AUDITING THE QUALITY OF PROCESS HAZARD ANALYSIS (PHA) STUDIES

A Thesis

by

FAISAL ABDULRAHMAN M. ALSHETHRY

Submitted to the Office of Graduate and Professional Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Chair of Committee,	M. Sam Mannan
Committee Members,	James C. Holste
	Mahmoud El-Halwagi
Head of Department,	M. Nazmul Karim

August 2017

Major Subject: Safety Engineering

ABSTRACT

The petrochemical industry is subject to various federal and local regulations and requirements that are challenging to meet and resource intensive. Time and human factors often lead to a “check box” mentality where requirements are fully complied with “on paper” with little or no emphases on quality of compliance. Occupational Safety and Health Administration’s (OSHA) Process Safety Management (PSM) requirements are often exposed to this “check box” mentality, especially the Process Hazard Analysis (PHA) element which is the engine that drives and affects the whole PSM program. Poor implementation of PHA affects mechanical integrity, operating procedures, training, and emergency response; and is considered a root cause of most major incidents. Unfortunately, poor quality PHAs are widespread, hard to identify and can be more dangerous than conducting no PHA at all since it may provide a false sense of safety. Unfortunately, existing literature as well as recognized and generally accepted good engineering practices (RAGAGEP) do not provide sufficient guidelines for assessing PHA quality. The guidelines proposed in this thesis help in properly auditing PHA studies by identifying traps and bad practices that most companies fall into when performing PHAs.

The resulting guidelines are developed based on detailed incident investigation reports where root causes included inadequate PHA performance. In addition, expert opinion expressed in published papers highlighting specific gaps in PHA performance,

and best practices of PHA implementation are utilized to identify common gaps and means for auditors to acquire evidence of reduced quality.

The biggest contributors to the reduction of PHA quality include failing to consider lessons learned previous incidents, reduced quality of PHA inputs such as process safety information, competence of the PHA team members in their respective fields and time allocated for them to complete the PHA, accounting for human factors when relying on operator action to return the process to its safe state, as well as failing to perform PHAs for non-routine mode of operations. These contributors and others are discussed thoroughly on how they affect quality of PHAs and how auditors would obtain evidence that supports lack of quality.

The proposed guidelines compiled in Appendix A should be used as part of an overall PSM audit. Using these guidelines by themselves would result in an incomplete assessment of the PHA. This is due to the fact that effective PHA element implementation depends on several other PSM elements that are considered foundational to PHA implementation quality. Spending the time and money to perform an audit utilizing these guidelines should be seen as a positive investment by facility's executives as it will unquestionably assist in saving a lot of money and ensure business continuity by closing the gaps in PHA performance and reducing the chance for the "check box" mentality, thus making their facilities, employees, community and assets safer.

ACKNOWLEDGEMENTS

I would like to thank my advisor and committee chair, Dr. Sam Mannan for allowing me to pursue the topic of this thesis. Tackling the problem presented in this thesis was one of the goals of joining the Mary Kay O'Connor Process Safety Center as this problem was a challenge I faced in my professional career with no satisfying results. Dr. Mannan's guidance and continuous support greatly assisted me in finding the answers I sought which are presented in this research. I would also like to thank my committee members, Dr. Mahmoud El-Halwagi, and Dr. James Holste for their guidance and support throughout the course of this research.

Thanks also go to my friends and colleagues and the department faculty and staff for making my time at Texas A&M University a great experience.

Finally and most importantly, I want to thank my wife for her encouragement, patience and love.

CONTRIBUTORS AND FUNDING SOURCES

This work was supervised by a thesis committee consisting of Professor M. Sam Mannan [advisor and chair] of the Department of Chemical Engineering and Professor Mahmoud El-Halwagi of the Department of Chemical Engineering and Professor James C. Holste of the Department of Chemical Engineering. All work for the dissertation was completed independently by the student.

This work was made possible by the Saudi Arabian Oil Company (Saudi Aramco), specifically the sponsorship of the Loss Prevention and Career Development Departments.

