Chapter 1

PROCESS HAZARDS ANALYSIS BASICS

INTRODUCTION

A Process Hazards Analysis — or PHA — has two primary purposes. The first is to identify high-risk hazards associated with a chemical process — where a process is defined as any activity involving the use, storage, manufacture, handling or movement of chemicals. Once the high-risk hazards have been identified, corrective action can then be taken either to eliminate them or to minimize their impact.

The second purpose of a PHA is to create a way of thinking among all managers, employees and contract workers so that they will recognize process hazards during the normal course of their work. For example, an operator working by himself at two o'clock in the morning may be about to open a valve, but before doing so he pauses for a moment, and says to himself:

> "You know, opening this valve could lead to reverse flow, which could lead to wrong chemicals mixing with each other. Before opening the valve, maybe I should take a break, make a cup of tea, and talk over what I'm planning to do with my colleagues and supervisor."

When an employee thinks and acts in this manner, the PHA program is working very well indeed.

The same change in thought processes can sometimes be seen following a PHA, when an employee who knows a plant very well looks at the equipment and processes with fresh eyes — he or she will see the potential for accidents and losses in a new way.

PHAs are usually directed toward the identification of very low probability scenarios that could cause fatalities, serious injuries or major economic loss. Since such events occur only rarely, even the most experienced personnel may not have considered the possibility of their occurrence, so a PHA is needed to help them understand and appreciate that such events can occur. Indeed, a PHA can be regarded as being an Incident Investigation that takes place before the incident has occurred.

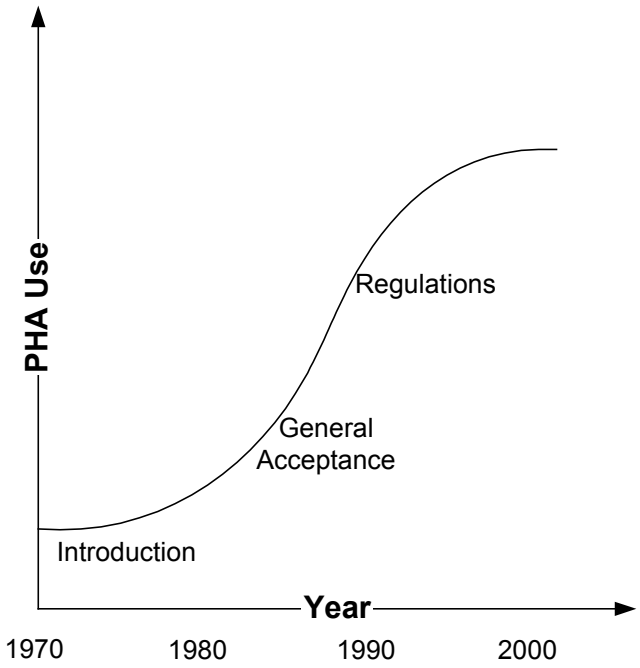
BACKGROUND

Before discussing PHA techniques in detail, it is appropriate to provide a very brief overview of the history of PHAs, the key elements of the PHA process, and the ways in which PHAs fit into the broader topic of Process Safety Management.

HISTORICAL REVIEW

The sketch in Figure 1-1 illustrates the growth in the use of PHAs over the last thirty years or so.

Figure 1-1
Historical Development Of PHAs



1960s/70s

Although companies in the process industries have always worked on the identification and control of hazards, the formal discipline of Process Hazards Analysis, specifically the HAZOP (Hazard and Operability) method, was not developed until the early 1960s by process plant professionals in the United Kingdom working for the British company ICI [1, 2]. The first formal paper describing the HAZOP technique was published in 1974 by an ICI employee [3].

1980/90s

During the 1980s the use of PHA techniques, particularly the HAZOP method, grew rapidly. However, it was the introduction of process safety regulations — particularly in the United States — in the late 1980s and early 1990s that caused the dramatic

growth shown in Figure 1-1. All process safety regulations stress the importance on finding and then correcting hazards, thus putting PHAs on center stage. Indeed, in the early days of Process Safety Management in the United States, it was not unknown to hear plant managers make statements along the lines of, “I know what Process Safety Management is — it’s HAZOPs!”

Although regulations may drive the schedule of a PHA program, such regulations rarely have much effect on the way in which PHAs are carried out. The means used for identifying hazards are pretty much the same everywhere; in particular, multi-national companies tend to implement a uniform policy regardless of where their plants are located.

The Future

By the end of the 1990s, most companies (at least in the United States) had conducted PHAs on those facilities with high-risk potential. These companies continue to conduct PHAs to validate changes and modifications. However, the initial growth spurt is now finished and most of the obvious hazards have been identified and addressed. Consequently some PHA professionals are looking for alternative ways of conducting PHAs. Some thoughts as to how PHAs may develop over the coming decade are provided in the final chapter of this book (page 278).

Elements Of A PHA

Although various PHA techniques are available, they tend to fall into one of three categories: those that encourage team members to “dream up” potential accident scenarios, those that draw on the experience of experts, and those that spell out the logic of how an incident may occur. Whichever method is chosen, a PHA should generally incorporate the elements discussed below.

1. Hazard Identification

The first goal of a PHA is identify hazards, where a hazard is defined as having the *potential* to cause a significant incident. For example, a PHA team may be discussing the possibility of a particular control valve failing open. This failure could, in turn, lead to an excess flow of chemicals into a reactor, which could then cause excessive pressure in that reactor, with the potential for its rupture. The hazard, therefore, is "Rupture of reactor initiated by failure in the open position of control valve number ___."

Having identified the hazard, the PHA team would then normally be expected to risk-rank that hazard in terms of consequence and predicted frequency, both with and without taking credit for safeguards. (How this is done is discussed in depth in Chapter 2). However, the PHA team is not expected to come up with specific conclusions or recommendations — that is the responsibility of the managers who follow up on the PHA.

2. Focus On Process Hazards

A PHA should focus on the identification of *process-related* hazards, *i.e.,* on the identification of process upsets that could create high risk hazards. A PHA team should not concern itself with occupational safety issues such as trips, falls, and the application of lock-out/tag-out rules. If such topics force their attention on the team, then the appropriate recommendation should be made — but such recommendations are incidental to the main purpose of the PHA. Further discussion regarding the differences between process and occupational safety is provided on page 40.

3. High Risk Hazards

The third goal of a PHA analysis should be to concentrate on *high-risk* hazards. Every hazard has associated with it a *consequence* (safety, environmental, economic) and likelihood or *predicted frequency* (not probability) of occurrence. From

these two parameters a risk ranked value for that hazard can be determined (*see* page 29).

In practice, many PHA teams concentrate not so much on the identification of high *risk* hazards, but of high *consequence* hazards. There is nothing inherently wrong with doing this, but the team members should be aware of the distinction. For example, it may be noted that the seal on Pump, P-101A, in the Standard Example (page 9) fails once a year with an estimated 1% chance that someone could be killed from a resulting fire. Hence, the estimated fatality rate from this incident is projected to be one in 100 years.

The same plant may also have the potential for rupturing a vessel containing large quantities of toxic chemicals. It is estimated that the consequences of such a rupture would be 10 deaths, but that the predicted frequency of such an event is once in a thousand years. Hence, the predicted fatality rate is one in 100 years — the same as for the pump seal incident. Each incident has the same *risk,* but the second incident has the higher *consequence.*

It is probably true to say that most PHA teams would spend more time analyzing the second incident (catastrophic vessel failure) rather than the more frequent seal failure. In other words, they are looking more for high consequence rather than high-risk hazards. Indeed, many companies consciously encourage their PHA teams to do this for two reasons. First, the higher frequency accidents (such as pump seals failing every year) are understood, and remedial actions may already be in hand. However, since high consequence incidents occur only very rarely, people cannot easily visualize such incidents. PHAs can be used to get these people to “think the unthinkable.” This is why one of the most important roles of the PHA team leader is to get the team members to think imaginatively, and to challenge statements of the type, “I’ve been here fourteen years, and I’ve never seen that happen . . .”, with the unspoken conclusion, .” . . therefore it cannot happen.”

One way of leading people to the belief that high consequence/low likelihood events can in fact occur is to use overall industry experience. For example, the probability of a major vapor cloud explosion on a refinery is around one in 2000 to 2500 years. Therefore, in a world universe of, say, 1000 refineries, it is likely that there will be such an explosion every two to three years — thus demonstrating that “it” can happen.

Another reason for focusing on high consequence incidents, is that they are the ones that tend to get the most publicity, that are the most emotionally wrenching, that generate law suits, and that have the potential of destroying a business (and the careers of those associated with that business).

Whether a PHA team focuses on high-risk incidents, or just on high-consequence incidents, depends on what management is looking for. Neither approach is inherently right or wrong; however, the team must be clear which goal they are pursuing.

Team Activity

PHAs are generally team activities (although some of the more specialized techniques, such as Fault Tree Analysis, may be conducted by a specialist working alone or with just one other person). The team members should represent a cross-section of disciplines and functions, typically including operations, engineering, maintenance, and process design. Having all the disciplines present helps ensure that all types of hazard scenarios are discussed. Furthermore, the interaction between team members helps uncover those hazards that may be created due to communication difficulties or misunderstandings between departments.

Thoroughness

A PHA must be thorough. Although no hazard analysis can claim to identify all hazards, PHAs should provide management and workers with an assurance that sufficient time was allowed for the analysis, and that the quality of the team, and of its discussions, were good.

Recommendations / Findings

The purpose of a PHA is to identify hazards, and then to assign a risk ranking to those hazards. It is not the purpose of a PHA to issue specific recommendations. The PHA analysis should merely list the hazards that have been identified, along with their associated risks. These *findings* will then be turned into specific *recommendations* by the appropriate departments and/or individuals following the conclusion of the PHA. The PHA team should be particularly careful not to become a "one-minute engineering department"; the purpose of the PHA is to find problems, not to solve them.

