

Consequences are the ultimate result of the scenario cause, that is, what eventually happens as the result of a hazard scenario. Actual consequences may consist of a range of occurrences from the benign or minor to the possibly catastrophic.

Consequences can be expressed as:

- releases, for example, quantity of flammable gas
- dispersion distances or areas, for example, a specific material concentration
- physical effects, for example, size of fire, explosion, toxic exposure
- impacts, for example, number of fatalities, value of damaged equipment, cost of environmental remediation.

Companies must decide which form to use, although impacts are preferred as they are easier to understand. Additional secondary consequences may arise from hazard scenarios such as:

- smoke inhalation from fire scenarios
- exposure to toxic combustion products from fire scenarios
- exposure to hazardous materials produced in unintended chemical reactions
- injuries from trying to escape a highly hazardous material release
- injuries during emergency response activities.

Also, non-safety scenarios such as those producing operability problems may lead to safety problems through actions required to overcome them. Companies must decide whether such scenarios should be addressed in the PHA.

For a hazard scenario, there is usually a range of possible consequences depending on which, if any, safeguards fail. The scenario variants differ by degree of damage or injury and they can be depicted using an event tree. Typically, the scenario in which all safeguards are assumed to fail is recorded in the PHA worksheet. This practice is viewed as a regulatory requirement in some parts of the world. Furthermore, a representative scenario must be selected to avoid an unmanageable documentation burden. The worst-consequence scenario in which all safeguards fail is the most logical choice. However, this scenario may not be the worst-risk scenario and teams should be alert to this possibility and record both scenarios in such cases.

21.19.4 Safeguards

Safeguards should be documented in PHA worksheets for several reasons, including to:

- facilitate making and justifying recommendations
- perform risk ranking
- demonstrate the safety of the process

- document code/standard compliance, if required
- meet applicable regulatory requirements.

Safeguards may act to prevent, detect or indicate, or mitigate hazard scenarios. Prevention safeguards act to cause an event not to happen. Detection/indication safeguards discover or identify an incident in progress. Mitigation safeguards act to cause the severity of the scenario consequence to be less severe.

Safeguards may involve actions by humans or be automated. Human safeguards rely on operators or other personnel to take action to prevent an undesired consequence, for example, in response to alarms. Automated safeguards act without the need for human intervention, for example, a relief valve or a shutdown system. The performance of humans is usually considered less reliable than automated safeguards and must be considered when crediting human safeguards in PHA.

Safeguards can be classed as *administrative*, for example, control over inventories, *procedural*, for example, emergency response procedures, or *engineered*, for example, protective barriers. Administrative and procedural safeguards are human safeguards for which less credit is taken in PHA. Engineered safeguards may be *passive* or *active*. Passive safeguards employ equipment that is not physically actuated to perform its intended function, for example, a dike. Active safeguards employ equipment that is physically actuated in response to changes in process parameters or signals to perform its function, for example, a deluge system. Generally, passive safeguards are more reliable than active safeguards and more credit may be taken for them in PHA.

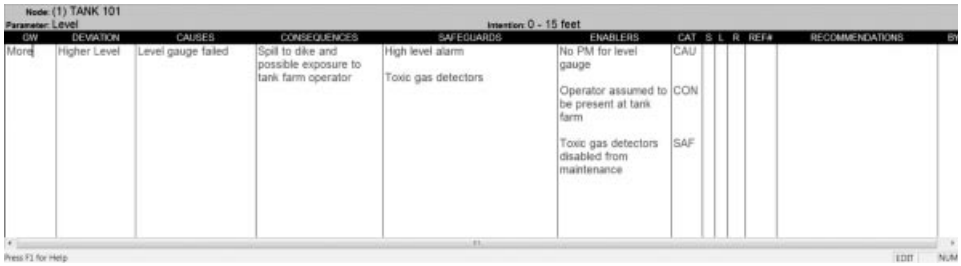
Safeguards should be qualified before being entered into the worksheet. Good practice is to use criteria such as:

- **Reliability**: Will it work?
- **Adequacy**: Is it enough?
- **Applicability**: Does it really apply? Is it directly applicable?
- **Effectiveness**: Does it accomplish its purpose?
- **Functionality**: Could it be inactive, bypassed, disabled, or easily removed?

Care should be exercised in taking credit for safeguards (Baybutt, 2012c). The inclusion of safeguards in a PHA increases their importance and they may become designated as critical safety systems requiring high reliability and more stringent preventive maintenance.

21.19.5 Enablers

Usually, enablers have not been addressed in PHA unless they were perceived to play a critical role for a scenario, for example, a disabled safety system. Some companies have begun to identify them when they plan to perform LOPA studies that address enablers. They can be captured in the PHA worksheet either by annotating the scenario element that they enable, that is, an initiating event, intermediate event, consequence, or safeguard failure, or by recording them in a separate enablers column (Figure 21.9). Enablers are key parts of hazard scenarios


Node: (1) TANK 101
Parameter: Level
Intention: 0 - 15 feet

GW	DEVIATION	CAUSES	CONSEQUENCES	SAFEGUARDS	ENABLERS	CAT	S	L	R	REF#	RECOMMENDATIONS	BY
More	Higher Level	Level gauge failed	Spill to dike and possible exposure to tank farm operator	High level alarm Toxic gas detectors	No PM for level gauge Operator assumed to be present at tank farm Toxic gas detectors disabled from maintenance	CAU CON SAF						

Press F1 for Help EDIT NUM

Figure 21.9 Example of a HAZOP worksheet with an enablers column.

and are often part of actual incidents. Consequently, it is good practice to address them in PHA.

21.19.6 Risk Ranking

There are no accepted industry standards for risk ranking schemes. However, it is advisable to establish corporate or, at the minimum, facility-wide schemes to lend consistency to PHA results for the company or facility. A standard risk ranking scheme allows the use of risk estimates in the compilation of recommendations into a centralized database.

Risk ranking schemes must provide for various types of consequences, for example, employee health impacts, public health impacts, and environmental impacts, depending on the types of consequences to be included in the PHA objectives. Frequently, schemes with multiple types of consequences and a single set of likelihood definitions for all consequence types are used (Figures 21.3 and 21.4). The same set of severity levels is typically used for different consequence types which may or may not imply equivalent impacts. If the impacts are equivalent, risk estimates can be compared across consequence types, otherwise such risk comparisons are not meaningful.

Usually, each combination of severity and likelihood is assigned a risk ranking (or risk level) (Figure 21.5), but there is no standard for making assignments. Risk levels can be labeled as classes, for example, using letters, and requirements for risk reduction defined for each class. Risk zones can also be used. They are areas on the risk matrix that define requirements for the management of recommendations that fall into that zone. The concept is similar to risk classes. Each zone can contain one or more risk levels and they are often displayed using colors. A risk profile can be provided for the process by plotting hazard scenarios on the risk matrix using either the total number of scenarios or the actual scenario numbers for each risk level. Risk profiles can be used to compare risks of different processes.

