Journal of Hazardous Materials 115 (2004) 181–192

Journal of Hazardous Materials

www.elsevier.com/locate/jhazmat

Evaluating and assessing process hazard analyses

P. John Palmer*

Vescen Consulting, 1523 Taos St., Santa Fe, NM 87505, USA

Available online 15 September 2004

Abstract

Process hazard analysis (PHA) is widely used across a spectrum of industries and facilities, but there are few metrics for the evaluation and assessment of PHAs. Most existing protocols address PHA solely in terms of regulatory compliance, but do not address the completeness or depth of the assessment, as most PHAs have been performed on a "performance basis" under the relevant regulations.

It is possible to objectively assess PHAs, in order to determine adequacy of completion and degree of review, using both audit protocol and scoring approaches. Audit protocol approaches offer simplicity and ease of use, and when combined with specific scoring for adequacy allow for informed decisions about remedial action with respect to the PHA.

Keywords: Process hazard analysis; Quality control; Process safety management; Risk management plan

1. Introduction

Process hazard analysis has a storied history for so relatively new a technical area. The last two decades have seen an enormous amount of effort expended within industry for the completion of PHAs. The various types of structured hazard analysis have come to defined usage in only the last 40 years evolving from useful problem identification techniques conducted in a less formal setting for certain defined issues into computer assisted approaches applied across the entire engineering project management spectrum, from near cocktail-napkin level drawings through final construction, and then to the demolition and removal of entire plants.

The evolution of process hazard analysis has occurred within the overall development of the field of process safety management or loss prevention, itself a relatively new engineering discipline, and has been well documented by those who were present for the entire genesis of the field [1].

The area of hazard analysis has taken on additional tasks as the evolution of the overall field has occurred, most notably becoming a documentation process within the United States for the evaluation of hazards starting with the New Jersey Toxic Catastrophe Prevention Act in 1985 [2], through federal legislation such as the process safety management standard [3] (PSM) and the risk management plan standard [4] (RMP). That various regulations require the performance of PHA, using techniques such as What-If, HAZOP, or What-If-Checklist, has driven formalized documentation within a PHA of regulatory compliance to become a critical area of completion.

In addition, the process of legal review of PHA by company counsel for compliance with regulations, as well as the consideration of PHA for potential legal liabilities in tort, has introduced a substantial aspect of wording and careful parsing of information to address the potential that PHA documentation will be dissected in trials or public hearings.

While no PHA practitioner would openly state that the issue(s) of regulatory compliance and protection for possible litigation are primary forces for the data within PHAs, it cannot be argued that the regulatory and liability implications are without a high level of importance.

Indeed, almost all audits of PHA within the context of PSM and RMP focus on regulatory compliance, often using the OSHA Compliance Guidelines and Enforcement Procedures [5] as the core of the audit protocol question set. And while the CPL approach offers some basis for understanding the overall level of compliance with the regulation, it does not address the issues of the completeness and adequacy of a given PHA, only that the PHA has documented performance to a specified checklist of regulatory requirements.

It has been widely said that "You only get what you measure", and so in compliance with this, PHA has become a process for many practitioners related to meeting items

* Tel.: +1-505-982-3222; fax: +1-505-989-9984.

0304-3894/$ – see front matter © 2004 Published by Elsevier B.V.
doi:10.1016/j.jhazmat.2004.05.032

on a checklist. However, there are vital areas to be assessed within PHA that are not related to compliance or liability alone, but address fundamental practices for the identification of hazards. Trevor Kletz, who has been a practitioner and proponent of PHA, especially HAZOP since its inception, has expressed, "... there is concern that some companies that claim to carry out Hazops are undertaking little more than a perfunctory examination of the line diagrams" [1].

Measurement of PHA performance requires quality criteria and performance metrics. At this point in time, there is no consensus generated or generally accepted set of quality criteria for the results of PHA. Aside from the application of regulatory compliance inspection measurements taken from government publications, there are no metrics for what constitutes a complete and appropriately in-depth PHA.

2. Basic issues

Before starting to measure items within PHA, it is critical to define the scope of what PHA can reasonably be expected to include, or perhaps more to the point, to exclude; and then to carefully identify the primary areas of concern within PHA. In order to consider these points, it is necessary to consider some basic assumptions within the industry for PHA. Following that, simple metrics can be defined, which can then be expanded into more complex performance measurement criteria to be used in an audit protocol format.

2.1. Unproven assumptions

PHA is not a group of techniques providing absolutes or definitive answers, in that there are a substantial number of assumptions underlying any PHA which are employed to allow PHA to be accomplished in a time and resource effective manner. Without addressing and understanding the assumptions used for PHAs, a belief in the results of PHA becomes almost a matter of faith. A number of the underlying assumptions within the use of PHA are unproven. Measuring performance against unproven assumptions will not provide an effective assessment of the adequacy of a PHA.

Although there is proven value to process hazard analysis, for some, PHA is used to address all issues, regardless of applicability, by setting out objectives for inclusion. In the last few years, PHA has been proposed as a method for assessing site security, critical control systems, and compliance with ISO standards. PHA is a group of tools, some more appropriate for a given set of circumstances, some less, but tools that can accomplish only certain tasks within a limited time.

The assumption that PHA can be applied to all conditions and will provide any result stipulated in advance as a "project objective" could well be considered the primary unproven assumption of PHA.

Companies typically attempt to perform PHA using techniques that lend themselves to more intuitive and simpler reviews, rather than more quantitative approaches, based on time and personnel resource issues. For this reason, the What-If and HAZOP techniques are more widely employed than fault tree analysis and failure modes and effects analysis. While techniques such as What-If and HAZOP are also considered to more easily address such things as human factors, the need to complete PHA within set regulatory time constraints has been the dominant reason for companies working within the United States' regulatory envelope to use them in preference to other techniques.