Intentional Error

PHAs are run on the assumption that everyone in the facility wants to do a good job and to foster a safe and productive environment. If people on the plant decide to deliberately create hazardous situations, or if external sabotage or terrorism are issues of concern, the PHA leader should immediately state that such problems are outside the project's scope, and must be managed in their own way — possibly including the use of law enforcement authorities. There is no defense against a knowledgeable employee, and very little against determined terrorists [a].

Process Safety Management

PHAs are part of the broader topic of Process Safety Management (PSM). To be fully effective, a PHA has to be linked to other elements of PSM, such as Process Safety

[a] This first edition of this book went to print immediately following the attacks of September 11th, 2001. It is likely that the current vulnerability study work will eventually be incorporated into the overall PHA process.

Information, Operating Procedures, and Management of Change. How this can be done is discussed in Chapter 9.

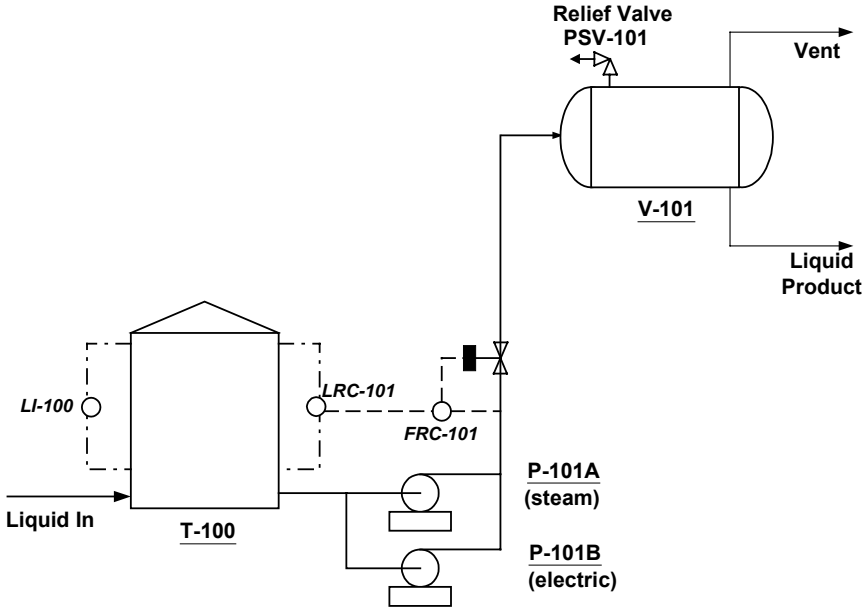
STANDARD WORKED EXAMPLE

In order to illustrate some of the ideas and methods that are discussed in this book, a simple worked, fictional example is provided in this section, and will be referred to at appropriate points in succeeding chapters.

Figure 1-2 shows liquid flowing into an Atmospheric Tank, T-100. From T-100 the liquid is pumped to Pressure Vessel, V-101, using either Pump, P-101A or P-101B (A is normally in service, B is normally on standby). The pumps are driven by a steam turbine and an electric motor, respectively. The liquid being pumped is flammable and toxic. The flow of liquid both into and out of T-100 is continuous. The in-flow varies according to upstream conditions and is not under the control of the operators in this area; the out-flow is controlled by FRC-101, whose set point is cascaded from LRC-101, which measures the level in T-100. The level in T-100 can also be measured manually using the sight glass, LI-100.

V-101 is protected against high pressure by safety instrumentation (not shown) which shuts down P-101 A/B, and by a relief valve, PSV-101.

Figure 1-2
Standard Worked Example



SAFE OPERATING LIMITS

Fundamental to all types of process safety work is the concept of Safe Operating Limits. The facility designers should define a safe operating envelope for all critical process variables. Operation outside that envelope is unsafe by definition, and is therefore not permitted. The PHA team needs to know what the safe limits are in order to have quantitative definitions for the word “safe” and “deviation.”

Unfortunately, the reality is that safe limits are often not known, particularly on older plants, where the original design values may have been lost, or were never provided. Even on new plants, the design team may have provided information on operating targets, but not on safe limits. Indeed, in many situations the only way of finding out the true safety limit is to take plant operations into the unsafe range, which, of course, cannot be done.

If quantified safe limit values are not available, PHAs can develop circular logic on the following lines:

1. Could high temperature cause an accident?
2. What is high temperature?
3. High temperature is that temperature which could cause an accident.

Circularity such as this is the underlying cause of much of the frustration to do with PHAs.

Table 1-1 provides some values for safe upper and lower limits for the Standard Example.

Table 1-1
Examples Of Safe Operating Limits

Item	Para-meter	Units	Safe Upper Limit (SUL)	Safe Lower Limit (SLL)	Comments
T-100	Level	%	95	10	Minimum flow protection for the pumps is not provided, so a minimum level in the tank must be maintained to protect the pumps, and prevent seal leaks.
P-101	Flow	kg/h	3000	500	The maximum flow rate is equivalent to the maximum pumping capacity of P-101 A/B.
V-101	Pressure	barg	12 (MAWP at 250C)	0	Vessel is not vacuum-rated, and there is uncertainty about lower pressure limit, so 0 barg (1 bar abs) has been arbitrarily set as the lower limit.
V-101	Temp-erature	°C	250	-10	Potential for stress cracking at low temperatures.

Some safe limits may have no meaningful value. For example, if a pressure vessel is designed for full vacuum operation, there is no safe lower limit for pressure for that vessel.

Figure 1-3 provides a graphical representation of safe limits. The variable shown could be any process parameter, such as the level in Tank T-100, or pressure in Vessel, V-101.

Figure 1-3
Safe Operating Limits

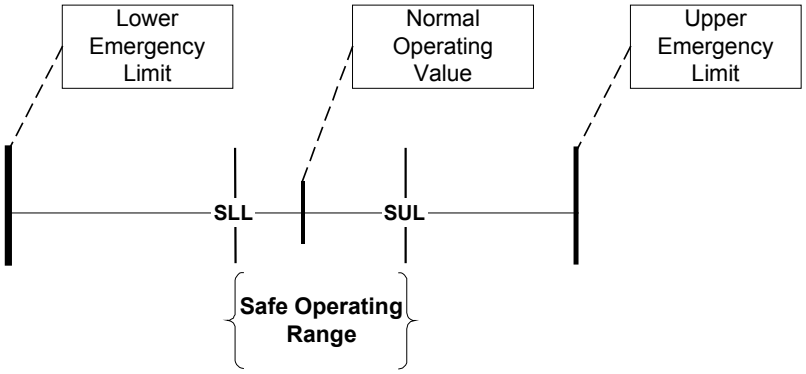


Figure 1-3 shows a Safe Operating Range that lies between the Safe Upper Limit (SUL) and Safe Lower Limit (SLL). The Normal operating value lies inside this Safe Operating Range. As long as the operating value stays within that range, then the process is defined as being safe with respect to this variable. However, if the operating value goes outside the safe range, then the process is, by definition, unsafe.

This means, therefore, that if a variable moves outside the safe range, the operator *must* take action, and/or the instrument logic should be designed to bring it back within the allowable envelope. The option of doing nothing is not an option. Also, if a variable moves outside the safe operating range, safety devices such as relief valves and interlocks will be activated.

In addition to safe limits, many variables will also have associated emergency limits, also illustrated in Figure 1-3. If a

variable value goes outside the emergency limit range, urgent action must be taken.

Maximum Allowable Working Pressure

Although safe limits in general may be difficult to obtain, values for one of the most important parameters, maximum pressures in vessels, are usually available in the form of Maximum Allowable Working Pressure (MAWP,) as defined by the American Society of Mechanical Engineers. Since the purpose of a PHA is to find out how loss of containment can occur, and since loss of containment in many cases indicates that a vessel has been over-pressured, knowledge of MAWP values is critically important.

PHA Team Estimate

If safe operating limits are not available, but the plant has had many years of operating history, the PHA team may help determine those limits using empirical experience. For example, the team may not be provided with the formal safe limit for a reactor temperature. However, if, during the PHA, an experienced operator makes a statement of the following sort, “Once we allowed the temperature in the reactor to rise above 225°C, and we nearly melted the catalyst bed”, a rough working safe limit value of 225°C has been defined. The proposed value of 225°C may be empirical, but it is probably quite accurate. (The actual limit value may be set at say 220°C in order to provide a margin for error).

Unsafe Mixing Scenarios

Serious accidents can result from the mixing of incompatible chemicals. Therefore, the safe limit values should include information on the mixing of the chemicals found in the process under consideration, and what concentrations are allowable. Mixing matrices, such as that shown in Table 1-2, are commonly used to provide this information.

Table 1-2 lists five chemicals: A — E. Information is provided on which chemicals can and cannot be mixed with one another safely.