TABLE OF CONTENTS

Page

LIST OF FIGURES

Page

LIST OF TABLES

Page

1. INTRODUCTION

The petrochemical industry is subject to various with federal and local regulations and requirements that are challenging to meet and resource intensive. Time and human factors often lead to a "check box" mentality where requirements are fully complied with "on paper" with little or no emphases on quality of compliance [7]. Occupational Safety and Health Administration's (OSHA) Process Safety Management (PSM) requirements are often exposed to this "check box" mentality, especially the Process Hazard Analysis (PHA) element which is the engine that drives and affects the whole PSM program [6]. Poor implementation of PHA affects mechanical integrity, operating procedures, training, and emergency response [6] (see Figure 1); and is considered a root cause of most major incidents. Unfortunately, poor quality PHAs are widespread, hard to identify and can be more dangerous than conducting no PHA at all since it may provide a false sense of safety. A classic example is the BP Texas City incident where the Management of Change (MOC) team were not trained on how to perform a building siting analysis as part of the MOC PHA procedure [8]. In addition, the PHA conducted on the isomerization unit indicated that a tower overfill scenario is not credible [8], which resulted in poor maintenance of critical tower level detectors. In this case, safety requirements were followed on paper. However, quality of implementation was poor. Unfortunately, existing literature as well as recognized and generally accepted good engineering practices (RAGAGEP) do not provide sufficient guidelines for assessing PHA quality. The purpose of this thesis is to develop guidelines

to properly audit PHA exercises which would help in identifying traps and bad practices that most companies fall into when performing PHAs.

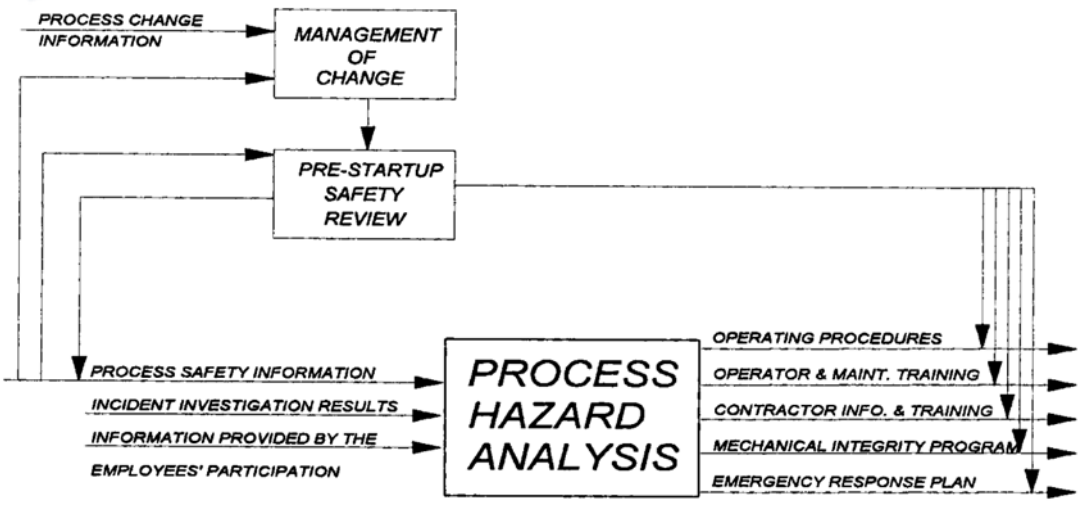

Figure 1: Effects of PHA on PSM Elements. Reprinted from [6].

2. OBJECTIVES

The purpose of this thesis is to develop guidelines to thoroughly audit the PHA exercises, which would help in identifying traps and bad practices that most companies fall into when performing PHAs. The audit guidelines developed would be in a survey format with questions that focus on assessing the quality of the PHA reports and auditing the implementation of OSHA's PSM PHA element. The guidelines developed in this thesis should be used as part of an overall PSM audit. Using these guidelines by themselves would result in an incomplete assessment of the PHA. This is due to the fact that PHA element implementation depends on several other PHA elements that are considered foundational to the PHA implementation quality. A typical survey would include questions, comments/findings, score, and weight reflecting the effect each question has on the overall PHA element implementation performance.

3. MAJOR INCIDENTS THAT UNDERSCORE THE PROBLEM

The OSHA PSM standard has been mandated since 1992 [9]. Yet, insufficient compliance can still be witnessed and incidents with PHA-related issues still continue to occur. 21 out of the 46 (43%) detailed investigation reports, published by the U.S. Chemical Safety and Hazard Investigation Board (CSB) between 1998 and 2008, had questionable issues pertaining to PHAs [10]. Out of these 21 cases, nine (43%) had no PHA conducted at all, eight (38%) did not incorporate lessons learned from previous incidents in their PHAs, six (21%) cases had PHA recommendations that were not implemented, four (19%) had PHAs which prescribed inadequate safeguards, four (19%) did not identify all hazardous scenarios, three (14%) had PHAs which did not consider facility siting, three (14%) did misestimated scaled up risk from lab experiments, and three others had various other PHA related issues [10].

