# ON THE ABILITY OF PROCESS HAZARD ANALYSIS TO IDENTIFY ACCIDENTS

by Paul Baybutt
Primatech Inc., 50 Northwoods Blvd., Columbus, OH 43235
paulb@primatech.com

A version of this paper appeared in Process Safety Progress, Vol. 22, No. 3, September, 2003.

## Abstract

Process hazard analysis (PHA) has become the standard way of identifying possible accidents in processes. However, despite the large number of studies that have been performed since OSHA's process safety management standard was issued in 1992, accidents still occur. When this happens the effectiveness of PHA and the quality of the studies performed may be questioned. Litigation can arise, and attorneys may try to make the case that someone was negligent because the PHA did not identify the accident that occurred.

While it is possible that PHAs may miss accident scenarios owing to the quality of the study performed, there are other reasons why scenarios may not be identified. This paper identifies and describes such reasons.

## Introduction

Process hazard analysis (PHA) is used to identify hazard, or accident, scenarios that may be possible for a process and could result in injuries to people (employees or the public), environmental impact, property loss (on-site or off-site), etc. The purpose in doing so is to provide information to help make decisions on *improving safety* and *reducing the risk* of hazardous chemical releases (see Figure 1).

Many thousands of PHAs have been conducted in the US since 1992 when its use was made mandatory for facilities handling highly hazardous materials covered by OSHA's Process Safety Management Standard (CFR 1910.119). However, there has been little attention paid in the literature to the extent to which PHA achieves its intended objectives of identifying accidents. Taylor has identified some pitfalls in HAZOP studies[(1)].

Whenever accidents occur, there is always the possibility of litigation. For PSM-covered facilities, companies' performance in PSM becomes a key issue, particularly for PHA. It may be argued that the PHA performed for the process should have identified the accident. The argument advanced is that if the accident had been identified, corrective action to prevent it would have been possible. While it is possible that a poor quality PHA may have been performed, there are various other reasons that may result in scenarios not being identified.

## Reasons Accident Scenarios May be Missed by PHA

*1) No PHA method can identify all accidents that could occur in a process.*

Systematic approaches that identify all accident scenarios for processes do not exist since the technical means are not available. Even after the application of best efforts, there will always exist the possibility of unidentified accidents occurring. Thus, there are no guarantees that a particular accident scenario will be identified by PHA. Indeed, this is implied by the very definition of the word "accident" as "an unfortunate incident that happens unexpectedly and unintentionally" or "something that happens by chance or without apparent cause".

The principle of ALARP (As Low As Reasonably Practicable) that is used in risk management[(2)] recognizes that not all risk can be eliminated (see Figure 2). There will always be residual risk of accidents since it may not be practicable to take further action to reduce the risk or to identify the accidents that pose the risk.

*2) The accident may have been excluded from the scope of the PHA study.*

In PHA studies performed for compliance with OSHA's PSM standard, the hazards of fires, explosions and toxic releases for covered chemicals present in a process must be addressed. Others hazards, such as falls off ladders, exposure to chemicals not covered by the regulation, etc., may have been intentionally excluded from the scope of the study. In such cases, accidents involving the hazards excluded from the study will not be identified.

*3) The PHA team may have been unaware of the accident cause.*

PHA does not, by itself, identify hazards or failure mechanisms that cause accidents. Rather, it provides an opportunity for the team conducting the study to use their knowledge and experience to identify accident sequences involving the occurrence of failure mechanisms and the realization of hazards. If the team does not have knowledge or experience of the failure mechanisms involved for certain accidents, they will not be identified in the study.

Typical PHA teams do not have individuals with extensive experience of all the phenomena that could occur in process plants. Rather, teams are staffed with people who have knowledge and experience of the particular plant being studied. This helps ensure accident scenarios specific to the plant are identified, but scenarios involving unusual phenomena of failure mechanisms may not be identified.

Even if the team has such knowledge and/or experience, they must still realize its applicability for the process being studied and how it could actually arise. Teams tend to

judge scenarios with which they are not personally experienced as not credible.

*4) The team may have considered the accident but judged it not credible.*

In order for a PHA team to consider an accident scenario possible, team members must believe there are credible causes for the accident scenario that would result in a hazard being realized, i.e. that a certain combination of events is possible. Often in a PHA study, there is debate about the likelihood of a particular accident scenario occurring. Individuals who believe a scenario is not credible may persuade other team members to their views.

Various factors influence the perception of the credibility of hazard scenarios by the team. These include the age and history of the process. For well-established processes that have operated successfully for many years, teams tend to judge some hazard scenarios as not credible. Human nature is to downplay risks that have not been encountered.