Table 1-2
Mixing Scenarios

	A	B	C	D	E
A	—				
B	‡	—			
C	√	√	—		
D	X	X	‡	—	
E	N/A	√	√	√	—

The symbols in Table 1-2 have the following meanings:

√	No known problems with the mixing of these two chemicals
‡	Problems in certain mixing ranges
X	Mixing not allowed in any range
N/A	Information not available

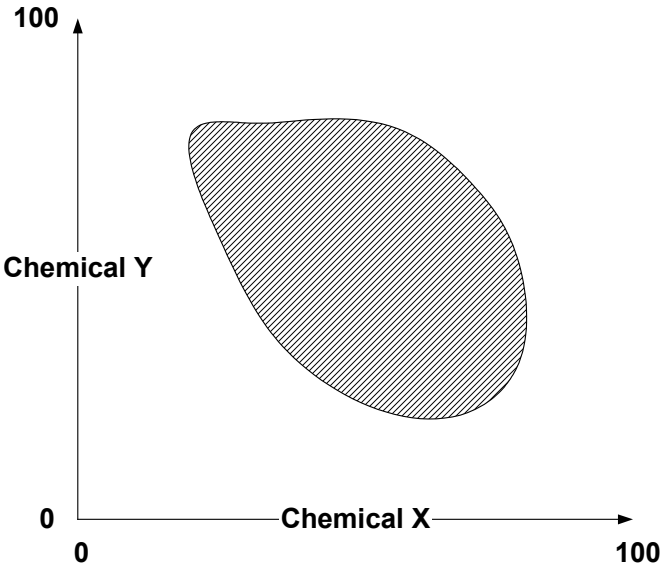
The following limitations generally apply to tables such as this:

- Mixing Tables usually consider only binary mixtures. The consequences of simultaneously mixing three or more materials is not usually known.

- Mixing Tables generally do not provide information on the levels of danger, except maybe as footnotes or marginalia.

- The Mixing Tables may not provide information about dangerous ranges. It could be that two chemicals are safe in one concentration range, and not safe in another range. If sufficient data on safe limits is available, a safe mixing envelope such as that shown in Figure 1-4 can be used. The shaded area represents the predicted unsafe mixing range of the chemicals X and Y at a given temperature.

Figure 1-4
Safe Mixing Envelope for a Given Temperature



Not much publicly available information to do with safe mixing is available. However, some information is available from the United States Coastguard CHRIS database [4].

MATERIALS OF CONSTRUCTION MATRIX

A materials of construction matrix should be part of the PHA documentation, particularly when a range of different chemicals is in use. Table 1-3 shows how various materials of construction can be used for containing chemicals A — E.

Table 1-3
Materials Of Construction Matrix

	Carbon Steel	*Stainless Steel 304*	*Stainless Steel 316*	*Gasket Material A*	*Gasket Material B*
Chem-ical					
A	√	√	√	√	√
B	‡	√	√	X	X
C	‡	N/A	N/A	N/A	N/A
D	X	X	‡	√	√
E	N/A	√	√	√	N/A

In Table 1-3 the symbols have the following meanings:

√ No known problems
‡ Potential problems, further information may be needed
X Not allowed
N/A Information not available

RISK

In normal conversation, the word “risk” tends to be used rather loosely. In formal risk analysis, however, the word has a very specific meaning, and the PHA team leader must be careful to ensure that words such as “risk,” “probability,” and “hazard” are used as precisely and correctly as possible. These terms are described below.

COMPONENTS OF RISK

Risk has three components:

- A hazard
- The consequences of that hazard (safety, environmental, economic)
- The frequency with which the hazard occurs, or is expected to occur.

The three terms are combined as shown in the Equation (1.1).

$$Risk_{hazard} = Consequence * Frequency \quad (1.1)$$

Equation (1.1) states that, the risk associated with a hazard is the product of that hazard's frequency and of its consequences.

SUBJECTIVE NATURE OF RISK

Equation (1.1) puts consequence and frequency on equal footing; it implies a linear trade-off between the two. For example, as mentioned on page 6, a hazard resulting in one fatality every hundred years has the same objective risk value as a hazard resulting in ten fatalities every thousand years. In both cases the fatality rate is 1 in a hundred years, or 0.01 fatalities yr^{-1}.

However, risk is fundamentally a subjective, and, at times, an emotional topic [5]. A PHA team needs to understand the way in which risk is actually perceived, particularly by members of the public, whose knowledge of the process industries is very limited and often inaccurate. Factors affecting the public perception of risk include:

- The degree to which a person has direct control over the risk. For example, someone who finds the presence of a chemical plant in his community unacceptable may willingly go rock-climbing on weekends because he feels that he has some control over the risk associated with the latter activity.

- The familiarity of the consequence term. For example, people understand and accept the possibility of a fatality in a road accident, but may be more worried about the consequences of being exposed to mysterious toxic chemicals.

- People are more willing to accept risk if they are direct recipients of the related benefit, whereas they are less willing to accept the risk of something that merely provides a general benefit to the community.

In general, people find rare, high-consequence accidents less acceptable than more frequent, low consequence accidents. For example, in a typical large American city, between 300 and 500 people die each year in road accidents. Although every effort is made to reduce this fatality rate, the fact remains that this loss of life is perceived as part of functioning in a modern community and so there is little outrage on the part of the public.

However, were an airplane carrying 300 people to crash at that same city's airport every year there would be an outcry. Yet the fatality rate is the same as for highway accidents: 300 deaths per city per year. The difference between the two risks is a perception rooted in emotion. To accommodate this perception difference, Equation (1.1) can be modified so as to take the form of Equation (1.2).

$$Risk_{hazard} = Consequence^{n} * Frequency \quad \text{.....} \quad (1.2)$$
$$\text{where } n > 1$$

Equation (1.2) shows that the consequence term has been raised by the exponent n, where n > 1. In other words, high consequence/low frequency accidents are *perceived* as being more serious than low consequence/high frequency accidents.

Since the variable 'n' represents a subjective feeling, it is impossible to assign to it a firm, defensible value. However, if a value of say 1.5 is given to 'n', then the perceived risk associated with the airplane crash mentioned earlier is 17.3 times greater than for the automobile fatalities. Stated another

way, the 300 airplane fatalities are perceived as being equivalent to over 5000 automobile fatalities.

For those hazards that have very high consequences, such as core meltdown in a nuclear power plant, perceived risk rises very fast due to the exponential term, thus explaining public fear over such facilities. Management has reduced risk by reducing the likelihood of a major accident (often by adding layers of safety instrumentation). However, since the worst-case scenario remains the same, the public remains nervous and antagonistic.

Fixation

Fixation occurs when a person or group of people comprehends just one or two observations (usually made early in the sequence of events,) or in a proposed solution to a problem, thereby unconsciously ignoring other data that might challenge their preconceptions. Fixation can be a serious problem in PHAs, particularly with regard to the more experienced team members whose memories and opinions may limit their ability to think imaginatively.

Some examples of fixation include:

- A plant experiences operating problems over a period of days. Different shifts witness different aspects of the problem, and so come up with different causes and proposed solutions. The people on each shift tend to discount the opinions of the other shifts because “seeing is believing”; people place more credence on their own experience than on the un-witnessed experience of others.

- During an emergency, an operator is typically swamped with a large amount of information, much of which is confusing or apparently self-contradictory, particularly if one or two instruments are in error. In such situations, most people tend to fixate on one or two factors, and then exclude all other information, regardless of its relevance. (Fixation was an important part of the Three Mile Island nuclear power plant incident, where operations personnel chose to believe a

faulty instrument, even though many other instruments were indicating that the signal from the first instrument was faulty.)

- People sometimes extrapolate from a small number of bad experiences. For example, if a particular supervisor has had two or three bad readings from the production lab, he may be inclined to generalize that "You can never trust the results from our lab," even though such an opinion really cannot be justified objectively.

- During discussions people tend to take up a particular point of view, and then defend it, even when proven wrong. They develop pride of ownership in their opinions.

Experience of Events

When PHA team members are discussing the anticipated frequency of an event (*see* page 27,) their experience of similar events is likely to have a major impact on their judgment. In particular, if a plant has had a serious accident, the team members are much more willing to assign a high frequency value to other, similar potential accidents than if such an accident has never actually occurred.

As already noted, one of the most important roles for a team leader is to break the "It's never happened here, therefore it's not going to happen" paradigm. An excellent way of doing this is to explain and discuss accidents that other companies have had, and to show that such accidents can reasonably occur on the facility being analyzed. Some professional societies, such as the Center for Chemical Process Safety provide case studies and "lessons learned" — sometimes illustrated with photographs. The Chemical Safety Board's summary of recent events is also a useful reference. [6, 7]

Quantifying Risk

A risk analysis should be quantified wherever possible for the following reasons:

- Quantification helps get around the fixation problems discussed above, as well as the general “I think / You think” difficulties that tend to occur in qualitative work.

- Quantification of safe limit values helps prevent circular discussions of the type described on page 11.

- A quantified analysis provides a rational basis for determining the allocation of resources for corrective action.

- Quantification can help the PHA leader challenge the person who has considerable experience and who may be over-confident (and incorrect) in his or her opinions.

Probably the most common means of quantifying risk in the process industries is through the use of Fault Trees, described in Chapter 6.

In practice, most PHAs use a semi-quantitative approach. Generally, a full quantitative analysis is impractical because it takes too long, and much of the basic data is either missing or of low quality. Most PHA teams use risk matrices, as discussed in the next section.

RISK MATRICES

The risk matrix approach is comprised of three separate matrices. For each hazard, the following matrices are used:

- Consequence Matrix
- Frequency Matrix
- Risk Matrix

CONSEQUENCE MATRIX

The first risk term to be considered is the consequence associated with a given hazard.

Fires And Explosions

The topic of fire analysis and control is covered by a wide range of standards from bodies such as the National Fire Protection Agency (www.nfpa.org). If management wants the PHA to consider the impact of fire in detail, a Fire Protection engineer should be part of the team.

The calculation of explosion effects is a complex topic involving many variables. The United States Environmental Protection Agency (EPA) provides lookup tables and simple equations for some of the commoner chemicals to calculate the distance of the overpressure waves [8]. Some practitioners believe that the EPA tables are conservative, *i.e.,* they predict greater impact than would be likely to actually occur. Nevertheless, they do provide a useful starting point.