Further, while the documentation requirements for PHA have increased greatly since the inception of PSM related regulations, and additional requirements have been added through complementary regulations such as RMP, successive revalidation PHAs completed within the framework are generally expected to take less time for each iteration, even in some cases assumed to be nothing more than a recitation of the existing materials. In some cases, the revalidation PHA team is automatically assumed to require a smaller investment in the preparation and team meeting effort to address hazards based on already having completed a previous PHA.

The assumption that a PHA can be both definitive and complete within successively shorter time constraints with a highly limited set of resources is unproven. The assumption that improved PHA will come with less effort is unproven.

PHA also makes the assumption that hazard identification can be accomplished by considering single causes without addressing supporting issues or secondary causes. Generally, PHA performed within the United States' regulatory envelope uses the simplification of generating single causes for hazard scenarios, even though the investigation of numerous incidents has shown that the assumption of single, often final triggering events is incorrect [6]. This assumption is typically addressed by identifying a list of safeguards, and then assessing the potential failure of safeguards within the likelihood estimated within a relative risk ranking of the scenario.

The assumption that the use of single causes with identified safeguards in a PHA adequately addresses root and supporting causes of incidents is unproven.

A corollary to the single cause assumption is the practice where scenarios are abbreviated within PHA documentation, sometimes to a cause and final consequence of concern, or to a cause and an intermediate result such as a release of flammable or toxic materials. The abbreviation of the scenario to shorter sequences serves to allow for the assessment of more scenarios within a given available time for an analysis, although the abbreviated scenarios would not seem to lend themselves to the assessment of safeguards for intermediate events. In certain cases, the PHA team addresses a scenario in great detail, but the written documentation is abbreviated to reduce team session time, or to make the process of documentation easier. The subsequent revalidation PHA team, often with little continuity of personnel from the previous PHA team, will many times assume that the scenario was fully discussed previously, and not delve into further review.

The assumption that a previous PHA team fully addressed a given issue in the absence of written documentation of the discussion is unsupported.

However, this brings up a perspective that has arisen for PHA in the last decade, that is, that a PHA covers all issues for a given studied process or facility. That assumption has led to facility managers or regulatory agency representatives demanding to see a PHA after a process incident to ensure that the incident had been predicted, and to determine what or which safeguards were operative, inoperative or even non-existent. The assumption that a PHA can have no errors in reviewing hazards for a process is highly suspect, but the concept that a PHA would clearly and perfectly predict the exact course of every possible process incident to allow for full prevention of such incidents is an intellectual leap of incredible proportion.

The failure to prevent the repetition of incidents when the causes are well understood and documented is the subject of a number of books [7–9]. To assume that a dense and difficult to read PHA document would prevent incidents in and of itself is at best wishful thinking, and at worst, purposeful ignorance.

The most damaging of unproven assumptions for PHA is the assumption that the performance of a PHA will then definitively and conclusively prevent incidents identified within the PHA.

2.2. Easily measurable aspects of PHA

The measurable aspects of PHA can be divided into relatively simple issues where the metrics are easily discerned and non-complex. Most of these issues are related to either simple project management metrics and/or to regulatory requirements, and would include:

- inclusion/exclusion of issues specified in the PHA scope;
- inclusion/exclusion of issues specified in the PHA objectives;
- regulatory requirements for the execution of the PHA, including:
  - appropriate PHA team members;
  - documentation including specified regulatory materials (e.g., identifying potential secondary sources for the hazard assessment in RMP);
  - handling of PHA findings such as resolution of recommendations and development of action plans.
- timetables for start and completion (which can also be tied to regulatory requirements).

The measurement of project management metrics can be developed into a checklist with “yes” or “no” answers, with some discretion for the reviewer to make limited performance assessments against the metrics. Many such metrics are, in fact, included in currently used PHA audit protocols, as these metrics fall within regulatory requirements for execution of PHAs.

In general, project management metrics applied to the assessment of PHA can only determine if the PHA meetings and recommendations were completed within the defined requirements, but cannot be used to assess the overall adequacy of the PHA process.

2.3. Simple measurement of categories within PHA

The next level of assessment of PHA has typically revolved around several issues, which address some simple concepts, including:

- Categories of causes:
  - human error;
  - equipment failure;
  - external events.
- Categories of consequences:
  - onsite personnel effects;
  - offsite public/environmental effects;
  - property damage;
  - production effects.
- Categories of safeguards:
  - prevention;
  - mitigation;
  - detection;
  - emergency response/evacuation measures.

The categorization of causes into three basic areas allows for simple mathematical assessment, making some assumptions about the relative importance of the categories (i.e., human error > equipment failure > external events). However, this approach can over- or underestimate categories based on simple counting. For example, a single cause for loss of flow in a manifold line could be “valve closed in error”, which would be counted as one cause. However, if there are 20 valves in regular use on the manifold, this has importance far out of proportion to the singular nature of the question.

The use of categories for measurement and assessment in PHA has limited opportunity to determine if the PHA has been adequately performed. An outright absence of causes related to human error could show inadequacy for example. That there is some distribution of cause categories is generally accepted; however, there are no consensus values or standard measurement for adequacy of the discussion of causes as a percentage or fraction of total causes considered within a PHA.

Similarly, there are no consensus values or standard measurement for adequacy of the discussion of categories of consequences or safeguards within a PHA.