The severity, *S*, is the severity of the *consequence* for the hazard scenario whereas the likelihood, *L*, is the likelihood of all the events in the hazard scenario occurring together, including the cause, intermediate events, consequence, safeguard successes/failures, and so on. The estimates are made based on the collective

knowledge and experience of the team members. Estimation of consequences is easier than for likelihoods. Most team members will have some appreciation of the full spectrum of consequence severities from personal experience or awareness of industry events, which facilitates consequence estimation. Likelihoods of events that occur up to once in 100 years (the nominal human lifetime) often can be estimated without difficulty, but likelihoods of less frequent events are much more difficult to estimate. If serious disagreements arise within the team, a recommendation can be made to calculate the scenario severity and/or likelihood using more quantitative methods. Usually, this is not necessary.

Common practice is to base the severity value on a worst-case evaluation of the consequences, that is, all safeguards fail. Alternatively, credit may be taken for passive safeguards. As noted previously, the worst-*consequence* scenario may not be the worst-*risk* scenario for the same initiating event, although often the assumption is made that the two are the same. Furthermore, the worst-consequence scenario may depend on the type of consequence, and a scenario involving the successful operation of mitigation safeguards may have a higher risk than a scenario in which the safeguard fails. Scenario variants can be documented to deal with these issues. However, most practitioners currently consider only worst-case consequence scenarios.

In estimating the likelihood of the worst-case consequence scenario, the failure of all safeguards is assumed, that is, safeguard failure probabilities are addressed. This is not the same as assuming that there are no safeguards present. The existence of multiple credible safeguards can reduce the likelihood substantially. This compensates for the assumption of worst-case consequences for the severity estimate.

In addition to the initiating event and safeguards failures, the likelihoods of all other events/conditions that define the hazard scenario must be factored into the scenario likelihood estimate, including intermediate events besides safeguards failures, for example, control system actions, enablers, and conditional modifiers. Intermediate events are treated like safeguards. The probabilities of conditional modifiers are often conservatively assumed to be 1 unless there are good reasons not to. Other enabler probabilities can also be considered conservatively to be 1. Adjustments for at-risk factors may be used, for example, the fraction of time that alarms are disabled. However, detailed analysis of these probabilities is not warranted in PHA unless they reduce the risk by at least an order of magnitude.

Risk rankings are used to determine if a recommendation needs to be made. They can also be used to set time periods within which action items must be implemented. In the latter case, rules for exceptions may be needed when circumstances prevent the guidance from being followed, for example, how to ensure adequate safety when implementation of a recommendation is delayed. Some companies require notification of senior managers if time periods for implementation of action items are not met. This is called *risk escalation* or *elevation* in which increasingly higher levels of management must sanction continued tolerance of increasingly higher levels of risk.

Some companies determine the need for a recommendation based on the number and strength of existing safeguards, for example, safeguards are assigned a point value according to their strength and scenarios must be protected by a minimum number of safeguard points.

Some practitioners risk rank the severity and likelihood of the initiating event without considering safeguards to produce a ''raw'' risk estimate. A set of *S*, *L*, and *R* columns is placed before the safeguards column and the need for additional or modified safeguards is determined by assessing the effect of the existing safeguards on reducing the raw risk estimate to a tolerable level by using a second set of *S*, *L*, and *R* columns placed after safeguards. The extent to which a recommendation will reduce risk can be assessed but using a third set of *S*, *L*, and *R* columns placed after the recommendation column. Currently, the most common approach is to use a single set of risk rankings placed after safeguards.

Corporate or facility guidelines should be established to provide guidance on decision-making using risk rankings or safeguard strengths. Guidelines should not inhibit or influence the identification of recommendations by team members, for example, if a PHA team is told that all recommendations must be implemented before startup, they may hold back on making recommendations.

21.19.7 Recommendations

Both action items and information needs can be captured in the recommendations column of a PHA worksheet. Action items are corrective measures to reduce risk or recommendations for further studies. Information needs identify information that is not immediately available but is needed to complete entries in the PHA worksheet.

Typically, action items are specific risk reduction measures such as enhancements to existing safeguards or new safeguards. Alternatively, they may identify the need to develop specific risk reduction measures to address problems in cases where the PHA team did not recommend a solution. They may also be recommendations for further study of issues after the PHA has been completed. Routine (non-safety) administrative items such as updates to correct inaccuracies in drawings, procedures, or other documents may also be identified. Usually, a separate list of such administrative items is maintained for follow-up independently of PHA.

The need for action items is determined based on scenario risk, consequences, existing safeguards, the type of hazard, and the number of scenarios of the same type. The PHA team makes recommendations to reduce the risk to a tolerable level. Teams may still make recommendations for hazard scenarios when the risk is judged tolerable for ''nice-to-have'' items. Such low risk recommendations should be kept as a separate list.

For each recommendation, the person or department responsible may be identified using a ''By'' column in the worksheet for the initials of the person or department. However, the assignment of responsibility during the PHA may adversely affect participation and team dynamics. Team members may be reluctant

to make recommendations for which they will be assigned responsibility and team members may debate assignments. Moreover, team members may not be the best qualified to make assignments so they may be best left to management after the PHA has been completed.

Only obvious recommendations should be recorded during the PHA to avoid wasting significant time brainstorming recommendations. Even then the team should not try to identify every recommendation they can think of. The principal goal of PHA is to identify problems. The development of solutions can be accomplished after the PHA is complete. Ideally, problem solution should be separated from problem identification as they require different thought processes that can interfere with each other. However, PHA teams have a need to brainstorm to a certain extent, particularly when a serious scenario is identified. Rules can be established to control such brainstorming, such as a time limit, after which the development of a solution is deferred and a recommendation is made for follow-up investigation. Sometimes, the PHA team may be charged by management with producing solutions for all problems identified. Usually, this occurs when the PHA team members are the same people who would have to develop problem solutions on completion of the PHA.

Regulations usually do not specifically require that the PHA be updated as recommendations are implemented, although such changes may be covered under pre-startup safety review (PSSR) or management of change (MOC) requirements [OSHA, 1992]. Changes do need to be addressed in the next revalidation of the PHA. Some companies annotate the PHA to indicate the resolution and implementation of recommendations. Companies may wish to update the PHA to ensure that no new hazards are created by the changes.