As an example of the EPA method, Equation (1.3) shows the overpressure equation for propane.

$$D = 0.0081 * (0.1 * W * (46{,}3333/4680))^{1/3} \quad \text{..... (1.3)}$$

Where D is the distance in miles that a 1 psi over-pressure wave (which has sufficient force to knock down non-reinforced buildings) can be expected to travel, and W is the weight in pounds of propane involved (see the EPA reference for an explanation of the other terms). Therefore, for example, if the inventory of propane in a tank is 50,000 lb and 10% of it is involved in an explosion, the 1 psi overpressure wave would extend for 0.3 miles.

Gas Releases

If a facility releases a toxic or flammable gas it is important to know how far the plume will travel, what the concentration gradient within the plume will be, and what impact various concentrations of gas are likely to have on human health.

The effect of a release depends on a plethora of factors such as the density of the gas, the amount released, weather conditions

at the time of the release, and the roughness of the ground surface. As with explosion analysis, the modeling of gas releases is a complex subject that lies beyond the scope of this book.

Representative Consequence Matrix

A representative consequence matrix is shown in Figure 1-5, which identifies four consequence categories: worker safety, public safety, environmental impact, and economic loss; each of these is divided into four levels of seriousness. There are no rules as to how many levels should be selected, nor does any major regulatory body insist on a particular size of matrix. However, many companies choose four levels; three levels does not provide sufficient flexibility and differentiation, but five levels imply a level of accuracy that is probably not justified — estimates of hazard consequences are usually very approximate.

Figure 1-5 also provides some examples of the values assigned to each level of consequence for each category. Once more, there are no rules regarding these levels; each company will select values that are most appropriate for its own circumstances.

Figure 1-5
Consequence Categories

	Worker Safety	**Public Safety**	**Environ-Ment**	**Economic** (Equipment and Product Loss)
Low 1	Report-able or equivalent	None	None	$10K[b] to $100K
Mod-erate 2	Hospit-alization or lost-time injury	Minor Medical Attention	Report to Agencies	$100K to/ $1 Million
Severe 3	Single disabling injury	Hospit-alization or serious injury	Remediation Required	$1 Million to $10 Million
Very Severe 4	Fatality or multiple serious injuries	Fatality or multiple serious injuries	Business Threatening	>=$10 Million

Worker Safety

The first of the consequence columns — Worker Safety — is the most important for most PHA teams. Indeed, many teams will elect to consider this item only, which is why it has been shaded in Figure 1-5. If the workers are safe, then the other factors probably fall into place.

Public Safety

It is exceedingly rare for even the most serious accidents to result in a member of the public being directly injured. However, in the event that someone is hurt due to shrapnel or other flying objects, or by the effects of a toxic vapor cloud crossing the plant boundary, the categories shown in the third column in

[b] The letter 'K' stands for a thousand. So, $10K is $10,000.

Figure 1-5 can be used. This column is basically the same as for worker safety, except that each level is rated one degree higher. This is why there is no “Low Consequence” category when applied to public safety. If a member of the public is hurt, even slightly, then that incident automatically has at least a “Moderate” consequence.

Environment

Generally, PHAs do not consider environmental issues directly. Most companies have dedicated specialists to take care of this topic, along with the associated regulations. PHAs can, however, help the environmental specialists to understand how releases may occur and how such releases can be mitigated.

Economic

The final category of consequence is Economic. All process incidents generate losses in one or more of the following areas:

- Damaged or destroyed equipment
- Lost production
- Off-quality product
- Litigation
- Clean-Up

The difficulty with using the ‘Economic Loss’ column in a risk-ranking matrix is that it seems to assign a financial value to human life and suffering. For example, Figure 1-5 suggests that a disabling injury is “worth” from $1 to $10 million. Since such statements can be controversial and almost impossible to defend, it is often best if purely economic issues arising from the PHA are handled separately from the safety and environmental findings. For example, a special risk ranking of ‘O’ — standing for ‘Operational Loss’ — can be used (*see* page 31). This allows management to handle findings in this category to be handled separately from the formal PHA findings.

FREQUENCY MATRIX

Once the PHA team members have ranked the predicted consequences of an identified hazard, they should then provide some estimate as to the frequency with which the hazard may occur.

A representative frequency matrix is shown in Figure 1-6. Once more, four value levels are provided. As with consequence values, three levels is probably too coarse, but five levels or more implies accuracy that probably cannot be justified.

Figure 1-6
Frequency Levels Matrix

	Frequency	Comments
Low	< 1 in 1000 years	Essentially impossible
Medium	1 in 100 years to 1 in 1000 years	Conceivable — has never happened in the facility being analyzed, but has probably occurred in a similar plant somewhere else.
High	1 in 10 years to 1 in 100 years	Might happen in a career.
Very High	> 1 in 10 years	It is likely that the event has occurred at the site if the facility is more than a few years old.

In practice, the important split occurs between “High” and “Medium” frequency. When an existing plant is being analyzed, long-term employees will have witnessed “Very High” frequency events, and may have observed events rated “High.” However, events rated “Medium” and “Low” have probably never been

witnessed at that site, so the leader will have to stimulate creative thinking and overcome the unwillingness to accept that such events can occur.

One way of helping people visualize low frequency events is to examine the overall industry record. For example, if a certain event has an estimated frequency of 1 in a 100 years, it is not likely that anyone on the plant will have witnessed that event. However, if there are 100 similar plants world-wide, then that event should be occurring about once a year somewhere in the world. (The usefulness of sharing information around an industry segment is recognized by various companies, such as those that manufacture ammonia.)

Frequency, Probability, Likelihood

The words frequency, probability and likelihood tend to be used interchangeably, yet, strictly speaking, they are different, and a risk professional should use them correctly.

Frequency is a *rate* term, and has units of inverse time, or time^{-1}. For example, a PHA team may determine that the *estimated frequency* of reverse flow from V-101 to T-100 in the Standard Example is once in ten years, or 0.1 yr^{-1}.

Probability, unlike frequency, is dimensionless, meaning that it has no units. Most safeguards are assigned a probability value. For example, if a check valve is installed in the line between T-100 and V-101, it will have an estimated probability of stopping reverse flow of say 98% (which means that it is expected to fail one time in 50). If linked to the frequency rate term, the frequency of reverse flow with the check valve included is 0.1 * 0.02, or 0.002 yr^{-1}. In other words, reverse flow in this case can be expected to occur once in 500 years.

The above example shows that frequency and probability terms are often used together (making up the AND Gate of a Fault Tree, as discussed in Chapter 6). The frequency value is applied to the predicted failure rate of a piece of equipment. For example, a vessel may overpressure once in ten years, thus

having a high pressure frequency of 0.1 yr^{-1}. If the relief valve on the vessel has a probability of failure on demand of one in 50 times, or 0.02, then the predicted failure rate for the system is 0.002 yr^{-1}, or once in 500 years.

Likelihood is a term that can be applied to either frequency or probability.

Safeguards

The team must decide how to handle safeguards when estimating frequency. In the above example, the safeguard (the check valve) is included in the overall frequency term for system failure caused by reverse flow. In other words credit, is taken for the protection that the check valve provides. However, some teams consider only the frequency of occurrence of the event itself, assuming that safeguards either do not exist, or that they do not work.

Further discussion on the topic of safeguards is provided on page 37.

Risk Matrix

Having determined Consequence and Frequency values, the overall risk associated with the hazard is determined using a third matrix, such as that shown in Figure 1-7, which shows four levels of risk.

Figure 1-7
Risk Ranking Matrix

		Consequence			
		Low	Mod-erate	Severe	Very Severe
Frequency	Low	D	D	C	B
	Medium	D	C	B	B
	High	C	B	B	A
	Very High	B	B	A	A

A — Requires prompt action: money is no object, and the option of doing nothing is not an option. An 'A' risk is urgent. If the A-level risk represents an emergency situation, management must implement Immediate Temporary Controls (ITC) while longer-term solutions are being investigated.

B — Risk must be reduced, but there is time to conduct more detailed analyses and investigations. Remediation is expected within say 90 days. If the resolution is expected to take longer than this, then an Immediate Temporary Control must be put in place to reduce the risk.

C — The risk is significant. However, cost considerations can be factored into the final action taken, as can normal scheduling constraints, such as the availability of spare parts or the timing of plant turnarounds. Resolution of the finding must occur within say 18 months.

D — Requires action, but is of low importance.

The decisions as to what values to assign the different letters, and which letters go in which boxes vary according to the company, the technology being used, and past experience of incidents. The following are some guidelines:

- The risk values will usually line up diagonally, as shown in Figure 1-7; all the values in any one diagonal are the same.

- An ‘A’ level risk is so serious that a normal PHA should not uncover such events. A risk so serious and so obvious should already have been identified and corrected. An ‘A’ risk implies an emergency situation, possibly including the immediate shut down of an operating facility or a major re-design of one that is currently being engineered.

- Frequently, the dividing line between ‘B’ and ‘C’ is that B-level risks must be addressed promptly, whereas C-level risks can be scheduled for the next turnaround (on a continuously operating plant,) or as a routine maintenance event.

- If the PHA is generating a large number of ‘D’ level risks, the team may be spending too much time on occupational safety issues (*see* page 40).

- No matter how low a risk value may be, management must eventually take action to address the identified hazard. Even ‘D’ level risks must be resolved and recommendations implemented according to a schedule.

Other useful risk terms include:

O — *Operational*. Sometimes the risk associated with a hazard is purely economic; it has neither safety nor environmental implications. Use of the letter ‘O’ tells management that they do not have to respond to this finding for safety reasons, but they may choose to do so simply to increase profits. Use of this term also means that the team will probably not use the economic consequence column in Figure 1-5. Instead all economic findings will be placed in the ‘O’ category.

S — *Standards*. Some risks represent a violation of industry consensus standards, code or company policy. It is difficult to assign frequency and consequence values to many of these hazards, but professional practice suggests that something should be done (and if the issue is a code violation, then something must be done). One option is to arbitrarily assign a B-level risk to code violations, and a C-level risk to non-conformance to consensus standards, but judgment has to be used in all cases.