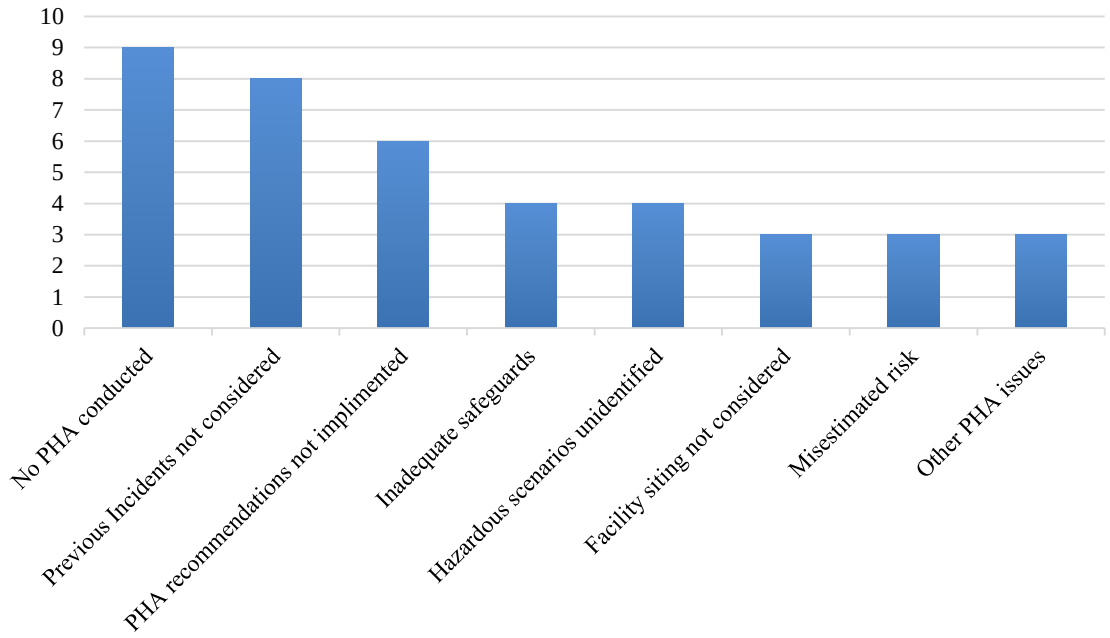

Figure 2: PHA Issues identified in CSB investigation reports published from 1998 to 2008. Adapted from [10].

As can be concluded from Figure 2, almost half of the major incidents in industry most probably had PHA-related root causes identified in their investigation reports. For example, the DPC Enterprises incident (at Glendale, Arizona in 2003), which resulted in the exposure of 11 police officers and five community residents to chlorine as well as the complete evacuation of a 1.5 square-mile-area in covering Glendale and Phoenix, had several PHA deficiencies. The CSB investigation revealed that the PHAs conducted did not identify over-chlorination of the scrubber system as a credible failure scenario (see Figure 3). As a result, no adequate safeguards were specified and DPC relied on administrative controls only to reduce the likelihood of the over-chlorination scenario which was a well-known scenario to facility operators. [4]

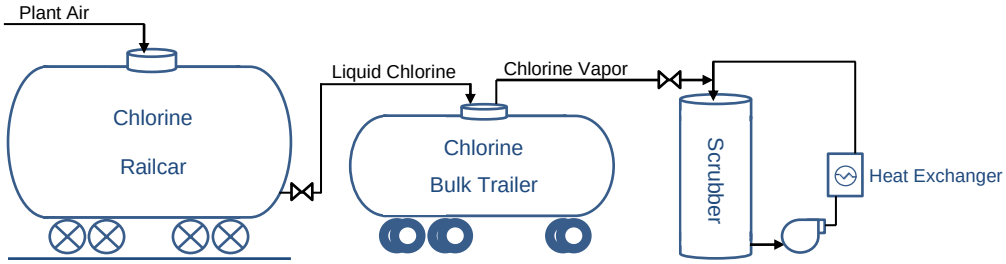

Figure 3: Chlorine Loading and Scrubber System at DPC. Adapted from [4].