Team members should not be allowed to waste time brainstorming entries for which they do not have needed information. An information need should be entered in the PHA worksheet so the team can move on and return to the issue when the information is available. All information needs must be addressed before the study team disbands and the study is completed. Consequently, on identification, information needs should be assigned to PHA team members who should be tasked with addressing the information need and reporting back to the team within one or two sessions. Time must be scheduled during the PHA sessions to go back and complete the worksheet using the information provided.

21.20 Special Topics

21.20.1 Multiple Failures

Multiple failures involve two or more events occurring together. They may be equipment failures, human failures, external events, or combinations thereof. Sometimes such failures are referred to as ''double jeopardy,'' ''triple jeopardy,''

and so on, and also as "double contingency," and so on. Failures that occur some time prior to another failure are usually considered to be latent conditions and treated as enablers. They include cases where equipment has been taken out of service or left in a disabled state, for example, a disabled alarm. Multiple failures may involve the initiating event or other elements of the scenario, for example, safeguards. For example, an initiating event may be the level controller on one fractionation column failing at the same time as the level controller on another fractionation column. This multiple failure might cause a higher than expected load of liquids in the overhead system that is not designed to handle both simultaneous failures. An example of multiple safeguard failures is where two redundant relief valves on a vessel fail at the same time, resulting in an overpressurization failure of the vessel.

It can be argued that actions taken to protect against single failures will also protect against multiple failures since they help protect against the individual contributors to the multiple failures, and that it is sufficient to address single failures only and not address multiple failures. Certainly, actions taken to prevent single failures that contribute to multiple failures will help prevent the multiple failures. However, that is not the whole story. Multiple failure scenarios may have more severe consequences than scenarios involving only one of their contributors and may merit additional safeguards beyond those implemented to protect against single failures. Furthermore, protective actions against single failures may not have been taken, having been deemed unnecessary for the lesser consequences involved. Thus, in the examples provided above, the failure of both column level controllers or both dual relief valves is more serious than the failure of either one individually. Consequently, credible multiple failures should be considered in PHA.

Possible guidelines for the consideration of multiple failures are:

- Two concurrent human failures are credible.
- A single equipment failure coupled with a single human failure is credible.
- The simultaneous failure of two or more *independent* pieces of equipment may not be credible.
- A single equipment or human failure with an external event may not be credible.
- The simultaneous occurrence of two or more independent external events is not credible.

These guidelines are based on the general relationship between rates of failure:
human failure > equipment failure > external events

Despite any guidelines, other multiple failures that the team may view as credible should not be eliminated. Also, regardless of their likelihood, some hazard scenarios which involve multiple failures may merit documentation owing to their extremely severe consequences or the existence of safeguards that protect against multiple failures which indicates that the designers considered such failures credible.

Usually, the team must be prompted to consider multiple failures, otherwise, there is a strong tendency towards considering only single failures. The identification of multiple failures for initiating events is challenging owing to the many possibilities that exist. Multiple failures involving other scenario elements are

easier to identify since the elements are defined as part of the scenario. Typically, teams use guidelines on the types of multiple failures that are considered credible and examine the process for such possibilities.

Multiple failures may be classified as non-credible because the contributors appear to lower the overall likelihood below the threshold for credibility, for example, a scenario with three contributors each with a probability of 1×10^{-3} produces an overall probability of 1×10^{-9}, which is negligible. However, the contributors must be independent for this to be true.

Some apparently independent failures may be dependent. In such cases, the likelihood of the multiple failure scenario will be higher than otherwise would be estimated. Therefore, dependent failures must be addressed in which two or more failures occur that are not independent of each other. Common-cause failures (CCFs) are a specific type of dependent failure where simultaneous (or near-simultaneous) multiple failures result from a single shared cause. The PHA team must understand CCFs and be aware of their importance. Common-cause multiple failures may be as likely as some single failures. Their presence can be identified using checklists. To be conservative in PHA, it should be assumed that dependent components do not reduce the scenario likelihood, for example, if two relief valves may fail dependently, the failure probability of only one is taken into account in estimating the scenario likelihood, that is, the failure probability of the second relief valve is assumed to be 1.

Suggested credible failures for inclusion in PHA are:

- single failures, for example, a pump failure
- common-cause multiple failures, for example, a breaker failure resulting in multiple pump failures
- non-common-cause multiple failures if they meet established guidelines or are considered credible by the team.

Usually, it is easier to get agreement on the credibility of single failures than multiple failures. However, multiple failures are important and guidelines for their treatment should be adopted and used.

21.20.2 Human Factors

PHA should address both human failures as causes of hazard scenarios and the human factors that impact human failures such as the operator/process interface (CCPS, 2007). Human factors engineering deals with the person/process and person/person interfaces and how they influence the performance of people. Human failure analysis deals with the failures that people may make in their interface with an engineered process. These failures and their rates are influenced directly by the human factors engineering design of the process.

Generally, human failures can be identified adequately in PHAs when brainstorming causes of hazard scenarios. Checklists of specific human failures can be developed and used to prompt the team to identify applicable failures. They range

from simple reminder checklists to detailed checklists. Use of reminder checklists is a common approach. More formal approaches are also available.

Human factors can be identified using simple checklists to remind the team of the types of human factors issues that should be considered in PHA. Entries are made in the PHA worksheets that identify human factors problems and their impact on hazard scenarios. Some companies use an auxiliary checklist, organized around human factors issues, which is more detailed and is applied to the entire process. More formal human factors studies can also be conducted. Performing a separate human factors study before the PHA study is preferred so the team can factor the information into the PHA without needing to generate it as the PHA is performed.

21.20.3 Facility Siting

Traditionally, facility siting has a broad interpretation and includes:

- location of the facility
- spacing of process units
- spacing between equipment
- spacing between equipment and potential ignition sources
- domino effects, that is, the potential for an incident to propagate from one area to another.

Facility siting can also address:

- some emergency response issues, for example:
  - accessibility for fire trucks
  - accessibility of fire hydrants/monitors
  - location of emergency refuges and assembly points
  - evacuation routes
- adequacy of hazardous area classifications:
  - Classes, Divisions, and Groups (United States)
  - Zones, Protection Types, Groups, Temperature Identifications (Europe).

Generally, it is accepted that facility siting also includes the spatial relationship between the hazards of the process and the location(s) of people in the facility, particularly in occupied buildings such as control rooms, although people may be present in other locations such as work stations, pipe yards, assembly points, and so on. Regulators are particularly concerned with the impacts of catastrophic accidents on employees, the public, and the environment owing to their locations with respect to the hazards of the process.

Pertinent facility siting issues should be addressed in PHA. A simple checklist can be used to remind the team of the types of facility siting issues that must be considered.