The assessment of categories within PHA is therefore a starting point for more detailed performance assessment, leading to performance measurements within the categories for PHA elements. The development of performance measurements will allow for discussion and eventual consensus. It should be noted that an assessment of a specific PHA would also include interviews with the PHA team; however, the focus of this paper is the review of the documentation.

3. Performance measurement of PHA elements

Measurement of the adequacy of process hazard analysis requires that a more formal audit approach to the PHA be implemented with valid sampling within the PHA combined with field checks of the material and efficacy of items noted within the PHA. This is a much larger commitment of effort and time than has been applied in many regulatory compliance audits, especially with respect to checking field conditions for engineering measures, and documentation verification of procedures and training for administrative measures.

The use of generally accepted audit approaches using sampling and a formal protocol provides a sound foundation for the assessment of PHA. However, issues of what would be considered "acceptable" performance are both significant and difficult to develop. Currently, there are no consensus standards for what is an "acceptable" performance level for PHA.

3.1. Audit samples for PHA

Generally accepted audit sampling approaches include:

- statistical sampling;
- non-statistical sampling including:
  - judgmental sampling;
  - interval sampling.
- "complete" sampling.

"Complete" sampling in this context is the review of *all* parts of the PHA, omitting no process section whatsoever. Where a PHA's documentation is small enough for complete sampling, this is the preferred approach. Having said that, if a plant has many small PHAs, complete sampling would entail reviewing all small PHAs. In many cases, complete sampling is not logistically possible within reasonable time constraints for an audit.

The use of statistically based sampling has many advantages, including the perception from users of audit results that the samples are objective and unbiased. However, there are a number of issues with respect to generally accepted statistical sampling approaches for the assessment of PHA.

Within a PHA, the overall population for sampling may be relatively small. For example, the number of nodes in a HAZOP may be less than 30, the generally accepted sample size for the normal distribution. Use of smaller sample sizes with other distributions introduces additional possible error. Hazard cases or scenarios are not distributed throughout the PHA according to most statistical distributions, which renders the sampling approach invalid. Moreover, certain parts of a process reviewed in a PHA can be much more hazardous than other parts, again, rendering the sampling approach invalid. A statistically generated sample plan for audit could potentially look at predominately at lower hazard areas as a result. Thus, the application of statistical sampling approaches for the assessment of PHA may not yield objective results.

Similarly, non-statistical interval sampling could look predominately at lower hazard areas. While interval testing has the advantage of simplicity (e.g., "pick every third system and subsystem in the What-If-Checklist"), it does not provide assurance that the PHA is adequate.

However, where a PHA encompasses many areas of relatively similar hazard, a statistical or interval sampling approach could be employed.

In the absence of a sufficiently large sample with evenly distributed hazard levels, a judgmental sampling approach may be the most appropriate direction to take. Judgmental sampling is sometimes derided as "subjective", but it would be better referred to as using "professional judgment", based on the use of experienced and expert auditors.

Judgmental sample choices should focus on:

- high hazard sections of the process, defined through such things as material, large inventories, enhanced process conditions such as pressure or temperature;
- sections of the process with high impact process safety incidents;
- sections of the process with high numbers of process safety incidents;
- sections of the process that correlate with high impact industry process safety incidents.

Inside defined judgmental sample sections of the process, it may be appropriate to employ complete or statistically based sampling of the specific PHA materials concerning that section of the process. If the number of judgmentally sampled sections of the process is small, it is more desirable to perform complete sampling within the judgmentally sampled section of the process.

3.2. Audit protocol elements for performance assessment

The audit protocol elements for performance assessment should follow the PHA technique that is employed at the facility. For the purposes of discussion, this paper will work with the HAZOP technique, but the approach would be similar for any of the generally accepted techniques.

An abbreviated and abridged sample protocol is attached in Appendix A as an example. The example protocol included in Appendix A is not represented as either a minimum or maximum level of performance for the execution of a HAZOP study, but is instead an illustration of performance criteria questions for an audit protocol.

The audit protocol elements for performance assessment in a HAZOP would include:

- node division;
- parameters/deviations;
- causes;
- consequences;
- safeguards;
- risk ranking;
- recommendations.

While the division of a process into nodes for the performance of a HAZOP has many qualifications and implications for the adequate performance of the PHA, this is not being addressed within this paper for brevity, although representative questions are included in the sample PHA protocol attached to the paper.

Audit protocol questions are typically written within a "yes"/"no" format to allow for ready use. In some cases, audit protocol questions can be scored using either a relative scheme (e.g., score 1–10), a functional scheme (e.g., "failed", "marginal", "functional") or an actual measurement of performance (e.g., availability measurements or incident case numbers).

It must be noted that the overall documentation for a PHA is not confined to the worksheets of the PHA, but can also include the PHA report, site-wide analysis of issues such as facility siting, or could be referenced within another PHA analysis and report. While the discussion below is oriented towards worksheets, this is done only for the purpose of simplicity of discussion within this paper.

The audit protocol performance questions for causes could follow a progressively more detailed question sequence such as:

- Categories of causes are all addressed (e.g., human error, equipment failure, external events, common cause events)?
- Causes include all reasonable potential issues within the node (e.g., all equipment malfunctions, human interactions, process and utility interactions with the node)?
- All previously identified incidents for the plant that fall within the node are addressed?
- Causes as much as possible include root and supporting causes for incidents or identified cases (see also discussion in the safeguards audit protocol performance questions)?