Another example is the incident that occurred at Honeywell International, Inc. (Honeywell) plant in Baton Rouge, Louisiana. The accidental chlorine gas release led to the injury of seven employees and a shelter-in-place advisory notification to the residents living within a half mile radius. The CSB investigation revealed that a tube, in the shell and tube type cooler, leaked into the chlorine cooling system, damaging the pump since it was not designed for handling chlorine. The damage to the pump led to the release of chlorine to the atmosphere (see Figure 4). The investigation identified inadequate PHA implementation as one of the main root causes of the incident. The PHA conducted did not consider the chlorine cooling system since it was considered a utility/support system, missing the opportunity to identify such a scenario. As a result, only generic safeguards were prescribed such as “design”, “inspection”, and “testing”. [5]

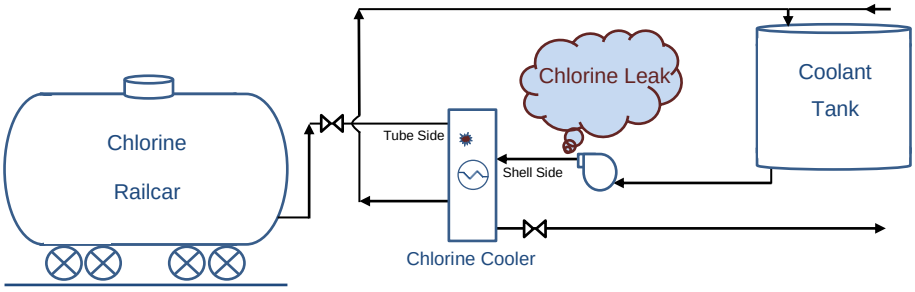

Figure 4: Chlorine Loading and Cooling System at Honeywell. Adapted from [5].

A more recent example is the incident that occurred at Williams Geismar Olefins Plant in Geismar, Louisiana in 2013. The overpressure of a standby reboiler (heat exchanger) for the propylene fractionator column caused a boiling liquid expanding vapor explosion (BLEVE), which led to the fatality of two employees and the injury of 167 others. The CSB investigation revealed that the reboiler's propane feed and discharge valves were isolated, which led to the lack of protection needed from the column's pressure relief valve. The steam feed valve to the reboiler was opened causing the temperature and pressure of the trapped propane to increase substantially causing the BLEVE (see Figure 5). The investigation identified inadequate PHA implementation as one of the main root causes of the incident. The PHA conducted did not prescribe adequate safeguards for non-routine mode of operation for the reboiler. In addition, the prescribed safeguard (which was locking the propane discharge valve open) was never implemented for the damaged reboiler even though it was indicated to be completed on paper. These examples and many others underscore the importance of ensuring that PHAs are properly implemented.

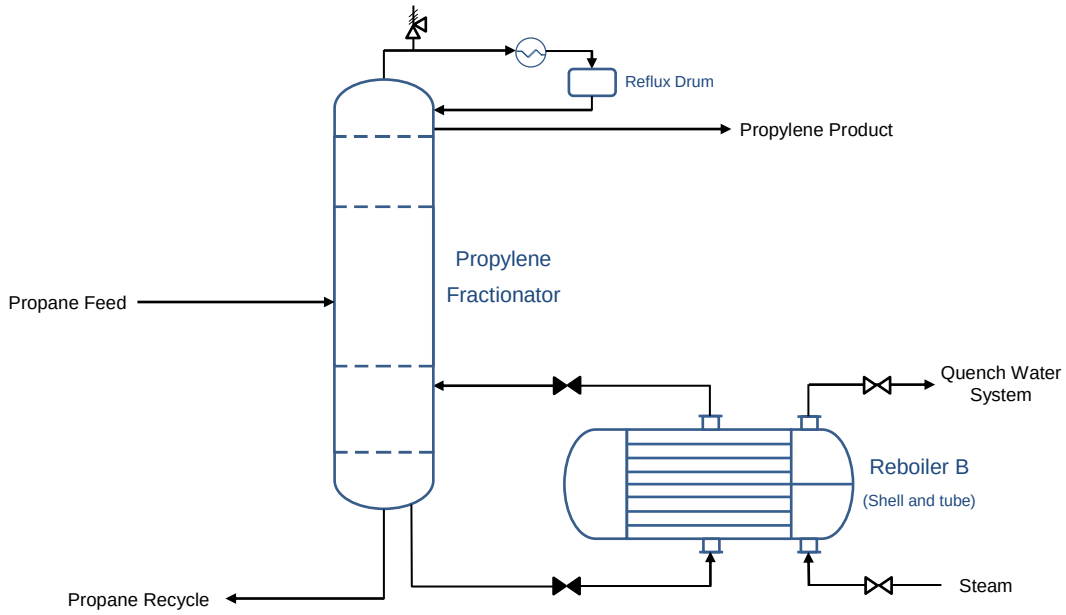

Figure 5: Propylene fractionator at Williams. Adapted from [3].