Entries are made in the PHA worksheets that identify facility siting issues and their impact on hazard scenarios. An auxiliary checklist can also be used, organized

around facility siting issues, which is more detailed and is applied to the entire process. Performing a separate facility siting study before the PHA study is preferred so that the team can factor the information into the PHA without needing to generate it as the PHA is performed. Guidance on facility siting has been developed by various organizations (CCPS, 1996, 2003; Chemical Industries Association, 1998; API, 2007, 2010).

21.20.4 Utilities

Utilities, services, and support systems are key parts of processes and must be addressed by PHA. Utilities include:

- water
- steam
- nitrogen
- instrument air
- electric power
- uninterruptible power supply
- standby power supply
- cooling/heating medium
- fuel.

Services and support systems include:

- communication system
- fire-fighting system
- flare
- incinerator
- scrubber
- medical services
- breathing air
- sewer
- waste water treatment
- weather station
- access control.

Utility failures are considered to be external events in PHA and their failures may be initiating events for scenarios. They may be treated in HAZOP as causes of deviations in process parameters such as flow or using parameters that represent the utility. Failures of services and support systems should also be addressed.

Utility systems are usually not subdivided into nodes or systems and subsystems unless:

- Utility interfaces directly with the process fluids, for example, nitrogen used for pressurized transfer of flammable materials.
- Utility plays an especially important role in key hazard scenarios.

- Hazards from the utility system are significant themselves, for example, high-pressure steam, hot oil, and they are within the study objectives.
- A separate PHA is performed on the utility system.

Utility systems often support multiple processes and sometimes a separate PHA is performed for the utility and referenced by the PHAs for the processes. Separate utility system PHAs may use different PHA methods than for the process. Often, simpler methods are used.

21.20.5 Modes of Operation

Modes of operation are stages of the process during its life-cycle, for example, routine startup, normal operation, routine shutdown, emergency shutdown. PHA studies should address all modes of operation that a process experiences. Characteristics of these other modes of operation can differ considerably from normal operation and hazard scenarios may be different. Other modes of operation may be more hazardous than normal operation. Operators may be less familiar with them and more prone to making errors. Non-steady-state conditions in some of these other modes of operation provide more potential for something to go wrong.

Multiple modes of operation can be addressed in several ways in PHA (Baybutt, 2012b). The simplest but least satisfactory way is to combine all modes into a single PHA. Many PHAs use this approach but it is not clear which entries correspond to which modes and it is difficult to treat all modes properly. In an effort to improve upon this approach, the guide word ''other than'' or parameters such as startup have been used. ''Other than'' is intended to be a reminder to include other modes of operation. Startup, shutdown, and so on are viewed as deviations from normal operation. This is a formal attempt to consider other modes but it usually lacks the detail provided for normal operation.

The use of a single PHA with annotation of worksheet entries and/or segmentation of worksheets for various modes is preferred to either of these approaches. Annotation of worksheet entries clarifies which ones belong to which modes of operation. For example, in HAZOP studies, nodes, parameters, or deviations can be annotated, for example, No Flow (startup), More Flow (normal operation), and so on. Care must be exercised to address appropriate deviations for each mode. For example, No Flow in a feed line may be a deviation during vessel charging but it may be the design intent after charging. Separate PHAs could be performed for each mode, although this is not common. Performing separate PHAs allows different PHA techniques to be used for different modes of operation.

Regardless of the approach selected, repetition of hazard scenarios from one mode to another should be avoided.

21.20.6
Process Changes

The impact on safety of changes in a process must be determined. PHA can be used for this purpose. Typically, it is used for major changes, extensive changes, high-risk changes, or where required by regulations. When PHAs on changes are performed that are not required by regulations, regulatory requirements need not be met so smaller teams may be acceptable and the PHA can be documented by exception.

PHAs on changes can be performed either by updating the existing PHA or by studying the change separately, which is best done for discrete, localized changes. When updating the previous PHA, of course, the same PHA method must be used. If a separate PHA is performed, a different PHA method may be used.

21.20.7
Procedures

Conventional PHAs focus on process equipment. Procedures for operation, maintenance, and so on are considered implicitly. This focus on equipment may lead to overlooking some hazard scenarios resulting from the procedures not being followed or being inadequate owing to human failures. Such hazard scenarios are important as procedures link people with the equipment and human failures are the most common type. An explicit treatment of procedures using PHA will produce more complete results. Procedural PHA can also be used to identify deficiencies when writing procedures.

Procedural PHA is necessarily a part of performing a PHA for non-steady-state processes such as batch processes. The process is similar to performing PHA on equipment. The principal difference is in how design intent is defined. Each step in the procedure is designated as a node or system/subsystem and the design intent is the content of the step. Deviations are generated from design intent by using HAZOP guide words or posing questions to identify possible failures in following procedures. Additional guide words are used to check steps for completeness and deficiencies. Typically, these are: how, why, when, where, who, check, and order. The remaining steps are the same as in an equipment-based PHA.

Procedural PHA overlaps to some extent with traditional equipment-based PHA but it provides more detail on human failures. Separate equipment and procedural PHAs may be performed. Any common hazard scenarios should not be repeated. Procedural PHA can be used as a ''fill-in'' for traditional equipment-based PHA so that hazard scenarios appear in a single study. This is accomplished by making another pass through the completed worksheets using the procedures as a formal design representation. Procedural PHA is not common for continuous processes. Typically, it might be conducted for high-risk processes, processes where accidents have occurred, and when questionable procedures exist.

21.20.8 Non-Steady-State Processes

PHA on non-steady-state operations, such as batch processes and multiple operating modes for continuous and batch processes, must identify hazard scenarios for each step in the process and each operating mode. Hazards may change from step to step and from one mode to another.

For PHA on batch processes, both the equipment and the batch procedure must be addressed. PHA results are confusing if the equipment is addressed for all batch steps simultaneously, and hazard scenarios may be missed if deviations from the batch procedure are not addressed directly. Therefore, PHA for batch processes is best accomplished by performing PHAs on both the equipment and the batch procedure following the timeline of steps in the batch procedure.

For the equipment-based PHA, the equipment involved in each step is identified and one or more nodes or systems/subsystems are defined in the usual way. The chosen PHA technique is applied to the nodes or systems/subsystems that have been defined for each step in the batch. The same pieces of equipment may appear in different batch steps, particularly central components such as mixing tanks, reactors, and so on. However, they should be viewed as being in different nodes or systems/subsystems as times and conditions are different and hazard scenarios may vary. Alternatively, each piece of equipment can be assigned to one individual node or system/subsystem and annotated information entered into the worksheet for the different times or steps. This approach is preferred as it is easier to reference earlier steps for the same piece of equipment. For the PHA on the batch procedure, each step in the procedure is designated as a node or system/subsystem and the study is performed in the way described in the preceding section.