Consequences in a PHA are sometimes referred to as the "worst reasonable case" that can occur. The audit protocol performance questions for consequences could follow a progressively more detailed question sequence such as:

- Consequences reflect the "full measure" of the cause and preceding consequences in the scenario (e.g., releases reflect the maximum reasonable quantity of highly hazardous chemical)?
- Consequences reflect the complete sequence of events that can reasonably occur (e.g., a large release can have both onsite and offsite effects where the plant fenceline is within a reasonable distance)?
- Consequences reflect site incident experience (e.g., a release could reasonably have significant personnel injuries where such an event has occurred)?
- Consequences reflect industry incident experience (e.g., a release from a failed railcar loading/unloading hose could reasonably vent down the entire railcar)?

Safeguards in a PHA take several levels of importance, ranging in order of importance from prevention, mitigation, detection/emergency response. The audit protocol performance questions for safeguards could follow a progressively more detailed question sequence such as:

- Safeguards include the performance of equipment, human interaction, and combinations of these which address supporting causes for incidents or identified cases (see also causes audit protocol performance questions above)?
- Safeguards are *applicable* and *capable* to the section of the process under evaluation (e.g., a fire monitor is capable of providing an adequate water stream that can reach the equipment under evaluation, and is not blocked or impeded by other process equipment)?
- Safeguards are *functional* within generally accepted measures of availability (e.g., a safeguard is functional within the time the process is operational or charged with highly hazardous materials)?
- Safeguards are not compromised by the scenario cause or consequences (e.g., a level alarm low is listed for a malfunction of the level control from which it derives its signal)?

The area of risk ranking, often using a relative severity and likelihood ranking approach, an influence whether a PHA team makes recommendations for changes, or not. As such, the risk ranking element of PHA is critical to the performance quality of the PHA. The audit protocol performance questions for risk ranking could follow a progressively more detailed question sequence such as:

- Severity clearly matches identified consequences (e.g., a "low" severity would not match a consequence of "potential severe injury personnel")?
- Severity is provided for all consequences of interest, not one consequence only (e.g., severities would be provided for *both* personnel injury and offsite injury consequences where these have been identified within the scenario)?
- Severity clearly applies to the "worst reasonable consequence" of the scenario (e.g., a railcar completely venting down would not have severities of "low" for all applicable consequences)?
- Severity is not "discounted" due to existing safeguards (e.g., a fire monitor safeguard would not reduce the consequence of a fire to "negligible")?
- Likelihood clearly matches the scenario up to the consequence of interest (e.g., a scenario with a valve left open, potentially resulting in a flammable release with personnel injury, in a plant where such valves are typically plugged or capped would reflect the cause–consequence series modified by the safeguard).
- Likelihood addresses the actual functionality of safeguards, not the hoped for level of performance (e.g., if the water supply for a deluge system is limited, it may only mitigate the consequences, and doesn't lower the likelihood of a large fire to "only known to occur in world-wide industry").

- Likelihood addresses incident results from the plant, possibly modified by improved safeguards since the incident (e.g., a plant unit where a large fire occurred 10 years ago could claim a lower likelihood if fire suppression has been improved).
- Likelihood addresses incident results from the industry, possibly modified by plant specific safeguards (e.g., if a given type of control device has an undesirable level of malfunction, the plant may have placed the device into an enhanced maintenance schedule).

Recommendations are typically addressed within the context of whether or not they were resolved and implemented. However, failures in resolution and implementation can be directly related to inadequately formed recommendations. The audit protocol performance questions for recommendations could include:

- Recommendations are written to allow for specific responses and not as generalities or continuances of existing policies (e.g., "Continue current Management of Change procedures to review changes in the plant" compared with "Consider updating the Management of Change procedure to include other changes such as staffing of the process").
- Recommendations are written to allow for acceptance or justified rejection according to OSHA CPL requirements (e.g., "Install multiple redundant level switches" compared with "Review the installation of a secondary level switch high against increased maintenance of the existing level switch to address potential fouling issues that could compromise performance").

3.3. Acceptability criteria for audit results

Acceptability criteria are an essential part of any audit, but are often complicated in that regulatory performance is confused with technique performance. Noting an area of exception within a PHA does not necessarily mean that the PHA is fatally flawed. A pattern of such failures or a high number of exceptions could mean that the PHA is fatally flawed. At the same time, it is recognized that process hazard analysis is conducted using a team of expert personnel, who by the very nature of being human, can make errors. As was pointed out in the Section 2.1, the assumption that a PHA will identify all possible incidents in a process is unproven.

The question then becomes, what level of performance, or perhaps more to the point, what level of failure would be "acceptable" within the results of an assessed process hazard analysis?

There is no one answer that would be applicable to all facilities and companies. To pick a failure percentage such as "10% of all causes are invalid", or "5% of safeguards are not considered functional" ignores the relative importance of the specific cases to the location or company. As well, if the identified 5% of safeguards are not primary preventative safeguards, does this make the failure "more acceptable" or less?

However, there are some common failures that could lead a given facility or company to further review or reject a PHA. Looking at the issue of causes within a HAZOP, for example, the following could be considered grounds for further review or rejection:

- a consistent failure to review potential causes within a given category such as human error, or
- causes do not address any incidents from the facility or similar industry cases, but address only superficial failures.

Another approach to provide acceptability criteria is to develop a scored or functional result for the audit protocol questions. Where the reviewed results fall below a desired level, this would prompt either further review or rejection.

3.4. Follow-up to audit findings

The concept of further review of a PHA with "unacceptable" audit results is perhaps the most appropriate approach. Where an audit has identified areas of concern, a more detailed assessment could be made to determine if the audit results are truly representative of the specific PHA and other PHAs within the facility. A detailed assessment could use statistical or interval testing for similar equipment, or causes/consequences/safeguards/risk rankings within the facility.

Alternately, the facility or company could determine that certain specific identified audit findings would be "threshold" issues requiring more immediate action in some cases.