This thesis will utilize the lessons learned from the detailed incident investigation reports published by CSB to fortify the proposed PHA auditing guidelines later produced in this thesis. It is true that there are several incident databases available to the public. However, detailed incident reports are limited as most databases do not include detailed incident investigation reports that dig deep enough to identify PHA-related issues. Even the ones that had incident investigation reports, the quality of these reports is quite often questionable. Excellent reports do exist, but they are not often shared, sometimes even within the company, due to legal notifications and liability issues. Perhaps, this is part of the reason why we still continue to make the same mistakes. The reports by the CSB are the exception, not only because they were created by qualified teams, but also because the team was unbiased and independent. In addition, major incidents that caught the

attention of the media such as Bhopal and Piper Alpha will also have quality detailed incident investigation reports and could provide some insights into how to audit the quality of PHAs. By taking these facts into consideration, this thesis focuses on incident reports produced by the CSB and major incidents that caught the attention of extensive studies and investigation such as Bhopal and Piper Alpha.

4. METHODOLOGY

The survey questions will be formed based on the information gathered from:

1) Detailed incident investigation reports where root causes include inadequate PHA performance,
2) Expert opinion expressed in published papers about specific aspects related to PHA auditing,
3) And literature review consisting of best practices of PHA implementation and PHA element execution.

5. LITERATURE REVIEW

Literature available which enable auditors to assess the quality of risk assessments are surprisingly scarce. Perhaps due to the huge amount of regulations that govern petrochemical plants safety and the inherent conflict between short-term financial goals with safety goals, most of the industry reacts to most safety enhancement endeavors by implementing only the bare minimum. Safety professionals are often faced by that most common of phrases "Is it mandatory?; if it is, then show me the regulation that mandates it" without even considering the potential of safety enhancements or long-term financial goals which often coincide. As Dr. Trevor Kletz once said:

"There's an old saying that if you think safety is expensive, try an accident. Accidents cost a lot of money. And, not only in damage to plant and in claims for injury, but also in the loss of the company's reputation."

As a result of this constant conflict between safety and short-term financial goals, most literature available contains guidelines backed up by existing regulations. The issue is that most regulations are reactive, governmental, and/or legislative responses to major incidents or catastrophes. Thus, these regulations are not always comprehensive. Moderate or minor incidents do not always trigger a new regulation to control the risk, even if it had the potential to have much higher consequences. Another reason why regulations may not always be comprehensive is that creating a regulation requires enormous resources to ensure proper monitoring and enforcement, especially when a regulation applies to a whole country with small and big businesses. So, it may not

always be practical to create a regulation. Therefore, the majority of PHA auditing knowhow exists in the form of company internal processes/procedures, or is embedded into the minds of experienced employees who do not always have the time to document or publish their knowledge. In addition, due to the qualitative nature of most of the available risk assessment techniques, PHAs prove to be often elusive and difficult to audit.

A good example of risk assessment auditing guidelines resource which is based on existing regulations is the *Guidelines for Auditing PSM Systems* developed by the Center for Chemical Process Safety (CCPS). Chapter 10, which contains guidelines on auditing *Hazard Identification and Risk Analysis* studies, mostly includes guidelines based on federal regulations such as OSHA and EPA regulations for PSM and RMP, respectively. Their developed guidelines do also incorporate state regulations such as New Jersey, California, and Delaware as well. However, they are not comprehensive enough and they do not focus on quality of implementation of PHA. They do give guidelines for auditing the overall performance of the PHA element implementation. For example, this resource does not adequately address the experience validation requirements of PHA team members and other sources of variance such as the inaccurate assessment of risk.

Another resource identified was a paper written by Thomas R. Moss, the managing director of RM Consultants Ltd. (RMC) at the time of the paper. In his paper titled, "*Auditing Offshore Safety Risk Assessments*," he created an audit process based on

his review of the RMC's internal quality-assurance procedures. His proposed and later tested process was as follows [12]:

1) The PHAs are reviewed to determine the scope and objectives to evaluate the methodology, assumptions and data used.
2) Previous relevant incidents in the offshore incident databases are reviewed to determine completeness of input data used by the PHA team.
3) PHA records as well as resulting procedures and recommendations are reviewed to verify if hazardous simulations operations (SIMOPS) are taken into consideration.
4) The PHA is reviewed in detail to ensure that data, assumptions, methodology, calculations, models, and consequence/probability assessments are complete and accurate.
5) The adequacy of safeguards proposed during SIMOPS is reviewed.
6) The results of the audit are discussed and areas of uncertainty are highlighted.