Both the equipment and the batch procedure must be covered. Usually an equipment-based PHA is performed first and then either a separate procedure-based PHA is completed, avoiding repetition of scenarios from the equipment-based PHA, or scenarios are added to the equipment-based PHA by performing a procedure-based PHA as an adjunct.

Performing a PHA for different operating modes of continuous processes is similar to performing an equipment-based PHA on a batch process. Hazard scenarios must be identified for each mode of operation. Different nodes or systems/subsystems are used for the same piece of equipment in different operating modes or worksheet entries are annotated to indicate the operating mode.

21.20.9 Quality Control

Quality control is a key part of performing PHA for many reasons. People's lives, company and private property, and the company's well-being are at stake. PHAs usually require considerable time and effort and the investment must be worthwhile. PHAs are subject to regulatory review with the potential for fines and

adverse publicity if omissions or deficiencies are found. Any litigation that may result from accidents will likely focus on the quality of PHAs.

Quality control actions should be taken during study preparation and the performance of the PHA, and on completion of the PHA. Usually, checklists of key issues are employed by team leaders, team members, third-party reviewers, and management. The ability of the team to use the chosen PHA method to yield high-quality results can be compromised by inattention to quality.

21.20.10
Limitations and Cautions

PHA is subjective and depends on team judgment and the assumptions made. The results are subject to analyst bias, motivation, experience, knowledge, and creativity and depend on the accuracy and completeness of the written and verbal input data and the amount and quality of effort invested. Study success depends on the interactions of the team members. The selected PHA team might not have all the answers. No PHA technique can identify all hazard scenarios possible (Baybutt, 2003b).

PHA should not be construed as a substitute for good engineering. What is provided to the PHA team should represent the best product the designers can develop. PHA should not be viewed as a way to correct a substandard design.

A PHA study is valid only to the extent that the actual construction, operation, and maintenance match the intent of the design. There is no point in looking at the design intent if it is ignored, reviewing drawings if the hardware is different, referring to written procedures if they are not followed, or relying on instruments if they have been disconnected or not maintained.

21.21
Revalidation

Government regulations and industry standards require that PHAs be revalidated periodically, typically at least every 5 years (OSHA, 1992). Revalidation involves updating the PHA to account for changes that have been made to the process. Update means to make corrections, edit, and/or add new content, and revalidate means to declare that the PHA is valid again. Any separate, related studies will also need to be revalidated such as facility siting or human factors studies, or PHAs on procedures or control systems.

Many changes are processed through a company's MOC program and the impacts of changes on safety addressed. However, usually MOC analyses focus on individual changes and may not adequately account for the context of other changes. This concern is especially an issue when there are large numbers of changes. Thus, periodic revalidation provides an opportunity to perform an integrated evaluation of the cumulative and possibly synergistic impacts of all changes. Furthermore,

MOC programs often do not address all types of change that may impact safety and do not require updates to the PHA. Consequently, the objective of PHA revalidation is to produce an updated PHA that adequately addresses process hazards as they currently exist. Process changes may have introduced new hazards or changed existing ones, and there may have been changes in off-site receptors. Hence, the primary purpose of revalidation is to address changes subsequent to the previous PHA. However, it is also an opportunity to address the possibility of omissions and deficiencies in the previous PHA, whether the process safety information is complete, current, and accurate, and whether procedures are up-to-date. Some regulators expect such matters to be addressed as part of revalidation. There may be other relevant issues such as new process technology that has been implemented, or new information that has become available, or new requirements that have emerged since the previous PHA.

Different types of revalidation PHAs are possible. In an endorsement revalidation, no modifications are needed to the previous PHA. Of course, this type is not encountered frequently. In a revision or retrofit revalidation, the previous PHA is modified focusing on items specified in a revalidation plan. This type is unlike an initial PHA, where all aspects of a process are normally studied. Usually, revision revalidations are documented by updating the previous PHA worksheets. In a replacement/redo revalidation, the team starts over with a new PHA. This type is similar to an initial PHA but it also addresses the issues identified in a revalidation plan. An archive copy of the previous PHA should be kept for the life of the process for possible future reference.

Each revalidation PHA should be guided by a plan that specifies:

- PSO
- items to be studied:
  - process changes
  - omissions and deficiencies in the previous PHA
  - incidents that have occurred since the previous PHA was performed
  - open recommendations
  - new process technology/information
  - new requirements
  - multiple regulations.
- PHA technique to be used
- team composition
- information needed
- schedule for study
- type of revalidation needed.

The revalidation plan contains checklists of items to be addressed that are used in performing the revalidation. Once the plan has been produced, other aspects of planning and organization of the PHA revalidation are similar to those for initial PHAs.

21.22
Report Preparation

PHA worksheets alone are not adequate to document a PHA study. A comprehensive written report should be produced and is typical industry practice. The report must be clear, accurate, and complete as it will be used by people who were not part of the study team, for example, to follow up on study recommendations. It provides a permanent record of the study and is prepared after the study is completed. The report provides proof to regulators and others that the study was conducted. It may be consulted by stakeholders such as facility personnel and other persons or organizations that have a legitimate interest in the PHA. A report is also needed to facilitate auditing, for periodic revalidation, and for MOC reviews.

Typical report contents include:

- process description
- study PSO
- summary of the study results
- list of recommendations made
- description of the PHA approach used
- how the study was conducted
- who participated
- assumptions made
- PHA worksheets
- copies of reference materials used during the study.

The report must be structured to meet the needs of various audiences, including management, technical reviewers, and regulators. It should be prepared as soon as possible after the study is completed when information is fresh and the report is easier to produce. Management should be provided with the results in a timely fashion so they can act promptly.

PHA reports are sensitive documents. They should be safeguarded from access or theft for malicious intent, and damage/destruction while providing access to meet regulatory requirements, and for valid uses such as PHA revalidations and auditing.

21.23
Follow-up

Various actions are needed on completion of a PHA, including:

- developing a full set of recommendations
- categorizing and prioritizing recommendations
- resolving recommendations
- managing action items, that is, recommendations that will be implemented
- communicating PHA results to affected parties.

A full set of recommendations must be produced for consideration by management.

Recommendations should be developed for problems where the PHA team did not develop recommendations. Additional and alternative recommendations to those developed by the PHA team can be considered. A group of engineers normally performs this task. The PHA Team Leader may need to participate to explain the PHA results. Once a full set of recommendations has been developed, they must be resolved by management, that is, decisions must be taken on which should be implemented. This review is the responsibility of management but it may involve various technical disciplines.

PHA results need to be presented in a form suitable for decision-making. Recommendations should be categorized and prioritized. Categorization helps to make sense of the PHA results and prioritization helps to decide the order of implementation. Recommendations should be categorized based on the PSO of the study, for example, by consequence type. Categorization helps in organizing the recommendations and assists in planning follow-up activities. Various factors may be considered in prioritizing recommendations, including risk, cost, feasibility, and so on. The key criterion is risk and usually risk ranking is employed.