Regardless of the findings of the detailed assessment, two alternatives exist for the follow-up to "unacceptable" findings within the assessed PHA. The PHA can be "repaired" or a "scratch revalidation" of the PHA can be performed. The choice would depend on the specific nature of the findings.

In a case where one specific audit protocol area or question was found to be consistently underperformed, it could be possible to edit and update the assessed PHA in that area, with a re-review performed after the edit/update. In the case where multiple areas or questions are found to have a consistent underperformance, a "scratch revalidation", essentially a completely new PHA, would need to be completed.

4. Example case and discussion

An example PHA was conducted for a process including a feed stream to a reactor with a heat exchanger. The example includes specific areas of underperformance (Fig. 1).

The large oval over the causes relates to a failure to assess any human error or external event issues. Only equipment based causes are included. The two smaller ovals on the second cause and related safeguard relates to a possible failure to address a cause that could render the safeguard ineffective. The second figure shows a safeguard that is non-functional

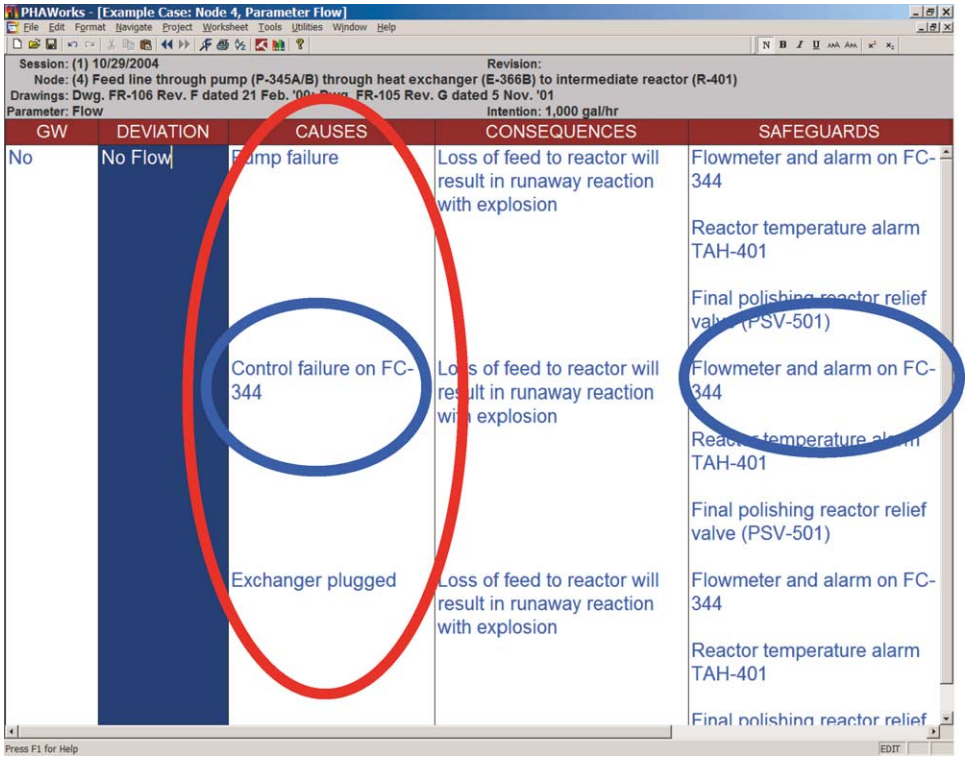


Fig. 1. Example case one.