As can be seen from Moss's proposed process, it is limited to the work flow of auditing offshore facilities, yet it can be applied to onshore facilities as well. However, his procedure is not detailed enough to help identify the traps and bad practices which most facilities fall into when performing PHAs, nor does it highlight telltale signs that assist the auditor in identifying systematic issues in the PHA element. Moss' process also precedes the introduction of the PSM regulation.

Other available literature focus on the best practices, techniques, and formats of auditing SMS systems which are outside the focus of this thesis. However, there are

several other resources containing guidelines and best practices for conducting PHAs such as Frank Crawley and Brian Tyler's book titled "*HAZOP: Guide to Best Practices*" and many other books developed by the Center for Chemical Process Safety (CCPS) such as the one titled "*Guidelines for Risk Based Process Safety*". These resources can be specific to a certain PHA methodology or general to most used ones. These guidelines are utilized in sections 6 and 7 below to develop PHA auditing guidelines in this thesis.

6. SOURCES OF VARIANCE

Sources of variance in quality of PHAs are always the result of variance in PHA inputs, mainly process safety information, incident and near miss investigation results, as well as input provided by the PHA team members which is derived from their experience [6] (see Figure 1). Poor PHA inputs can render the whole study invalid, lead to overdesigning or under designing the process. All these consequences lead to financial ramifications such as redoing PHA studies, paying extra for overdesigned safe guards acquisition, installation, and maintenance; incident damage when hazard scenarios are missed; interruption in business continuity; environmental remediation; and/or lawsuits, among others. Therefore, minimizing the input variance and increasing the input quality is essential to the overall quality of a PHA and the overall safety and business continuity.

6.1. Incomplete List of PHA Input Sources

The first step is to ensure that all information is incorporated in a PHA. To some, this step might seem obvious and wonder why/how a lot of companies still fall short of completing this very basic yet extremely important step. As previously mentioned 38% of incidents investigated by the CSB between 1998 and 2008 failed to include lessons learned from previous incidents, even though it is an OSHA requirement [10]. The issue might lie in the fact that OSHA is not specific on the scope of incidents that needs to be included in the analyses during a PHA. For example, should the analysis include incidents that occurred only within the facility? Or should it include other incidents that

occurred at other facilities within the company with similar processes? Should even consider incidents that occurred in other companies? OSHA does not specify [10]. Kaszniak's review revealed that some PHAs failed to include previous incidents within the same process (*i.e.,* BP Amoco Polymers), some failed to includes ones that occurred at similar processes in the same facility (*e.g.,* BP Texas City), others failed to include incidents that occurred at similar processes at other facilities within the same company (*e.g.,* Formosa, IL).

In addition, most experts agree that most companies are not 100% compliant in implementing the PSM regulations. For example, depending on the safety culture, some may not report all incidents or near-misses if that might get them into trouble. Due to company culture, process upsets might not be considered as near-misses. Time pressure and lack of manpower might make some people ignore near-miss investigations all together, missing the opportunity to identify some residual risk that went unidentified in previous PHAs. Yet, evidence of these incidents or near-misses might still be available in the form of emergency maintenance work orders. Reviewing emergency work orders is also helpful in giving the PHA team an idea about some the actual equipment failure frequency when evaluating risk. That is why emergency maintenance work orders should always be part of a PHA input, even if it might seem redundant.

The same can be said about corrosion inspection worksheets. They also may indicate the existence of a previous incident. However, they do also identify nodes or types of equipment prone to corrosion or deterioration. In addition, they can help in prioritizing nodes or parts of a plant that has a higher risk of failure from corrosion.

Again, redundancy of information helps reduce the size of gaps in terms of information completeness.

Another example is Management of Change (MOC). It is no surprise to most safety professionals that MOC implementation has not been perfect in many companies. For example, the level of review determined for the MOC was not sufficient and the impact on the health and safety might have been underestimated. The risk assessment of a complex change might have been reviewed by an unqualified or incomplete team. In fact, many of the issues that affect the quality of a PHA affect MOCs as well. So, there might be some residual risk unidentified or underestimated. Therefore, it is crucial to include MOCs as part of a PHA revalidation exercise even if it might seem redundant.