Familiarity with hazards can also cause them to be underrated by team members who have worked with a process for many years. In a PHA study, hazards that have been accepted by team members may be judged of low significance compared to other hazards which may not have been previously considered. Most people are not overly concerned about driving on a narrow two-lane road. However, the risk of a head-on collision can be significant and the potential consequences deadly. Familiarity can triumph over logic. For example, in the Australian outback there are two-lane roads without speed limits. Vehicles routinely travel at over 100 mph and may be overtaken by other vehicles traveling at even higher speeds.

*5) The team may have considered the accident but judged it not significant.*

If a team member has experienced accident conditions that did not result in significant consequences, the scenario may be dismissed by the team, even though a variant of it may pose serious consequences. For example, operators may come to accept temperature excursions above normal operating limits when no adverse consequences are experienced. However, it may only be a matter of time before an excursion results in a runway reaction.

*6) The team may have overlooked the accident.*

There are various reasons an accident scenario may be overlooked by a team:

<u>Human Nature</u>

It would be unreasonable to expect perfection in the performance of participants. Indeed, people can rarely, if ever, perform complex tasks perfectly and PHA studies are complex, intellectually demanding activities that place high demands on the cognitive

resources of participants that are almost always higher than in their normal work. Studies involve intense brainstorming performed over extended time periods. To compound the problem, the work is also often repetitive. Fatigue and boredom have to be combated. Participants can become jaded, even in the face of the desire to do a good job.

The distractions and demands of everyday life can also be a factor. Problems in personal lives and at work can influence the performance of team members in ways that are difficult to assess and may not even be known or recognized. Human performance can fluctuate from day-to-day even under normal circumstances.

These human factors act to decrease the likelihood of identifying accidents in a PHA, particularly the more complex scenarios. Even if hazard analysis participants could perform perfectly, unidentified accident scenarios will remain, as described earlier.

## Overlooking the Obvious

Teams are understandably concerned with identifying scenarios that are not readily apparent. That is the strength of predictive hazard analysis. They focus on the complexities of the process trying to identify such scenarios. However, this may result in overlooking simple scenarios that, with hindsight, may be obvious.

## Information Overload

The team may be unable to digest all process information. There are practical limits to how much process information can be read, understood and applied in a PHA. Process drawings such as P&IDs are typically the standard reference for teams. Other documents may be consulted, such as electrical one-line diagrams, operating procedures, equipment specification sheets, etc., but typically teams cannot read every document that is available.

During an accident investigation it may be determined that a particular piece of information was available to the PHA team and, if considered, may have prevented the accident. While such conclusions may seem obvious with the benefit of hindsight, they may have been far from obvious for the PHA team. The nugget of information may have been buried in a haystack of paper, or its significance may not have been obvious at the time.

It may also be argued that abundant checklists are available on many topics and they should all be used in PHA. However, there are practical limits on how many checklists can be applied by a team during a PHA. For example, Appendix B, “Supplemental Questions for Hazard Evaluations” of “Guidelines for Hazard Evaluation Procedures, AIChE/CCPS, 1994" contains a 46-page checklist of questions. It is simply not practical

to use such a checklist, or others like it, throughout a PHA. The repetition involved and fatigue induced in the team members would quickly negate the benefits provided by the checklist.

False Sense of Security

Whenever a serious, previously unknown, potential accident is identified by a team there is usually considerable discussion that can take significant time. In these circumstances the team may move on to the next part of the process in the belief they have done the job needed for the current part of the process. The team has a sense of mission accomplished that may not be justified. The satisfaction felt by the team in discovering the scenario can distract them from continuing with the process.

Inappropriate analogies.

Commonly, processes contain sections that are similar or even identical. Teams conclude the hazard scenarios for them should be the same, provide a cross-reference, and move on. However, sometimes apparently minor differences can result in the possibility of other types of accidents that may go unidentified. It may be the team recognizes the differences but does not see any significance from the viewpoint of hazard analysis. For example, two process lines appear to be identical but one has relief and the other does not.

*7) The accident sequence may be too complex for the team to identify.*

PHA is dependent on the team being able to identify the events that may result in accidents and judge their likelihood to determine if the accidents are credible. The more events involved in an accident sequence, the harder it is for the team to conceptualize and identify the sequence, and the less likely it will be judged as credible. In a hazard analysis these decisions are made qualitatively, almost always without recourse to calculations or quantitative data.

An analogy can be made with drawing colored balls from a bag. If balls of different colors are placed in the bag, it is not hard to identify the possible colors of a single ball drawn from the bag, if the colors are known. It is harder to identify the possible color combinations of multiple balls drawn from the bag. The more colors of balls in the bag, the more difficult it becomes to identify the possible color combinations. If the number of balls of each color varies, it is harder still to predict the likelihood of occurrence of a particular color combination. Yet this is akin to what is attempted in a hazard analysis where the analysts have to identify the possible events (colors of balls), and consider their possible combinations (hazard scenarios) and likelihood (i.e. credibility).