L — *Low Hanging Fruit.* This term is obviously written tongue-in-cheek, yet many times it is unnecessary to dwell on the development of recommendations; what needs to be done is simple, straightforward, effective, cheap and non-controversial. In such cases, there is little point in conducting a risk assessment — it is better simply to fix them. The following are examples of this type of recommendation:

- If an operating procedure is not up to date, it is better just to rewrite it rather than worrying about the risk associated with use of the present procedure.

- If a certain safety sign is unreadable, just replace or repaint it.

Although problems such as these can be addressed right away, the team may consider the management implications of why these minor problems existed in the first place. If the procedure was improperly formatted, does this indicate a structural problem with the procedures-writing system? Does an illegible safety sign indicate deeper problems regarding occupational safety or with housekeeping?

Human Presence Contingency

When calculating risk, it is important to consider how often someone may be present at the incident site. For example, the seal of P-101 in the Standard Example may leak once every two

years (“Very High” frequency). IF someone is present, THEN the leaking material could seriously hurt them (“Severe” in Figure 1-5,) hence the risk of this event is a ‘A’ (Figure 1-7). However, if a person is present at the release site say only 1% of the time, then the predicted frequency of the event and its associated consequence drops to “High”, and the risk level falls to ‘B’.

The presence of humans in an area automatically raises the level of risk. Consequently, one of the best ways of improving safety is simply to remove people from the site of potential releases —“If a person’s not there, he can’t be killed.” This line of reasoning provides a strong argument for increased automation, for moving human beings away from the immediate work site, and into a remote, blast-proof control room.

Unfortunately, a large number of maintenance workers are often present at the time of a release because they are working on what was perceived to be a minor problem. During the course of the work the situation becomes catastrophic with the maintenance people being directly in the line of fire.

Example

Table 1-4, which is based on the Standard Example on page 10, provides some examples of the hazards that may be identified by a PHA, along with the associated estimated consequence, frequency, and risk-ranking values. (Other information, such as causes of the hazards, has been omitted from this Table).

Table 1-4
Examples Of Risk Determination

Hazard	Conse-quence	Frequ-ency yr^{-1}	Risk	Discussion
T-100 overflows (1)	Worker injury **"Moderate"**	0.025 (once in 40 years) **"High"**	**B**	Frequency based on one observed spill in 20 years, and 50/50 chance of worker being present.
T-100 overflows (2)	Environ-mental spill requiring remediation **"Severe"**	0.0005 (once in 2000 years) **"Low"**	**C**	Frequency based on one spill in 20 years, with containment that has a 0.01 probability of failing.
Pump, P-101 A/B, seal failure	Disabling worker injury **"Severe"**	0.25 (once in 4 years) **"Very High"**	**A**	Seals fail once every two years, operator present one in two times. Requires an Immediate Temporary Control (ITC).

Hazard	Conse-quence	Frequ-ency yr^{-1}	Risk	Discussion
PSV-101 may not meet new code (ASME)	—	—	**S**	There are no signs of either pressure setting or capacity problems to do with this relief valve, but it is old and may not conform to current requirements.
P-101 A/B, impeller corrosion	Operational consequences only.		**O**	Each incident costs $20,000 in repair costs and lost production.

HAZARD IDENTIFICATION

Many techniques for identifying hazards are available. They all use one or more of the following approaches.

- Creative Thinking
- Extrapolation of Experience
- Formal Analysis Using Boolean Algebra (and possibly Monte Carlo simulation)

CREATIVE THINKING

An effective PHA will encourage the team members to identify low frequency/high consequence hazards that have never been seen in the field. The team members should be encouraged to

think of hazard scenarios that would fall in the “Low” or “Medium” categories in Figure 1-6, the Frequency Matrix.

Getting the team to think in this manner is one of the leader’s biggest challenges. First, he or she has to overcome the “I’ve never seen it happen, therefore it can’t happen” syndrome already discussed. Second, low probability scenarios usually involve the simultaneous occurrence of contingent events (which is why the predicted frequency of such events is low). Once more, team members typically have trouble accepting and understanding unlikely combinations of events. To help overcome this block, the leader may choose to describe a number of real accidents that occurred elsewhere to show how “weird” they were — yet they happened.

Checklists And Standards

All PHAs draw heavily on the experience and knowledge of the team members who provide invaluable information as to the types of incident, how likely their occurrence may be, and the effectiveness of safeguards. This experience is the foundation of the Checklist and FMEA methods described in Chapter 5. Typically, checklists are developed for equipment items such as pumps, pressure vessels, valves, and tanks. Checklists can also be created from standards such as regulations, codes, and company policies.

Formal Logic Analysis

A final approach to hazard analysis is the use of stochastic modeling techniques, usually based on Boolean algebra. The use of these techniques helps clarify the logic as to how accidents may occur, and also provides a foundation for the quantification or risk. The Boolean method of Fault Tree Analysis is described in Chapter 6.

SAFEGUARDS

A PHA team should be clear about its use of the term "safeguard." The discussion below provides some guidelines on this topic.

DEFINING A SAFEGUARD

A safeguard is an item whose only purpose is to enhance safety. Any device used during normal operation is not a safeguard; nor is a post-accident mitigation system.

The following examples expand on the above definition.

- A pressure relief valve is a safeguard against high pressure because it ensures that the pressure in a vessel does not exceed the safe upper limit. However, neither normal pressure controllers nor operating relief valves are safeguards. (Strictly speaking it could be argued that a relief valve is not a safeguard since it is only used when a Safe Upper Limit for pressure has been exceeded. Hence the relief valve does not ensure safety — it merely mitigates the impact of an already unsafe operation).

- Special procedures and training in how to handle a particular high-hazard scenario could be regarded as safeguards. However, normal plant training in the handling of upsets is not a safeguard.

- Post-accident safety systems such as the use of firefighting equipment or the Emergency Response Team do not qualify as safeguards because they come into use after the event has occurred, when the plant is already in an unsafe condition.

- Generally check valves are a weak safeguard. “If you rely on a check valve to be safe, then you’re probably not safe.” (*See* page 137 for further discussion on the use of check valves).

- Safeguards can be either active or passive. An active safeguard would be a device such as an interlock or relief valve that responds to an unsafe condition. A passive safeguard would be a device such as an overflow drain on a tank or secondary containment around the tank — no action is required to make it to work. Generally, passive safeguards offer better protection because they are more reliable.

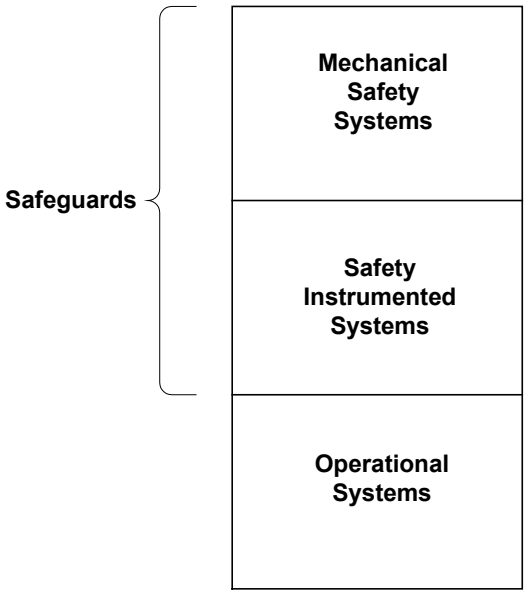
- Personal Protective Equipment (PPE) is not a safeguard because the unsafe condition has already occurred, and even when wearing PPE, an employee is likely to be affected in the event of a major chemical release or fire.

Safeguards can themselves create a hazard, although usually much less serious than the one that they are protecting against. For example, a relief valve that discharges to atmosphere protects against vessel rupture, but it may also may lead to an employee being affected by the fumes, or to an environmental complaint if the discharge has to be flared off.

LEVELS OF PROTECTION

Figure 1-8 shows three levels of protection for handling deviations from the safe operating limits.

Figure 1-8
Levels Of Protection



Operational Systems

At the lowest level, Figure 1-7 shows that a deviation is handled by Operating Systems such as normal control loops and operator intervention. Since such systems are part of the normal operation, they are not really safeguards — even though they effectively handle the overwhelming majority of potential safety deviations.

Safety Instrumented Systems

Increasingly, companies are installing dedicated Safety Instrumented Systems (SIS) whose only purpose is to bring the plant into a safe state in the event of a serious upset. Hence, such systems are true safeguards — they take action before an unsafe condition is reached. SIS systems are discussed on page 282.

Mechanical Safety Systems

Mechanical safety systems such as relief valves and rupture disks are usually the last line of defense in an out-of-control situation, and therefore should never actually be required to operate.

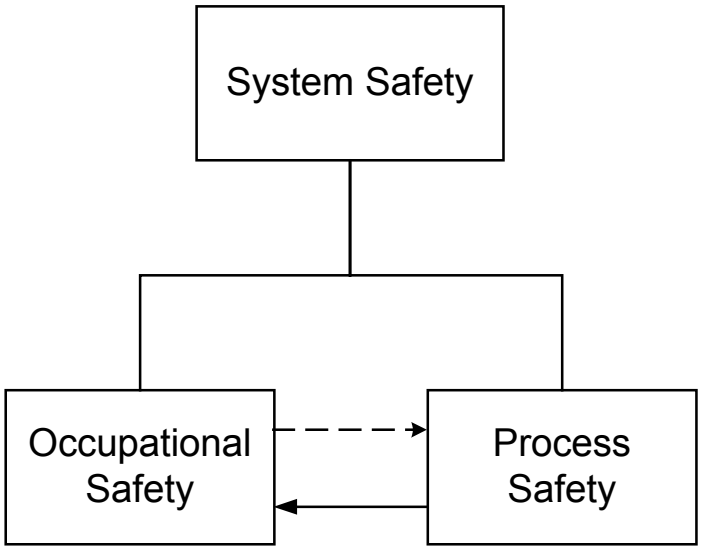
OCCUPATIONAL SAFETY

The purpose of a *Process* Hazards Analysis is to find hazards associated with the *process* being analyzed. Occupational safety, on the other hand, is more concerned with "normal" safety topics such as lock-out/tag-out, protective clothing, and safe access to equipment.