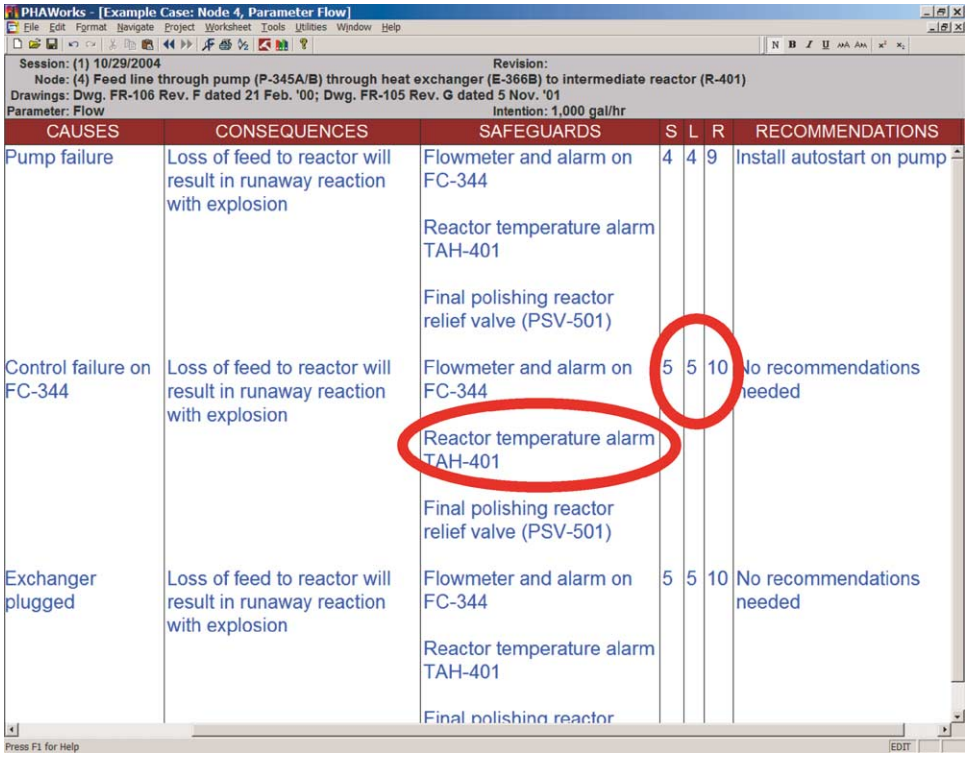
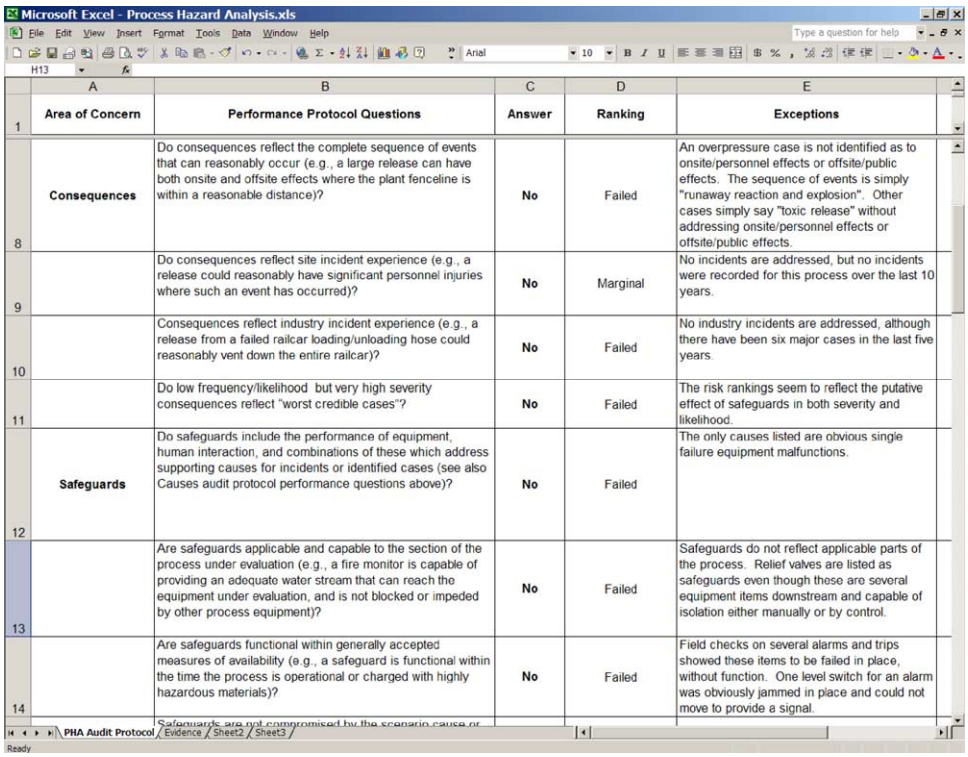


Fig. 2. Example case two (higher risk ranking is more severe).



Microsoft Excel - Process Hazard Analysis.xls

	A	B	C	D	E
1	Area of Concern	Performance Protocol Questions	Answer	Ranking	Exceptions
8	Consequences	Do consequences reflect the complete sequence of events that can reasonably occur (e.g., a large release can have both onsite and offsite effects where the plant fenceline is within a reasonable distance)?	No	Failed	An overpressure case is not identified as to onsite/personnel effects or offsite/public effects. The sequence of events is simply "runaway reaction and explosion". Other cases simply say "toxic release" without addressing onsite/personnel effects or offsite/public effects.
9		Do consequences reflect site incident experience (e.g., a release could reasonably have significant personnel injuries where such an event has occurred)?	No	Marginal	No incidents are addressed, but no incidents were recorded for this process over the last 10 years.
10		Consequences reflect industry incident experience (e.g., a release from a failed railcar loading/unloading hose could reasonably vent down the entire railcar)?	No	Failed	No industry incidents are addressed, although there have been six major cases in the last five years.
11		Do low frequency/likelihood but very high severity consequences reflect "worst credible cases"?	No	Failed	The risk rankings seem to reflect the putative effect of safeguards in both severity and likelihood.
12	Safeguards	Do safeguards include the performance of equipment, human interaction, and combinations of these which address supporting causes for incidents or identified cases (see also Causes audit protocol performance questions above)?	No	Failed	The only causes listed are obvious single failure equipment malfunctions.
13		Are safeguards applicable and capable to the section of the process under evaluation (e.g., a fire monitor is capable of providing an adequate water stream that can reach the equipment under evaluation, and is not blocked or impeded by other process equipment)?	No	Failed	Safeguards do not reflect applicable parts of the process. Relief valves are listed as safeguards even though these are several equipment items downstream and capable of isolation either manually or by control.
14		Are safeguards functional within generally accepted measures of availability (e.g., a safeguard is functional within the time the process is operational or charged with highly hazardous materials)?	No	Failed	Field checks on several alarms and trips showed these items to be failed in place, without function. One level switch for an alarm was obviously jammed in place and could not move to provide a signal.

Fig. 3. Representative audit protocol worksheet.

in the field, as well as a risk ranking that does not reflect the consequence of "... runaway reaction with explosion" (Fig. 2).

A representative audit protocol sheet is shown in Fig. 3. The example case shows many deficiencies—this would most likely not be typical of PHAs conducted in the latter part of the 1990s through today.

The example case also demonstrates an important issue—PHA has evolved significantly in terms of the overall quality of review and documentation in the last 15 years. The author was handed a PHA for an entire refinery in a small stack of paper circa 1990, but today such would comprise many volumes of paper. The process of PHA revalidation has had significant effect on the improvement of PHA findings and documentation, which continues.