Moreover, processes are invariably engineered so that the likelihood of high consequence accidents such as major fires, explosions and toxic releases is low (see Figure 3). This is often accomplished using process designs that require multiple failures for high consequence accidents. Generally, the more events that make up an accident scenario, the lower its likelihood. Therefore, when hazard analysis teams consider scenarios composed of multiple events, there can be a tendency for the scenarios to be judged of sufficiently low likelihood not to be credible.

Furthermore, identification of hazard scenarios is particularly challenging when accident contributors originate from within different parts of the process. In a PHA study the process is broken down into constituent pieces (called “nodes” in the jargon of HAZOP, for example) to facilitate the analysis. While this has the advantage of focusing attention on specific parts of the process to facilitate analysis, it has the unfortunate disadvantage of complicating the identification of scenarios whose contributors originate within different parts (nodes) of the process. The use of a global node can help address this problem but there are no guarantees it will result in the identification of such scenarios.

*8) The process may be too complex for the team to identify a particular accident.*

Process complexity complicates the identification of scenarios. For example, manifolds with multiple valves and pipe routings can be difficult for teams to understand fully. The same is true for complicated control systems. Teams may be reluctant to admit or even be unaware they do not fully understand the process. Unfortunately, wherever there is lack of understanding, there is the potential for missed accident scenarios.

*9) Accident scenarios may be variants of that recorded in a PHA.*

PHA simplifies accident scenarios. Accidents begin with initiating events. Various intermediate events follow. There can be multiple ways in which an accident scenario develops, depending on the success or failure of process responses to the initiating event. The various combinations of events define variants of an accident scenario. Usually, the variant with the worst-case consequences is recorded in PHA.

It is possible a team may be mistaken in their identification of worst-case scenarios. Another variant of the scenario may turn out to pose worse consequences. It is also possible that corrective actions taken for a worst-case scenario may not help protect against lesser consequence accidents. For example, a team may consider rupture of a ground-level line and recommend the installation of a vehicle barrier. However, this would not protect against smaller ruptures caused by dropping objects from a lift.

*10) The accident may involve new phenomena or previously unknown failure*

*mechanisms.*

New phenomena and/or failure mechanisms are periodically discovered. Consequently, by definition, they cannot be addressed in PHA.

## Further Reasons Accidents May Occur

Even when an accident scenario is identified by a team, several additional requirements must be met before action is taken to protect against the scenario:

1) *The PHA team must consider the scenario significant enough to warrant a recommendation for risk reduction.*

Decisions on risk reduction measures are made qualitatively in PHA. There is scope for misjudgment of the actual risk. If the risk is underestimated or judged acceptable, there will be no recommendation made for risk reduction measures.

2) *In reviewing the results of the PHA study, management must agree with recommendations that actions to reduce risks should be taken.*

Risks recognized by the PHA team may be judged acceptable by management. Consequently, it is possible that a PHA finding would not necessarily prompt or result in a process modification.

3) *Work on risk reduction actions must be scheduled and performed.*

Recommendations from a PHA must be resolved and an action plan developed for their implementation. Furthermore, some risk reduction measures may take significant time to implement. Therefore, it is possible that accidents may occur as actions are being taken to deal with them.

## Conclusions

When accidents do occur subsequent to the performance of a PHA, as is inevitable, one does not need much imagination to envision the anguish of participants who may have lost colleagues in the accident. Absent evidence of inadequate performance by PHA team participants, criticism of team performance is unfair and unfounded given the nature of PHA. This is like blaming a doctor for losing a patient after responsible care has been administered. As much as we would like to be able to control all aspects of the performance of a process, or the functioning of the human body, unfortunately we

cannot.

Additionally, at best, PHA identifies potential accidents and cannot prevent them from occurring. Before any steps are taken to ameliorate risks identified, team members and/or company engineers must first decide action is necessary to reduce risk and develop specific recommendations. These recommendations must then be evaluated, endorsed and prioritized by management for implementation.

Even if an accident scenario is identified in a PHA, and actions are taken to ameliorate the risk, there are still no guarantees that the accident will not occur since ameliorative measures can fail.

Also, owing to the probabilistic nature of events in processes, no matter how low their probability of occurrence, there is no guarantee they will not occur tomorrow. Therefore, the actual occurrence of an accident is not an automatic indicator that a PHA should have identified it.

While the issues discussed in this paper are important limitations for PHA, it is still the best tool available to identify potential accident scenarios.

## References


1. J. R. Taylor, Risk Analysis for Process Plant, Pipelines and Transport, Chapman & Hall, 1994.

2. The Tolerability of Risk from Nuclear Power Stations, Health and Safety Executive, 1992.

Figure 1.Process Hazard Analysis and Decision Making.