It is suggested here that the two topics are distinct from one another, as illustrated in Figure 1-9. Occupational Safety and Process Safety are both part of overall System Safety, but they are separate and distinct from one another. Indeed, during the follow-up to serious process-related accidents, it is often observed that the facility in question had a good occupational safety record, which is one reason senior managers are often so stunned after a major incident — their good Occupational Safety record had led them to believe that all was well.

For these reasons, the line from Occupational Safety to Process Safety in Figure 1-9 is not solid, indicating a weak link. On the other hand, a facility with a good Process Safety program probably will do well at Occupational Safety, so that line is shown as solid, indicating a stronger link.

Figure 1-9
System Safety



Occupational Safety tends to focus on people issues such as their behavior and willingness to take risks. *Process Safety*, on the other hand, focuses on processes themselves, and on the ways in which operators and maintenance personnel interact with those processes.

Although the focus of a PHA is on Process Safety issues, it is likely that the team will uncover some Occupational Safety items, such as problems with safe access to equipment or instruments. These items should be noted in the PHA report and communicated separately to the safety manager or whoever is responsible for such matters.

PHA TECHNIQUES

An overview of the key PHA methodologies is provided in the list provided below. Greater detail is provided in the succeeding chapters. The list of techniques listed below is taken directly from the OSHA PSM regulation (page 240).

- Hazard And Operability Method (HAZOP)
- What-If
- Checklist
- What-If / Checklist
- Failure Modes and Effects Analysis (FMEA)
- Fault Tree Analysis
- Other Appropriate Methods (such as Monte Carlo Analysis)

No one of these methods is inherently any better than any of the others. They all have their place, and are often used in combination with one another. For example, a team that has started an analysis with the HAZOP method (generally the most rigorous and time-consuming) may gradually switch to the What-If technique, particularly if it is found that many of the scenarios being discussed toward the end of the PHA resemble those that were discussed in depth at the start of the analysis.

The differences between the various PHA methods are not as great as might appear at first, particularly when the PHA team is very experienced. For example, if the team is using one of the less-structured methods, such as What-If or Checklist, often the team members will almost reflexively start using the systematic HAZOP guidewords. Similarly, an engineer analyzing an equipment item with an FMEA may draw up a fault tree to help him understand how the equipment parts interact with one another.

Moreover, the methods often complement one another, particularly on a new project, when a series of PHAs of increasing depth, complexity and rigor can be performed as the plant design matures.

HAZARD AND OPERABILITY METHOD (HAZOP)

Being the most systematic and thorough type of PHA, the HAZOP technique is sometimes used simply to ensure maximum compliance with regulations, even though it may not be the best technical choice, and even though one of the other methods can be just as effective at finding the hazards in a

particular situation. Frequently, a company's legal advisors recommend use of the HAZOP method because of its completeness and because of its acceptance by regulatory agencies.

The HAZOP method is discussed in detail in Chapter 3.

What-If Method

The What-If [c] method is the least structured of the creative PHA techniques. Its use requires a team composed of experienced analysts capable of identifying incident scenarios based on their experience and knowledge. This method is often used for Conceptual PHAs, where very little detail is available concerning the process or the equipment because the plant is still being designed.

The What-If method allows the team to quickly focus on issues that are critical, and obviates the danger of wasting large amounts of time discussing guidewords that generate little or no significant insight. The speed of a What-If analysis also helps reduce the boredom of PHA meetings, a common problem with the more formal methods, such as HAZOP. What-If analyses are also good at analyzing global issues, such as loss of utilities or the impact of a major fire.

Due to its lack of structure, the success of a What-If analysis is highly dependent on the knowledge, creativity, experience and attitudes of the individual team members; the method does not structure a discussion in the way that HAZOP does. The What-If method also poses the greatest challenge to the team leader since he or she has little structure with which to work.

Because relatively little prompting will be provided by guidewords or line-by-line analysis, it is vital that the team

[c] The phrase "What-If" is spelled here in the same way as it is printed in the OSHA regulation. It is hyphenated and the question mark is omitted unless the term is used at the start of direct question.

members prepare very thoroughly before the team analysis commences; the free-ranging nature of the discussion will require that everyone be up to speed on the process and its general hazards before meetings start.

The What-If analysis itself is usually organized around sections of the P&ID, typically major equipment items, or operating systems (such as the condensing system of a distillation tower). Team members ask questions such as:

- "What-If there is high pressure in the tower?"
- "What-If the operator forgets to open the drain valve?"
- "What-If there is an external fire in this area?"

Details on the use of the What-If method are provided in Chapter 4.

CHECKLISTS

The Checklist Method uses a set of pre-written questions to stimulate discussion and thinking. The questions are developed prior to the PHA by experts who have conducted many PHAs and other similar analyses, and by experts in the process being reviewed. Checklists are not comprehensive — no PHA method can make that claim. Nevertheless, the list of questions should be long enough to ensure that no obvious issues are overlooked.

The use of Checklists is discussed in Chapter 5.

WHAT-IF / CHECKLIST METHOD

The What-If/Checklist approach combines the two methods just discussed. In effect, it encourages a team to think creatively, using a Checklist to provide structure to the discussion.

Failure Modes & Effects Analysis (FMEA)

Failure Modes and Effects Analysis (FMEA) is a technique for determining the ways in which equipment items and their internal components can fail, and what the consequences of such failures would be on the overall system reliability and safety.

Traditionally, the FMEA method has been used primarily in the aerospace and nuclear power industries, but not so much by the process industries because single equipment failures do not usually have catastrophic results.

More detail on the FMEA method is provided in Chapter 5.

Fault Tree Analysis

A Fault Tree is a logic diagram that shows the combination of events that have to take place before an accident can occur. Fault Trees are normally used to analyze systems rather than to creatively identify hazards, although the Qualitative Fault Tree method discussed on page 199 can provide a fresh approach to hazards identification.

The Fault Tree method differs from the other PHA techniques discussed to this point in that its application is often more suited for a single individual rather than a team. Teams have trouble discussing situations involving multiple contingent events.

Fault Tree Analysis is discussed in detail in Chapter 6.

Other Appropriate Methods

Other methods of identifying hazards can be used (and, for those companies operating in the United States, are accepted by OSHA). For example, some companies use what is referred to as an “experience-based HAZOP” which combines elements of the HAZOP technique described above with the checklist approach.

Another technique, the Focused What-If, is discussed by Goodman. [9]

Many companies are interested in using “Other Appropriate” methods as a means of generating fresh insights into what could go wrong. Some thoughts on second-generation PHAs are provided in the final chapter.

MAJOR HAZARDS SCREENING

If an existing facility is large, and PHAs are being carried out for the first time, management has to decide the order in which the PHAs are to be carried out. Generally these decisions are made through the use of a Major Hazards Screening Analysis (sometimes referred to as a Preliminary Hazards Analysis); those areas with the highest consequence (not risk) are handled first. The frequency with which such incidents may occur tends to be handled rather qualitatively at this stage of the PHA process.

The Major Hazards Screening should be conducted by individuals with a high level of experience both in the way processes operate and in hazard identification. Generally, they will use a checklist method, focusing on the following areas:

- The hazards associated with raw materials, feedstocks, catalysts, intermediates, and final products.
- Equipment used, particularly high-speed rotating items, vessels and piping subject to corrosion, and equipment operating at high pressures and temperatures.
- Layout of equipment, and ancillary services, such as fire fighting systems.
- Operations, including procedures and training.
- Maintenance, including procedures and training.

DESIGN PHAs

Because many companies, particularly in the United States. had to play catch-up following the introduction of regulations in the 1990s, most PHAs have been conducted on facilities that are already in operation. However, the original purpose of PHAs was to analyze plants in either the design or the engineering phase, and now that the regulatory catch-up phase is largely complete, it is reasonable to assume that PHAs will be used increasingly in their original role.

A PHA for a yet-to-be-built plant differs from a PHA for a plant that is already operating in five important ways:

1. Such a plant has no direct operating experience to draw on, particularly if the basic technology is new. However, if the facility being designed and built is similar to others already in service, then the PHA team should be able to find operations and maintenance personnel for other, similar plants who can provide the requisite knowledge and working experience.

2. When the facility is in the design stage, it is quite easy to make sweeping changes such as adding or removing equipment items. However, once a facility is built, even quite small changes can be very expensive, and implementation could lead to serious downtime.

3. Because the plant is not yet operating the leader is less likely to run into problems with “thinking the unthinkable” that have been discussed in earlier chapters.

4. In general, newer facilities will have more complex and sophisticated control logic, which exacerbate the difficulties associated with analyzing such schemes.

5. If the process being built uses brand new technology, then the team will probably have to delve into basic chemistry and design intent more thoroughly than is normal. Generally, the full time presence of a chemist is not required on a PHA, unless the process technology is new.

LEADING A DESIGN PHA

The PHA team leader will often find that leading a PHA for a new facility is more difficult than for an existing facility for the following reasons:

1. Teams are often quite large, since many groups are actively involved in the design and construction of the plant.

2. During the design analyses, team members may bring to the table many agendas and disputes, some hidden and others open. The leader's job is to make sure that these agendas do not get in the way of finding high-risk hazards.