Another important source of information is pre-startup safety reviews action items. Poor safety culture can lead to plant startups without completing all critical action items. Inspectors may often put a lot of time and effort in finding issues like standards/regulations exceptions, issues requiring further studies, and other team recommendations [11]. Findings may also include incomplete transfer of process knowledge (*e.g.,* missing or poor PSI, or training for operators/maintenance personnel). These findings can affect the integrity of the design, and reliability of safeguards. Therefore, this valuable source of information should be considered in PHAs.

Drill critique meetings might also contain significant findings that might affect the outcome of PHAs. Findings such as response time, fire truck access, and manual isolation valve access comes to mind and needs to be considered during a PHA revalidation.

In addition, the chemical material inventory should always be considered when performing a PHA when storage warehouses are part of the facility. The amount and reactivity of chemicals stored in these storage facilities could have a tremendous effect on the resulting risk. China's Tianjin incident comes to mind where a chemical warehouse fire led to explosions equivalent to 24 tons of TNT, destroyed more than 5,500 cars [15], injured more than 700 people [16], killed 173, and demolished more than 300 homes [17]. This is not an isolated case. In China alone, similar incidents led to more than 68,000 deaths in 2014 as reported by the Chinese government [16]. So, not only can similar incidents have severe consequences, but high frequency as well, so the risk is higher than expected. During PHA revalidations, it is essential to ensure that the PHA considered the maximum inventory of chemicals that had been stored in previous years and any future plan of increase. Due to low perception of risk of storage facilities, this source of information could be easily overlooked.

As a result, the complete list of PHA inputs that should be considered and documented during a PHA should include the following at a minimum:

1) Piping and Instrumentation Diagrams (P&IDs) [18]
2) Process Flow Diagrams (PFDs) with material/energy balances [18]
3) Layout drawings [18]

4) Equipment specifications sheets [18]
5) Process description [19]
6) Maximum chemical inventory in storage facilities.
7) Previous PHA* [19]
8) Incident and near-miss investigation reports* [20]
9) Emergency work orders*
10) Inspection worksheets*
11) MOCs* [20]
12) Emergency Drill critiques* [20]
13) Pre-startup safety reviews action items.*

* Required only during PHA revalidation.

6.2. Quality of PHA Inputs

The quality and comprehensiveness of the PSI is not only crucial to obtain a quality PHA but also for the overall design, training, operation, maintenance, and MOC of the whole facility. The Process Safety Information (PSI) element is one of the foundational elements affecting the whole PSM system [21]. Therefore, it is imperative that this element is thoroughly audited as part of the whole PHA quality audit. Usually, due to time and manpower constraints, auditors are only able to verify that P&IDs used in the PHA were up-to-date and as-built at the time of the PHA report. This is usually the case when a PHA is audited separately and not as part of a complete PSM audit. However, due to the criticality of the PSI element to the quality of the PHA, it should be

audited exhaustively. The same could be said to some extent about the MOC, and incident investigation elements. Since they would be considered inputs to the PHA, they should have their own full blown audits and the results should be used to revise the overall score of PHA element. For example, if the incident investigation element was audited and scored only 20% implementation, it stands to reason that the overall score of the PHA element cannot be 100% or anything close to 100%. A similar argument can be made about the PSI element where gaps and/or inaccuracies were identified; a low audit score in PSI should automatically affect the score of the PHA element because of the inherent interconnectedness.

Some audit guidelines can be recommended in this section. However, it is not advised to use them in lieu of a comprehensive audit of other relevant elements such as the PSI and incident investigation. Having a CAD drafter as part of audit team can be huge asset to ensure comprehensiveness of the review.

1) Check pre-startup safety reviews for any pending action items or closed items regarding PSI and verify closure through field verification and/or interviews.
2) Check previous PHAs for comments regarding lack or inaccuracy of PSI.
3) Interview PHA team members and inquire about any missing information or inaccuracies identified during the PHA [20].
4) Interview process engineers, plant operators, and maintenance engineers and inquire about any missing information or inaccuracies they encounter in PSI.
5) Check MOCs which needed PSI updates and verify that information were updated prior to the PHA.