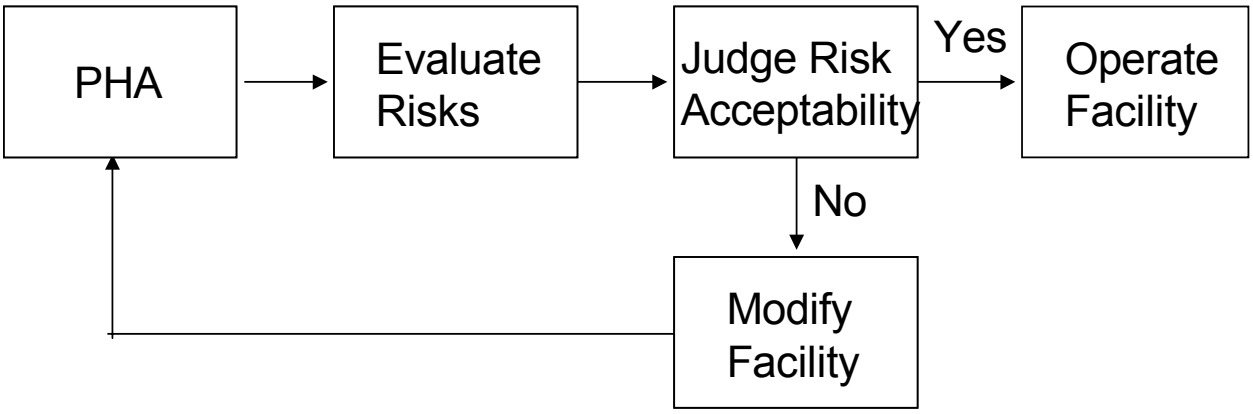

Figure 2. The ALARP Principle

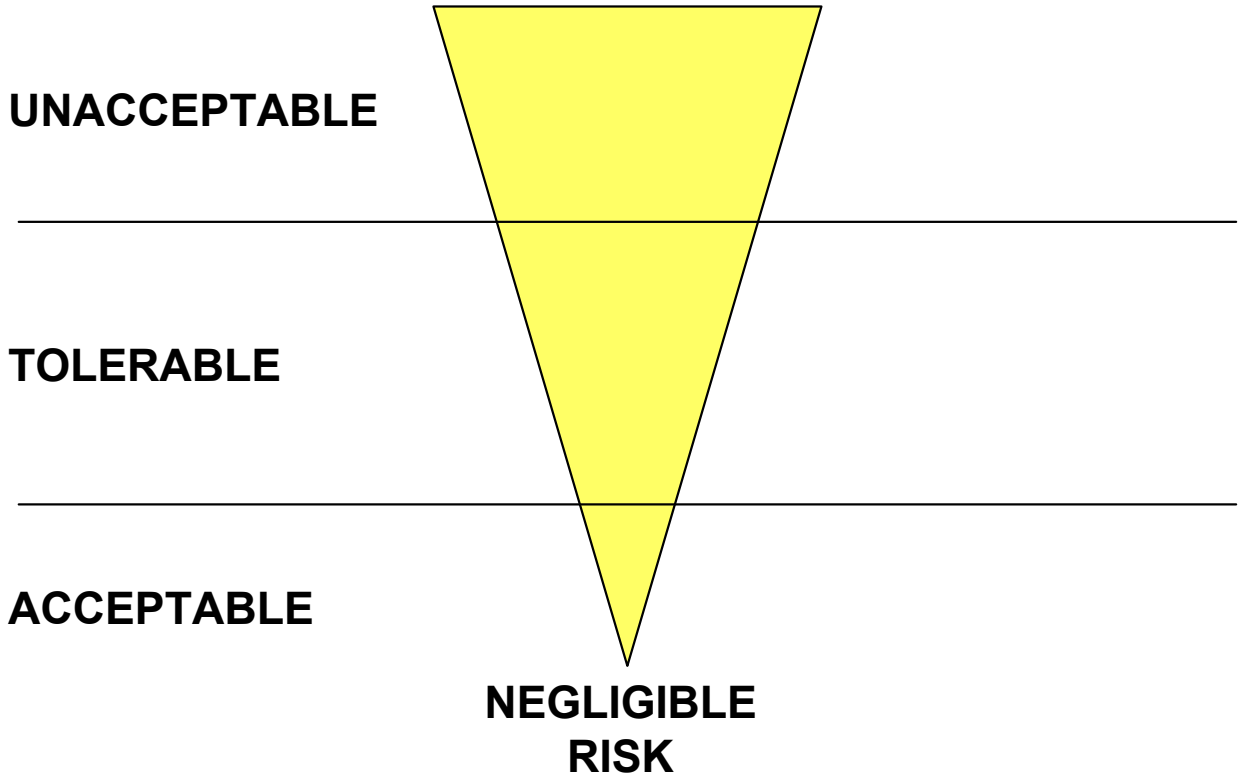

Figure 3. Incident Spectrum