3. If the contract is fixed price, the client may want to "pile on" during the PHA, whereas the design company will want to get the PHA completed as quickly as possible, with a minimal number of design changes. On the other hand, if the contract is cost-plus, the design company will be glad to add changes to the scope of work, since such changes are often high margin mark-up items.

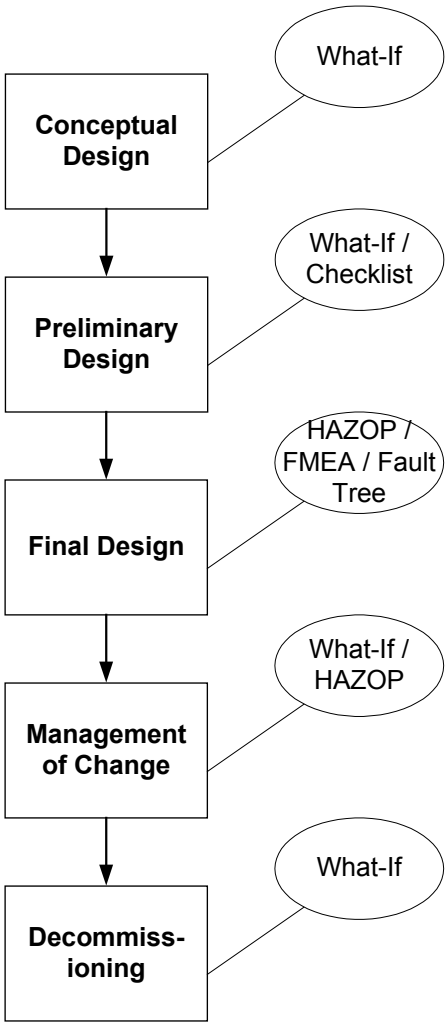
4. Problems to do with hurting the feelings of the design engineers can be an issue, since the designers are likely to be part of the PHA team. (This is not usually the case with operating plants because the design team will have moved on to other projects.)

SEQUENCE OF PHAS

When a new process is being designed and constructed, it is normal for different types of PHA to be performed at each stage of the design. The method selected will reflect the increasing amount of engineering data that is available. Figure 1-10 provides some guidance as to which method can be used at

which stage in the process. The team will decide on the method that best fits its own particular needs.

Figure 1-10
PHA Sequence



CONCEPTUAL DESIGN

A Conceptual Design PHA provides a preliminary safety analysis at the time that the basic process or plant design is still being developed (which means that proposed changes may not cost much to implement). For example, one company had developed a new process that was very profitable but used large quantities of a very hazardous chemical as an intermediate. The chemical had almost no odor, making it difficult to detect in the event of a an accidental release. Furthermore, a second chemical in the process had a very pungent odor which effectively masked the first chemical. Only when a reliable instrument “sniffer” was developed that could detect the toxic gas in low concentrations in all plausible locations did senior management give the go-ahead to commercialize the process.

A conceptual PHA provides an excellent opportunity for eliminating hazards entirely and for making fundamental changes to the process to achieve an Inherently Safer Design. For example, a hazardous catalyst may be replaced with one that is more benign. Or it may be found that some equipment can be entirely eliminated, thus reducing that particular risk to zero. To paraphrase Trevor Kletz, “If it’s not there, it can’t leak.”

Even if a hazard cannot be totally eliminated, the conceptual PHA can encourage the design engineers to select lower temperatures and pressures so as to reduce the worst-case scenarios. Conceptual PHAs may also identify critical missing information, such as flammability information or the consequences of mixing certain process chemicals.

At this stage in the design no detailed engineering documentation exists. Therefore the use of those methods such as HAZOP that require completed P&IDs is not appropriate. Nor is a checklist approach likely to be of much benefit because there is no plant experience on which to draw, and much of the equipment detail will not be known. Hence the What-If method is probably the best method for this phase of the PHA because it is good at encouraging conceptual and creative thinking.

Preliminary Design

Once the basic process design is complete, a Preliminary Design PHA can be conducted. The available documentation will generally be limited to block flow diagrams, preliminary Process Flow Diagrams (PFDs) and Material Flow Diagrams (which also provide information on materials of construction). Once more, the What-If method works well at this stage because opportunities to make major changes in the process design remain and to reduce inventories of hazardous chemicals. The What-If/Checklist method is also a good choice at this stage. The What-If approach encourages broad-range thinking, while the Checklist questions provide a framework on which to base the analysis.

Final Design

At the conclusion of the final design, a complete set of P&IDs will have been published. Other documentation available to the PHA team will include electrical loop drawings, MSDS, and draft operating manuals. The final design PHA is usually a full HAZOP involving many people. This approach is thorough, and should not be performed until the P&IDs are finalized. If a problem arises within the facility after it is built, it is the Final Design PHA that will be used as evidence that the company carried out a proper PHA.

Prestartup Safety Review

The last process safety evaluation to be carried out before the start-up of a new or modified facility is the Prestartup Safety Review, or PSSR. A PSSR is not a PHA — instead it serves to ensure that the plant was constructed as required by the original design and that all required changes (including those stemming from the PHA) have either been implemented or meet the original design intent. PSSRs, and their link to PHAs, are discussed in more detail on page 272.

MANAGEMENT OF CHANGE

Any significant proposed change to a plant that is already running, or whose design has been finalized, should be analyzed with a PHA as part of the Management of Change process (*see* page 273). A What-If or a brief HAZOP is a good choice for the PHA.

DECOMMISSIONING / DEMOLITION

When a plant is decommissioned, it has two possible fates. The first is that it will be simply mothballed in the hope that it can be renovated and restarted at some unspecified time in the future when economic conditions call for such action. The second possibility is that the plant will be torn down and the site used for something else. In either case, a PHA should be performed, with the What-If technique probably being the preferred method. In the case of the plant that is being mothballed, the analysis will include items such as the following:

- Ensure that rotating equipment is turned through half a revolution on a regular basis.
- Check for leaks into and around equipment.
- Check electrical and instrument systems for integrity.
- Check all pollution containment systems for leaks.

If the plant is to be demolished, the checklist will focus on due diligence items such as:

- Hidden pockets of hazardous chemical in the equipment and piping — particularly corrosive materials trapped in the steel at the base of storage tanks.
- Contaminated soil.
- Hazardous construction materials such as asbestos insulation.

One issue to keep note of when decommissioning a plant is that, once the threshold quantities of hazardous chemicals are below

the prescribed limits, the facility is no longer covered by the pertinent process safety standards.

Insurance PHA

Occasionally a PHA team will analyze a process for insurance purposes. If there has been a serious accident resulting in extensive equipment damage, and a plant has to be rebuilt, it is highly unlikely that the replacement plant will be exactly the same as the plant that was destroyed, for two reasons. First, if the plant was more than a few years old initially, it is likely that the rebuilt unit will have to meet newer and more stringent environmental and safety regulations. No longer can a grand fathering be used. Second, it is virtually certain that management will want the new plant to incorporate new features (such as the latest DCS) that simply improve the plant's economic performance.

The insurance company that is paying for the rebuild is likely to accept that it should pay for regulatory upgrades, but not for technology upgrades. In order to determine which of the plant changes are optional, management may choose to commission a PHA team to examine a true rebuild of the original plant, to determine which upgrades are necessary and which are optional.

STRENGTHS AND LIMITATIONS OF PHAs

Because PHAs are now so widely used and accepted, it is useful to examine some of their strengths and weaknesses. Doing so will help a team select the most appropriate method, and will help provide a sense of proportion regarding the benefits to be obtained from conducting a PHA.

Strengths Of PHAs

Many of the strengths of the PHA process have been discussed in the previous pages. The following are particularly important.

Time To Think

One of the greatest benefits of a PHA is that it gives the team members time to systematically and thoroughly think through the hazards associated with the facilities for which they are responsible. Most team members are normally very busy with their day-to-day work, thus they rarely have chance to take an extended period of time to think in a long-range manner about the safety of the units for which they are responsible. Similarly, designers of new facilities are usually under considerable short-term pressures to get their work completed. The PHA provides everyone on the design team with an opportunity to kick back, catch their breath, and reflect on the overall safety of the facility that they have just designed.

Because it is so important that the team members distance themselves from day-to-day chores, it is critical that the team leader ensure there are no interruptions in the form of telephone calls or radio messages during the PHA meetings. He or she must ensure that the team members' commitment of time is not violated by the demands of "real work." Maintaining such discipline can be difficult; the team members generally know the unit well, and are highly respected. Consequently, there is constant pressure to take them off the PHA to attend to "more important" issues. Phrases such as, "we've got a business to run, we can't spend all day in meetings, you know" are symptomatic of this attitude. The leader must make it clear to everyone, particularly managers, that the PHA *is* the most important issue for these key people at this particular point in time.

Cross-Discipline Thinking

An effective PHA brings together people with different skills and backgrounds, thus leading to fruitful cross-disciplinary thinking. The presence of persons from multiple disciplines is particularly helpful at flushing out potentially hazardous assumptions on the lines of, "I thought that your department handled that. Oh, I thought your people were taking care of it."

Economic Payoff

Although the normal reason for carrying out a PHA is to improve safety, many managers believe that the insights generated can also help improve production economics. Unfortunately, it is often hard to verify such opinions. In particular, if the team identifies a high-consequence, low-frequency hazard, which is then ameliorated, there is no direct financial benefit to the company (apart from a possible reduction in insurance premiums) because nothing in a day-to-day sense has changed. It can be difficult to justify spending funds on protecting against what has never actually happened and what is unlikely ever to happen. Therefore, the economic justification for PHAs usually has to focus on the prevention of events that have a high frequency — say, once every five years or less.

Process Training

As an additional, if indirect, form of economic payoff, PHAs provide an excellent training forum for those who are unfamiliar with the process being analyzed. These people obtain an excellent overall picture of the process; they see how different aspects of the operation — instrumentation, operating strategy, and equipment performance — all fit together.