A management system is needed to facilitate implementation of recommendations and to ensure that:

- Recommendations are addressed promptly.
- Recommendations are resolved in a timely manner.
- Resolutions are documented.
- Differences of opinion between management and the PHA team are addressed.
- Actions to be taken are documented.
- A written schedule is developed for the completion of actions.
- Responsibilities for actions are assigned.
- Needed resources are provided.
- Actions are communicated to people whose work assignments are in the process and who may be affected.
- Commitment is obtained from affected employees.
- Management oversight and follow-up occur.
- Actions are completed as soon as possible.
- Actions are implemented in the way intended by the PHA team.
- Completion of actions is verified.
- Completion of actions is documented.

Periodic audits can help to ensure that recommendations have been resolved and action items have been implemented in a timely manner.

The results of PHAs should be communicated to affected employees, including operators, mechanics, contractors, and so on. Access to PHA reports alone is not sufficient; proactive communication is needed. Communication should be tailored to the audience and information relevant to the job presented. For example,

operators may be informed of errors to watch out for and new cautions and warnings that will be placed in procedures.

Proper management and follow-up of study recommendations are needed to comply with regulations and industry standards and to ensure that PHA study findings and recommendations are not neglected.

Acknowledgments

The copyright of all figures and tables in this chapter is held by Primatech Inc. or Professional Training Services Inc. The copyright of Appendices 21.A and 21.B is held by the Primatech Press Inc. The figures, tables, and appendices are used with permission.

Appendix 21.A. Descriptions of PHA Methods

Preliminary Hazard Analysis (PrHA)

PrHA identifies the hazards of a process and the hazardous situations they may produce. Possible causes, consequences, and recommendations for protective measures are addressed. A criticality ranking may be assigned and used to prioritize protective measures.

Typically, PrHA is used to evaluate and prioritize hazards early in the life of a process as a precursor to more detailed hazard analysis studies. Generally, it is applied during conceptual design or at the R&D stage when there is little information available on design details or operating procedures. Commonly, it is used as a design review tool before a P&ID is developed. It is useful in making site selection decisions and in analyzing large facilities when circumstances prevent other techniques from being used.

The procedure for conducting a PrHA is:

1) Prepare and organize the study.
2) Subdivide the process.
3) Identify process hazards and hazardous situations.
4) List causes.
5) Specify consequences.
6) Assign criticality ranking.
7) Identify any recommendations.
8) Document the results.
9) Resolve recommendations.
10) Follow up on recommendations.

Checklist

A checklist used as a hazard evaluation procedure employs prepared lists of questions relating to process safety to identify concerns and prompt the analysts to

determine whether existing safeguards are adequate. Checklists are used to identify common hazards and ensure compliance with procedures, codes of practice, regulations, and so on. Checklist questions are based on experience and knowledge of safety issues for the process and applicable codes, standards, and regulations.

Checklists can be applied to virtually any aspect of a process, such as equipment, materials, procedures, and so on. Their application requires knowledge of the process and its procedures and an understanding of the meaning of the checklist questions. Checklists may become outdated and they should be audited and updated regularly.

The procedure for performing a checklist study is:

1) Prepare and organize the study.
2) Select or generate the checklist.
3) Perform the study.
4) Identify any recommendations.
5) Document the results.
6) Resolve recommendations.
7) Follow up on recommendations.

What-If (WI) and What-If Checklist (WIC)

WI studies involve posing questions relating to initiating events to identify hazard scenarios for a process. The PHA team brainstorms questions in a WI study. The team starts with a prepared list of questions in a WIC study, although almost always additional questions are added as a study proceeds. Sometimes PHA teams develop questions based on the HAZOP thought process by thinking through what questions would arise if a HAZOP study were being performed.

WI methods are well suited to examining the impacts of proposed changes in MOC PHA studies because the questions can be tailored to the change and the areas affected by it. They can be used to study virtually any aspect of a process, such as equipment, procedures, control systems, management practices, and so on. Team leaders should be experienced with the technique since it is provides less structure than other PHA methods.

The procedure for conducting a WI or WIC study is:

1) Prepare and organize the study.
2) Subdivide the process.
3) Develop questions.
4) Identify hazards and/or hazard scenarios.
5) Specify consequences.
6) Identify safeguards.
7) Optionally, identify enablers.
8) Perform risk ranking.
9) Identify any recommendations.
10) Document the results.

11) Resolve recommendations.
12) Follow up on recommendations.

Hazard and Operability (HAZOP) Study

The HAZOP method is used to identify hazard scenarios with impacts on people and the environment in addition to operability scenarios where the concern is the capacity of the process to function. Originally, it was developed for fluid processes but it has also been applied to non-fluid systems such as materials handling, drilling operations, aerospace systems, and so on. Currently, it is the most commonly used technique in the process industries.

The HAZOP method focuses on investigating *deviations* from design intent such as ''no flow'' at a location in the process where flow is intended or ''high pressure'' in a vessel which should not exceed a pressure limit. By definition, deviations are potential problems, for example, no flow in a transfer line or overpressuring a vessel. Deviations from design intent are generated by applying *guide words* to process *parameters* at different locations (*nodes*) throughout the process, for example, for an inlet line to a vessel, No + Flow = No Flow, or for a vessel, High + Pressure = High Pressure.

A standard list of seven guide words is used: No, More, Less, As Well As, Part Of, Reverse, and Other Than. The team chooses appropriate parameters for each node, for example, flow, pressure, temperature, composition, level, addition, cooling, location, and so on. The use of guide words with parameters provides the opportunity to explore deviations from design intent in every conceivable way, thus helping to ensure completeness of the PHA study.

The procedure for conducting a HAZOP study is:

1) Prepare and organize the study.
2) Subdivide the process.
3) Select process parameters.
4) Specify parameter intention.
5) Generate deviations.
6) Identify causes of deviations.
7) Specify consequences.
8) Identify safeguards.
9) Optionally, identify enablers.
10) Perform risk ranking.
11) Identify any recommendations.
12) Document the results.
13) Resolve recommendations.
14) Follow-up on recommendations.

Failure Modes and Effects Analysis (FMEA)

FMEA is a hazard evaluation procedure in which failure modes of system components, typically process equipment, are considered to determine whether existing

safeguards are adequate. Failure modes describe how components fail (e.g., open, closed, on, off, leaks, etc.). The effects of each failure mode are the process responses or incident resulting from the component failures, that is, hazard scenario consequences. An FMEA becomes an FMECA (failure modes and effects and criticality analysis) when a criticality ranking is included for each failure mode and effect. A criticality ranking is the same as a risk ranking.