However, there are areas where the more widespread and extensive use of PHA has revealed areas for definite improvement, and new technical standards such as S84.01 [10] or API RP752 [11] that have arisen since the initial regulatory drivers in 1992. As these areas have been explored and carefully considered, authors have identified issues such as operator response to multiple alarms [12] that were not considered in the earlier PHAs conducted in good faith by facilities and companies.

In addition, regulatory agencies have developed added expectations for the levels of detail that should be included in PHA. Some of these have arisen in incident findings [13], others through interpretation, but the effect of adding additional areas for review is the same.

As such, the audit process will inevitably show that older PHAs are not as detailed or robust as recent studies. This will need to be addressed through the revalidation process, with enhanced review and requirements. The intent of improved audit protocols for PHA is not to negate or refute previous PHA efforts, but instead to provide better tools to assist in improvement and the evolution of the PHA process.

5. Conclusions

Although the use of process hazard analysis is on the order of four decades old, and has been intensively used within the last two decades, most evaluations and assessments of PHA within the United States have been and are oriented towards regulatory compliance. Successfully addressing regulatory requirements does not automatically translate into an effective or adequate PHA. Simple approaches to counting various PHA elements to determine if categories are met allows for limited assessment, but does not address more subtle issues.

An audit approach with progressively more detailed performance criteria questions could allow for an improved level of evaluation and assessment. Sharing detailed performance criteria questions among various facilities and companies will allow for the development of consensus standards for acceptable performance requirements within PHA.

Appendix A

Example performance audit protocol for review of HAZOP analysis

Area of concern	Performance protocol questions	Answer	Ranking	Exceptions	Recommendations
Node	Does the node breakdown include all process equipment noted within the scope for the PHA?				
	Does the node breakdown include related utilities or other support equipment noted within the scope for the PHA?				
	Are node designations consistent throughout the PHA with respect to the scope and objectives for the PHA?				
	Are nodes for similar or identical types of equipment identified as general cases/examples with all relevant equipment numbers listed, or is there an explanation in the accompanying report that explains the use of general nodes?				
Parameter	Is the parameter measured, controlled, or otherwise maintained in this node?				
	Is the parameter intention clearly explained with upper and lower limits (e.g., flowrate of 1500 ± 200 GPH)?				
	Are the upper and lower limits for the parameter the *reasonable* upper and lower limits for safe operation (is there evidence the process has run or regularly runs outside the upper and lower limits for the parameter)?				
	Is there only one intention with limits for the parameter and not multiple intentions included (e.g., flow is 500 GPM on line A and 250 GPM on line B)?				
	Are all parameters relevant to the node used, and are parameters not relevant clearly excluded?				
	Are all parameters that relate to the node either documented or referenced specifically?				
Deviation	Are all *reasonable* deviations for the parameter used or referenced?				
	Are the deviations outside of the defined upper and lower parameter limits for the node?				
	Are the deviations reasonably documented (e.g., less hydrocarbon level *and* less water level in an accumulator/separator)?				
Causes	Are all causes inside the node boundaries or documented where they extend across boundaries (e.g., level control causes could be within a vessel node and a line node)?				
	Are credible low likelihood but high severity causes included (e.g., large storage vessel failures)?				
	Are all categories of causes addressed (e.g., human error, equipment failure, external events, common cause events)?				
	Do causes include all reasonable potential issues within the node (e.g., all equipment malfunctions, human interactions, process and utility interactions with the node)?				
	Are all previously identified incidents for the plant that fall within the node addressed (note that this can also be documented in other parts of the worksheet)?				
	Do causes as much as possible include root (primary) and supporting causes for incidents or identified cases (see also discussion in the safeguards audit protocol performance questions)?				
	Are causes explored to a depth appropriate for the scope and objectives of the PHA (e.g., “control failure” is listed when the scope and objectives indicate a detailed study with critical control identification issues to be addressed)?				

Appendix A (*Continued*)

Area of concern	Performance protocol questions	Answer	Ranking	Exceptions	Recommendations
	Are causes consistently addressed between separate deviations and nodes (e.g., a detailed assessment of individual valve positions in one case, where another case simply considers "closed valves"), or is there an explanation for the difference?				
	Are "common cause" cases considered adequately (e.g., failure of level control and a level switch high is not a "double jeopardy" case if the base bridle valve is closed; failure of multiple level floats due to fouling; failure of multiple level switches due to short chain polymer formation in situ)?				
	Are combinations of human error/factors and equipment failures considered (e.g., LEL detector failure when making routine rounds, failure to complete rounds when LEL detection is in an undetected failed state)?				
	Are redundant equipment failures considered for cases where the "spare" is under repair or failed (e.g., spare pump with autostart is removed for refit, spare relief is being bench-tested)?				
	Do human error cases consider errors in maintenance (e.g., equipment improperly returned to service, control set points incorrect reset, improper LO/TO)?				
	Do human error cases consider errors in written procedures or other areas that could allow for error(e.g., procedure is missing a step, or procedure is not used because it is essentially unreadable)?				
	Do human error cases consider errors in management (e.g., turn off alarms or interlocks to minimize shutdowns, increase production beyond safe limits)?				
	Do human error cases consider failures in PSM and RMP elements (e.g., failure to properly close out a temporary MOC)?				
	Are causes where equipment is failed, *but not detected as failed* considered?				
	Are control failures considered in terms of failure-in-place, fail high, and, fail low?				
	Do control failures consider cases where the loop fails in-place, high, or low, but does not alarm or detect out of limits?				
	Are failures of utilities or other support systems considered as per the scope and objectives for the PHA?				
	Are external events considered in each node or referenced to a global node?				
	Do causes identify specific equipment to allow for later review or search in support of MOCs (e.g., "pressure safety valve RV-455 fails to open at nominal set pressure of 75 psig)?				
	Are all cause "spaces" appropriately filled with a cause or a standard disclaimer (e.g., "No causes determined for this deviation by the team")?				
Consequences	Do consequences reflect the "full measure" of the cause and preceding consequences in the scenario (e.g., releases reflect the maximum reasonable quantity of highly hazardous chemical)?				
	Do consequences reflect the complete sequence of events that can reasonably occur (e.g., a large release can have both onsite and offsite effects where the plant fenceline is within a reasonable distance)?				