The training benefits also apply to personnel with years of experience on the facility being analyzed. These people are often surprised to find that they learn a considerable amount about their process, particularly with regard to the original design decisions and the roles of other departments. In particular, those who work in maintenance often get to understand the process *as a process* — often for the first time.

Development Of Process Safety Information

An important side-benefit of the PHA process is that it puts management's feet to the fire with respect to developing up-to-date Process Safety Information (page 269). In particular, preparing for a PHA ensures that the time and effort is spent on

making sure that the P&IDs and other drawings do indeed reflect the “as-built” condition of the unit.

During the course of a PHA, the team will almost certainly find problems with some of the Process Safety Information — particularly the availability of Safe Upper and Lower Limits. Where possible, the technical management at the facility should attempt to find or develop that information before the conclusion of the PHA. On the other hand, minor errors in the P&IDs and other documents can be recorded separately from the main PHA notes, and corrected following the PHA meetings.

Limitations Of PHAs

Although PHAs are a powerful and effective tool for finding and analyzing hazards, they do have limitations, some of which are discussed below.

False Confidence

Given the investment that managers make in the PHA process, they tend to expect that the PHA team will uncover all hazards. Management sometimes has trouble understanding that the team — no matter how well qualified — will not identify all hazards. Then, if an accident occurs on the unit following the completion of the PHA, and the team had not identified that particular scenario, some people will use this to “prove” that PHAs “don’t work”, or to blame the PHA team for not having been thorough enough.

The response to this line of argument is that the number of potential accident scenarios on a facility is very large indeed — so large that no PHA team can spot them all. However, the PHA will identify many of the potential accidents. Furthermore, everyone should understand that the purpose of a PHA is not just to find hazards, but also to create a way of thinking among all employees.

Safeguards

Safeguards can be another source of false confidence. It is highly unlikely that a highly hazardous situation has never been considered at all; hence, safeguards such as relief valves and interlocks will already be in place. However, if these safeguards are not working properly, or if an overlooked common-cause effect (page 191) exists, then the safety of the facility may be much less than anticipated. Moreover, given that most safeguards are passive devices, it is quite possible that they will fail covertly. For example, a relief valve may become plugged with polymer, with no one perceiving the problem until it is too late.

Team Quality and Composition

The quality of any PHA depends entirely on the composition of the team, and on the capabilities of the team members. The downsizing trends that have become so prevalent have had a double impact on PHAs. First, the need for hazards analyses has increased as fewer people in the organization possess "corporate memory" as to what can go wrong. Second, because experienced people are fewer in number, the demands on their time from all quarters has dramatically increased, so it is increasingly difficult to get them to schedule blocks of time to participate in the PHAs.

Sophisticated Use Of Language

PHAs use complex language constructs. A statement such as, "If the valve *could* leak, a vapor cloud *would* form, and so we *should* reduce the pressure" is far from easy to understand for those whose first language is not English. No doubt all languages could come up with similar examples.

If the team members are not fluent in the language of the PHA, the quality of the analysis will be degraded. Yet many PHAs are international with team members from many nations. Often English is the official language of the project, yet many of the personnel assigned to the PHA team do not speak English

fluently, and naturally prefer to think in their mother tongue. One HAZOP team, for example, was composed of participants whose respective native tongues were German, Spanish and English. It was agreed that English would be the language of record, since almost all the team members spoke English quite well. However, the leader, recognizing that people need to think and speak in their own languages, established the following rules:

1. Any person on the team could declare a “language time-out” like a quarterback. The leader then declared an official timeout, using the official’s signal shown in Figure 1-11.

Figure 1-11
PHA Leader’s Time-Out Signal

2. During the course of the timeout (which usually lasted around five minutes,) the team members broke into language groups, and chatted in their language about the hazard in question.

3. At the end of the timeout, each team reported to the scribe, who recorded the insights and concerns in English in the HAZOP software.

Ironically, far from detracting from the quality of the analysis, this “language time-out” method actually improved the quality of the analysis because it forced everyone to slow down, and to think things through. It effectively short-circuited the “Oh, come on!

That's no big deal — let's get on with it!" attitude sometimes observed in experienced (and bored) PHA teams.

Difficulties With Reporting

PHA reports can be very difficult to read and understand. During the PHA meetings, the team may have had an exciting and insightful discussion into a particular situation. However, unless the quality of the written notes is of the highest, it is often difficult for others (even the original team members) to re-create the discussion later and to understand the rationale behind some of the recommendations and discussions using just the written report.

A well-written report, however, may make the team's work more valuable over time by reinforcing corporate memory and avoiding redundant labor.

The important topic of PHA reports is discussed in Chapter 7.

Qualitative / Circularity

Issues to do with the qualitative nature of PHAs and the danger of circular thinking have already been discussed on page 11. The team leader should make every effort to quantify the analysis as far as possible so as to provide a clear definition of the risks associated with the identified hazards.

Abstraction

The focus on high consequence/low probability accident scenarios can give the impression that PHAs are abstract and irrelevant. The great majority of recommendations only show their benefit by preventing something from happening that has never happened anyway, and probably never will happen, regardless of what anyone does. This is not a weakness of the PHA concept so much as a creation of information above and beyond immediate needs, thus generating a perception of irrelevance.

Boredom

Process Hazards Analyses are frequently long-winded and boring. It is difficult for anyone to maintain concentration and enthusiasm when the meetings drag on for days — even weeks, especially when few significant findings are being generated. Boredom is a particularly vexing problem for experienced PHA team members, especially when participating in Revalidation PHAs (page 277). Such PHAs are, by definition, going over plowed ground, so the chance of finding a major issue is low. The team members may feel that they have seen it all before and that they really do not need to go through a full guideword discussion of every point. To some extent, they are correct in this opinion. The catch is that, in their reluctance to thoroughly review all possibilities, they may overlook an unusual situation that falls outside their previous experience. Boredom induces an attitude of “let’s just get on with it, ” and “let’s get this over with — after all we’ve got real work to do.” Such attitudes can lead the team to miss critical issues. In order to overcome these difficulties, it is suggested that the Revalidation PHA use a different analytical technique from the original PHA

The above comments on the potentially boring nature of a PHA are not merely aesthetic. Only if the discussions are lively and interesting will the team members participate to the fullest extent. No one can maintain enthusiasm over a long period of time unless he or she feels that meaningful results are being obtained.

Equipment Orientation

Most PHA teams are composed of persons who have a technical background. As such, they tend to view the plant in terms of equipment rather than people or management systems. There is nothing inherently wrong with this approach, but it is limiting. Other ways of looking at a unit are in terms of people or management systems.

For example, an equipment-oriented team might say, “The tank overflowed because the level controller failed.” A people-

oriented team may say, “The tank overflowed because the instrument technician did not maintain the level controller properly.” A management-oriented team would say, “The tank overflowed because we did not have an adequate training program for our instrument technicians.”

The team leader should encourage those team members with an equipment/technical background to look at hazards from these other points of view.

Contingent, System, and Common-Cause Failures

PHAs are usually team exercises. Interactions between the team members, and the different sets of knowledge that each person brings to the meetings are crucial to the success of the outcome. However, teams typically have trouble discussing scenarios that involve more than one hazard event because the discussion becomes confused and difficult to follow. The following events can create difficulties.

- *Contingent Failures* are those where one event triggers another, in some type of domino effect. Complex instrumentation systems can create chains of events, not all of which are easy to forecast.

- *System Failures* are usually associated with utilities such as electrical power, cooling water, and steam. The failure of a system has multiple effects at many points in the process. Once more, it can be difficult to predict exactly what will happen, and where.

- *Common-Cause Failures* are described in the chapter on Fault Trees. They represent those situations where a single event can disable two or more supposedly independent systems. For example, in the standard example P-101A and B are driven by steam and electricity, thus providing redundancy of systems. However, if the electrical power fails, the boilers may go down, thus leading to a loss of steam and a failure of

the complete P-101 system. In this case, the electrical power failure is a common-cause effect.

When PHA teams have trouble analyzing the complex systems, the leader should consider opting for a technique such as Fault Tree Analysis, that uses rigorous logic, and that can deal with intricate interactions of systems.

NON-PROCESS APPLICATIONS

As the name implies, a Process Hazards Analysis has to do with the analysis of *processes.* However, many of the PHA principles can be used in non-process situations. For example, when discussing transportation risks, the traditional HAZOP guidewords (described in Chapter 3) can be transformed to analyze vehicle, ship or train movements, as shown in Table 1-5, to create a “THA” or Transportation Hazards Analysis.

Table 1-5
THA Guidewords

PHA	THA
High Flow	High speed of vehicle
Low/No Flow	Vehicle accidentally stops Ship hits dock Train locomotive loses power
Reverse Flow	Truck Reverses Inadvertent reversing of train
High Temperature	Locomotive fire Engine Room fire Truck fire Freight car fire
Loss of Containment	Derailment Ship runs aground Truck overturns

When considering the use of PHA techniques for non-process situations, the key question that the team must consider is whether the system being examined can be modeled as a process. In the case of transportation, as shown above, the movement of a ship or train can be compared to the flow of liquid in a pipe. “Reverse Flow”, for example, becomes “Vehicle Reverses.” However, in pure manufacturing situations, the PHA technique is not as likely to be equally effective because the “process” consists of a series of discrete events, rather than a flow of materials around the system.

CONCLUSIONS

Process Hazards Analyses have become an integral part of the way in which most companies in the process industries do business. Furthermore, many regulatory bodies require that PHAs be conducted on a regular basis. A wide range of PHA

techniques is available, but all are team efforts in which a combination of plant knowledge and creative thinking helps everyone understand what hazards exist on the facility.