FMEA is used extensively in the aerospace, nuclear, and defense industries. Typically, it is used in the process industries for special applications such as reliability centered maintenance (RCM) programs and the analysis of control systems.

FMEA can be conducted at different levels of resolution. For PHA purposes, usually it is conducted at the equipment level, for example, valves, pumps, lines, and so on. For RCM purposes, usually it is conducted at the equipment component level, for example, motor, shaft, impeller, casing, seal, bearings, and so on for a pump.

The procedure for conducting a FMEA is:

1) Prepare and organize the study.
2) Subdivide the process.
3) List process equipment.
4) Identify equipment failure modes.
5) Optionally, identify causes of failure modes.
6) Specify effects (consequences).
7) Identify safeguards.
8) Perform risk ranking.
9) Identify any recommendations.
10) Document the results.
11) Resolve recommendations.
12) Follow up on recommendations.

Major Hazard Analysis (MHA)/Direct Hazard Analysis (DHA)

MHA was developed specifically to support process safety studies (Baybutt, 2003a; Baybutt and Agraz-Boeneker, 2008). It is used to identify major hazard scenarios involving fires, explosions, toxic releases, and reactivity excursions. Direct hazard analysis (DHA) is an extension of MHA used to address any type of hazard.

MHA employs a structured approach to identify loss of containment scenarios. Causes of loss of containment can be direct, for example, valves left open or ruptures in lines or vessels, or indirect, for example, runaway reactions resulting in releases through pressure relief devices or vessel and piping rupture. MHA constrains brainstorming to such scenarios within a structured framework to guide the identification of initiating events using standard checklists. Brainstorming focuses on specific categories of initiating events to focus the team's brainstorming without narrowing their vision. The checklists provide guidance to the team and help assure completeness. They can be customized for specific facilities or types of processes. The method prompts consideration of items not already in the checklists. MHA uses a process subdivision similar to other PHA methods.

DHA extends MHA to address other hazards such as overpressurization, entrapment by moving equipment, and so on. Each hazard type uses a structured list of categories of initiating events and ways they can occur. Such lists can be developed for any hazard.

The procedure for conducting a MHA or DHA is:

1) Prepare and organize the study.
2) Subdivide the process.
3) Identify initiating events.
4) Specify consequences.
5) Identify safeguards.
6) Optionally, identify enablers.
7) Perform risk ranking.
8) Identify any recommendations.
9) Document the results.
10) Resolve recommendations.
11) Follow up on recommendations.

Process Hazard Review (PHR)

PHR was developed for use with operating plants as an alternative to HAZOP (Ellis, 2004). It addresses major hazards. There are variants that address other types of hazards and environmental releases. It is based on the premise that most major hazard process incidents involve loss of containment. PHR uses prompts covering the range of mechanisms for loss of containment to identify hazard scenarios. The method has been extended to address other hazard types (Operational Hazard Review) and environmental releases (Environmental Hazard Review).

The procedure for conducting a PHR is:

1) Prepare and organize the study.
2) Subdivide the process.
3) Select prompt/guide word.
4) Describe hazardous event scenarios.
5) Identify causes of hazardous event scenarios.
6) Specify consequences.
7) Identify safeguards/existing controls.
8) Perform risk ranking.
9) Identify any recommendations.
10) Document the results.
11) Resolve recommendations.
12) Follow up on recommendations.

Fault Tree Analysis (FTA)

FTA is not really comparable to standard PHA methods. It does not identify a full set of hazard scenarios for a process. Rather, it is used to identify the causes of

a particular incident (called a top event) using deductive reasoning. Often, it is used when other PHA techniques indicate that a particular type of accident is of special concern and a more thorough understanding of its causes is needed. Thus, it is a useful supplement to other PHA techniques. Sometimes FTA is used in the investigation of incidents to deconstruct what happened. FTA is also used to quantify the likelihood of the top event. It is best suited for the analysis of highly redundant systems.

FTA identifies and graphically displays the combinations of equipment failures, human failures, and external events that can result in an incident. Computer programs are used to provide graphical representations of fault trees and to calculate top event likelihoods. FTA is not a technique that lends itself to a team-based study. Typically, one or two people construct a fault tree. It requires different training and resources than other PHA techniques.

The procedure for conducting a FTA is:

1) Prepare and organize the study.
2) Construct fault tree.
3) Analyze fault tree.
4) Quantify fault tree.
5) Evaluate results.
6) Identify any recommendations.
7) Document the results.
8) Resolve recommendations.
9) Follow up on recommendations.

Event Tree Analysis (ETA)

ETA is not really comparable to standard PHA methods. It does not identify a full set of hazard scenarios for a process. Rather it is used to identify the possible outcomes following the success or failure of protective systems after the occurrence of a given starting event and, optionally, to calculate the frequencies of the outcomes. Event trees graphically display the progression of event sequences beginning with a starting event, proceeding to control and safety system responses, and ending with the event sequence consequences.

ETA helps analysts to determine where additional safety functions will be most effective in protecting against the event sequences. Typically, ETA is used to analyze complex processes that have several layers of safety systems or emergency procedures to respond to starting events. ETA is not a technique that lends itself to a team-based study. Typically, one or two people construct an event tree.

The procedure for conducting an ETA is:

1) Prepare and organize the study.
2) Identify a starting event.
3) Identify controls and safeguards that respond to the event.
4) Construct the event tree.
5) Describe the event sequence outcomes.

6) Optionally, calculate the frequencies of the outcomes.
7) Identify any recommendations.
8) Document the results.
9) Resolve recommendations.
10) Follow up on recommendations.

Cause–Consequence Analysis (CCA)

CCA is a blend of FTA and ETA that produces a CCA diagram combining fault and event trees. It is used to identify causes and consequences of hazard scenarios. The CCA diagram displays the relationships between the incident outcomes (consequences) and their causes and it can depict and evaluate multiple scenario outcomes, including recovery paths where the operator, or system, recovers or mitigates the consequences, as well as the worst consequence path. CCA is commonly used when the failure logic of hazard scenarios is simple.

The procedure for conducting a CCA is:

1) Prepare and organize the study.
2) Select an event to be analyzed.
3) Identify safety functions that respond to the event.
4) Develop the event sequence paths resulting from the event.
5) Develop the combinations of basic failures that result in the starting event and safety function failures.
6) Evaluate the event sequences.
7) Identify any recommendations.
8) Document the results.
9) Resolve recommendations.
10) Follow up on recommendations.