Appendix A (*Continued*)

Area of concern	Performance protocol questions	Answer	Ranking	Exceptions	Recommendations
	Do consequences reflect site incident experience (e.g., a release could reasonably have significant personnel injuries where such an event has occurred)?				
	Consequences reflect industry incident experience (e.g., a release from a failed railcar loading/unloading hose could reasonably vent down the entire railcar)?				
	Do low frequency/likelihood but very high severity consequences reflect "worst credible cases"?				
	Are consequences considered wherever they may impact throughout the process (e.g., loss of feed to a day tank could starve a downstream reactor allowing a potential runaway)?				
	Are the consequences considered consistent with the scope and objectives of the PHA (e.g., equipment damage issues are addressed when the PHA scope and objectives only include on-site or offsite impacts on people)?				
	Are consequences discussed to the level of detail required by the scope and objectives for the PHA (e.g., a very detailed product color quality issue is discussed when the objectives do not include operability and sales issues)?				
	Are consequences for different areas of concern (e.g., public injury, employee injury, production losses) separated to allow for separate risk rankings as defined by the scope and objectives for the PHA?				
	Are all consequence "spaces" appropriately filled with a consequence or a standard disclaimer (e.g., "no hazardous consequences determined for this cause by the team"; "no hazardous or operability consequences identified for this cause by the team")?				
Safeguards	Do safeguards include the performance of equipment, human interaction, and combinations of these which address supporting causes for incidents or identified cases (see also causes audit protocol performance questions above)?				
	Are safeguards applicable and capable to the section of the process under evaluation (e.g., a fire monitor is incapable of providing an adequate water stream that can reach the equipment under evaluation, or is blocked or impeded by other process equipment; sound alarms can not be heard in the process area due to high ambient noise)?				
	Are engineering or hardware safeguards functional within generally accepted measures of availability (a safeguard is functional within the time the process is operational or charged with highly hazardous materials—e.g., relief valves have not been tested since installation; phosgene detectors are not calibrated as required by the manufacturer)?				
	Are administrative controls/safeguards (e.g., management systems, procedures, practices, permits) assessed to be operational (e.g., permits exist, but are not used; refresher training is not provided at set intervals)?				
	Safeguards are not compromised by the scenario cause or consequences (e.g., a level alarm low is listed for a malfunction of the level control from which it derives its signal)?				
	Are safeguards not malfunctioning or failed for a common cause related to the scenario cause or consequences (e.g., a large scale fire within the plant destroys cable trays for controls for that section of the process)?				

Appendix A (*Continued*)

Area of concern	Performance protocol questions	Answer	Ranking	Exceptions	Recommendations
	Safeguards do not include items listed as recommendations within the same PHA (e.g., updates to procedures for highly specific lockout/tagout of certain types of equipment are listed as safeguards later in the PHA documentation)? Safeguards do not include items that are planned for installation or implementation (e.g., a deluge system planned for installation in late 2005 is included in a PHA conducted in early 2004)? Are safeguards specifically applicable to the cause and consequence(s) under consideration (e.g., the generic safeguard "training" is listed for a complex switchover between two reactors with toxic and pyrophoric catalyst residues, but no specific training is provided to operations and/or maintenance staff performing this function)?				

References

[1] K. Trevor, Trans. Inst. Chem. Eng. B 77 (B3) (1999) 109–116.
[2] N.J.S.A. 13:1K-19 et seq, Toxic Catastrophe Prevention Act.
[3] 29 CFR 1910.119 (e) Process Hazard Analysis.
[4] 40 CFR Part 68 Sec. 68.67 Process Hazard Analysis.
[5] OSHA CPL 2-2.45A CH-1, 1994.
[6] K. Trevor, Trans. Inst. Chem. Eng. B 80 (1) (1999) 3–8.
[7] K. Trevor, What Went Wrong? Case Histories of Process Plant Disasters, 3rd ed., Gulf Publishing Company, Houston, 1994.
[8] R.E. Sanders, Management of Change in Chemical Plants: Problems and Case Histories, Butterworths-Heinemann Ltd., Oxford, 1993.
[9] K. Trevor, Learning from Accidents, 2nd ed., Butterworths-Heinemann Ltd., Oxford, 1994.
[10] Instrumentation, Systems, and Automation Society, ANSI/ISA S84.01-1996, Application of Safety Instrumented Systems (SIS) for the Process Industry, Instrumentation, Systems, and Automation Society, Research Triangle Park, NC, 1996.
[11] American Petroleum Institute, API RP752 1995, Management of Hazard Associated with Location of Process Plant Buildings, American Petroleum Institute, Washington, DC, 1995.
[12] Summers, E. Angela, Bridging the safe automation gap, in: Proceedings of the 2001 Mary Kay O'Connor Process Safety Center Symposium, College Station, TX, October 30–31, 2001.
[13] United States Environmental Protection Agency, United States Occupational Safety and Health Administration, EPA/OSHA Joint Chemical Accident Investigation Report—Shell Chemical Company Deer Park, Texas, June 1998, pp. iv, 30, 31, 34.