Bow-Tie Analysis (BTA)

BTA is a less formal variation of CCA. It uses a combination of high-level fault and event trees to produce a diagram resembling a bow tie. Hazards and initiating events appear on the pre-event side (left side) and impacts (consequences) appear on the post-event side (right side). The focal point of the diagram is the specific loss event that ties together the initiating events and consequences. There is a time progression from the left to the right of the diagram. Associated prevention and mitigation safeguards are shown on either side of the loss event and they are viewed as barriers, some of which may apply to more than one cause.

BTA is used for screening hazards of well-understood processes and to perform an initial analysis for existing processes or in the middle stages of process design.

The procedure for conducting a BTA is:

1) Prepare and organize the study.
2) Select an event to be analyzed.

3) Develop the pre-event side of the diagram.
4) Develop the post-event side of the diagram.
5) Identify any recommendations.
6) Document the results.
7) Resolve recommendations.
8) Follow up on recommendations.

Appendix 21.B. Comparison of PHA Methods

Method	Advantages	Disadvantages
PrHA	Easy to understand Fast to perform	Requires careful judgment Not a detailed PHA method
Checklist	Easy to use and provides results quickly Level of detail can be varied Communicates information well Effective way to take advantage of lessons learned	Does not help in identifying new or unrecognized hazards May overlook unusual hazards or novel elements of a process No cause and effect analysis Usually requires some subjective interpretation Limited to the experience of the author Repetitive nature can lead to errors May not apply to the particular situation Provides a minimum level of hazard evaluation
WI and WIC	Easily understood Flexible Less effort/time Can help to identify scenarios that involve interactions between different parts of the process	Loose structure Results particularly dependent on the skill, experience, and thoroughness of users No assurance that the breadth or depth of the questions considered is adequate
HAZOP	Viewed as the most effective of traditional PHA methods Provides assurance that hazard scenarios have been identified Addresses both safety and operability	Difficult to exclude operability scenarios Difficult to consider all aspects of intention in a reasonable time period Effort involved can be significant Focuses on individual nodes and may miss some hazard scenarios that involve interactions between nodes
FMEA	Systematic, element-by-element procedure that helps ensure completeness Easily understood and used by engineers Easily updated for design changes or facility modifications	Not efficient for identifying combinations of equipment failures Human failures are not generally examined although the effects of misoperation can be described by an equipment failure mode or by the causes of a failure External events are not easily addressed

Appendix 21.B. (*continued*)

Method	Advantages	Disadvantages
MHA/ DHA	Focuses exclusively on hazard scenarios, that is, does not address operability scenarios Time required is substantially less than in traditional methods Structured approach Readily understood by PHA teams All hazard scenarios for a node appear in a single worksheet Current PHA studies can be converted easily into MHA format	Does not address operability scenarios
PHR	Structured method Quickly identifies and assesses major hazard scenarios Operations personnel can share their experience effectively	Focuses more on what team members know, not on what they do not know Generates more general recommendations rather than specific ones Proprietary method
FTA	Thorough and systematic	Can be time consuming Binary representation of faults (either success or failure, no partial failures)
ETA	Easy to understand	Can be time consuming Binary representation of failures (either success or failure, no partial failures)
CCA	Provides a detailed graphical depiction of hazard scenarios	CCA diagram can become complex
BTA	Easy to understand	Provides only a simple analysis Does not provide a formal way to identify loss events Can become complex for larger processes

References

API (American Petroleum Institute) (2007) *Management of Hazards Associated with Location of Process Plant Portable Buildings*, RP 753, 1st edn, American Petroleum Institute, Washington, DC.

API (American Petroleum Institute) (2010) *Management of Hazards Associated with Location of Process Plant Buildings*, RP 752, 3rd edn, American Petroleum Institute, Washington, DC.

Baybutt, P. and Agraz-Boeneker, R. (2008) A comparison of the hazard and operability (HAZOP) study with major hazard analysis (MHA): a more efficient and effective erocess hazard analysis (PHA) method. Presented at the 1st Latin American Process Safety Conference and Exposition, Center for Chemical Process Safety, Buenos Aires, 27–29 May 2008.

Baybutt, P. (2003a) Major Hazard Analysis: An Improved Process Hazard Analysis Method. *Process Saf. Prog.*, **22** (1), 21–26.

Baybutt, P. (2003b) On the ability of process hazard analysis to identify accidents. *Process Saf. Prog.*, **22** (3), 191–194.

Baybutt, P. (2012a) Prework and precompletion of worksheets for process hazard analysis. *Process Saf. Prog.*, **31** (3), 275–278.

Baybutt, P. (2012b) Process hazard analysis for phases of operation in the process life cycle. *Process Saf. Prog.*, **31** (3), 779–781.

Baybutt, P. (2012c) What risk reduction measures should be credited in process hazard analysis?. *Process Saf. Prog.*, **31** (4), 359–362.

CCPS (Center for Chemical Process Safety) (1996) *Guidelines for Evaluating Process Plant Buildings for External Fires and Explosions*, American Institute of Chemical Engineers, New York.

CCPS (Center for Chemical Process Safety) (2003) *Guidelines for Facility Siting and Layout*, American Institute of Chemical Engineers, New York.

CCPS (Center for Chemical Process Safety) (2007) *Human Factors Methods for Improving Performance in the Process Industries*, American Institute of Chemical Engineers, New York.

CCPS (Center for Chemical Process Safety) (2008a) *Guidelines for Hazard Evaluation Procedures*, 3rd edn, American Institute of Chemical Engineers, New York.

CCPS (Center for Chemical Process Safety) (2008b) *Inherently Safer Chemical Processes: a Life Cycle Approach*, 2nd edn, American Institute of Chemical Engineers, New York.

Chemical Industries Association (1998) *Guidance for the Location and Design of Occupied Buildings on Chemical Manufacturing Sites*, Chemical Industries Association, London.

Crawley, F., Preston, M., and Tyler, B. (2008) *HAZOP Guide to Best Practice*, 2nd edn, Institution of Chemical Engineers, Rugby.

Ellis, G.R. (2004) Process hazard review: the efficient risk assessment of existing plants. Presented at Loss Prevention and Safety Promotion in the Process Industries, 11th International Symposium, 2004.

IEC (International Electrotechnical Commission) (2001) IEC 61882. *Hazard and Operability Studies (HAZOP Studies) – Application Guide*, International Electrotechnical Commission, Geneva.

Kletz, T. (1999) *Hazop & Hazan: Identifying and Assessing Process Industry Hazards*, 4th edn, CRC Press, Boca Raton, FL.

Knowlton, R.E. (1992) *A Manual of Hazard and Operability Studies*, Chemetics International, Vancouver.

OSHA (Occupational Safety and Health Administration) (1992) *Final Rule on Process Safety Management of Highly Hazardous Chemicals; Explosives and Blasting Agents*, 29 CFR 1910.119. Occupational Safety and Health Administration, Washington, DC.