6) The auditor should review the incident databases of similar facilities; especially other facilities belonging to the same company and verify if they had been incorporated in the PHA. If several facilities exist under the same company, sometime they do operate in silos and lessons learned from other facilities are not communicated or implemented.
7) Verify that the PSK system exist that ensures that PSI are complete, accurate, and up-to-date and captures any changes to the PSI [11].
8) Verify that an MOC system exist that meets the requirements of the PSM.
9) Interview personnel and inquire about any recent changes to the process and verify that all these changes went through the MOC process and associated PSI were updated as necessary.
10) Reduce overall score of PHA implementation if MOC, PSI, or incident investigation elements audit scores are below 80%.
11) Review any previous internal/external or third party audit reports to find any relevant issues.

6.3. Inaccurate Assessment of Risk

One of the greatest strengths of a PHA is its systematic structure which aids the team in determining an initiating event that has the potential to create an incident (credible scenario). However, if the PHA is qualitative in nature (*e.g.,* HAZOP), the task of determining the risk of a credible scenario becomes susceptible to inaccuracy, inconsistency and a source of disagreement between team members. Utilizing accurate

incident frequency figures and consequence estimation will heavily influence the overall assessment of risk for a potential incident and the level of safeguards required to mitigate it. Factors that may influence the accuracy of risk estimation are discussed in the sections 6.3.1, 6.3.2 and 6.3.3.

6.3.1. Inaccurate Assessment of Frequency

There are many sources for frequency data. Some PHA teams utilize historical records or even generic failure frequency databases to determine the overall risk of the identified hazards. Some might rely solely on their experience to determine the frequency. This major source of variance can result in gross underestimation or overestimation of risk.

6.3.1.1. Historical Data

As per the Guidelines for Chemical Process Quantitative Risk Analysis (CPQRA) developed by the Center for Chemical Process Safety, historical records should only be utilized to determine the frequency of an initiating event if the data is derived from sufficiently similar facilities [22]. In addition, if the applications were deemed similar, historical data should also be reviewed to determine similarity of conditions like fluid aggressiveness, temperature, pressure, and vibration [23].

6.3.1.2. Generic Failure Data

It is easy to understand why some risk assessors use generic failure data in their risk assessments. However, there are issues with these generic databases that have to be taken into consideration when evaluating risks. Most of the generic failure rate databases are outdated [24]. Some of the failure data resources were originally published in the

1970s [25]. Updated manufacturing standards, changes in maintenance and operation practices, and the added number of failures in the last 50 years could have changed the average frequency of failure used in these databases [24]. It is difficult to ascertain that these generic frequency values are still representative of the current equipment failure trends. In addition, some studies reveal that real failure rates tend to be higher than some failure databases such as the Purple book [24].

In addition, it may be necessary to adjust these data based on the differences in operational and environmental conditions [25]. Unfortunately, not all generic databases define the operation and environmental conditions of the collected data [25].

Yet, generic data can be one of the few options especially during the initial design. Reviewing generic failure databases during every PHA is impractical and takes a lot of time and experience. In addition, members of the team may spend a significant amount of time arguing about the failure rate values. So, it is expected that large companies, especially the ones that have huge resources and similar process facilities, develop their own incident databases. At least, generic databases should be reviewed, complied, and modified to produce an internal failure rate handbook that suits the company's operational and environmental conditions. Small companies should consider the latter route as well especially since over/under-estimating the risk could lead to huge financial burdens. However, reviewing generic data when required for a PHA could prove more practical for smaller companies. Both small and large companies are expected to revalidate these failure estimates during PHA revalidation.

6.3.2. Inaccurate Assessment of Consequences

Initially during a PHA study, the team must consider the worst-case credible consequence for a given scenario without considering the effects of any existing safeguard/s [20].Some PHA teams fall into the trap of assessing the consequence of a given scenario while considering the effects of safeguards in place. For example, a team might not consider overpressure damage of a vessel as a worst-case consequence if they have considered the installed relief valve, which gives them a false risk estimate. This often happens with inexperienced teams while performing revalidation PHA studies. The auditor must validate that the initial risk assessment of identified scenarios have been considered without considering safeguards [20].

6.3.3. Experience

Relying on one's experience has its limitations, especially when approximating the likelihood of rare initiating events unless the person's experience covered a sufficient number of plants with similar design, equipment, and applications which is usually rare. So even if the team had a collectively long experience, they might still dismiss the probability of rare events happening entirely. So it is vital that the team use historical and generic data rather than depending on their own experience for extremely rare events. The team's experience is more useful in reviewing generic data and estimating the likelihood of events if no previous data exist for incidents that are considered frequent. Generally, the more often the incident occurs the more accurate the experienced team's estimate can be in estimating the probability and consequence of an initiating event, see Figure 6 below.

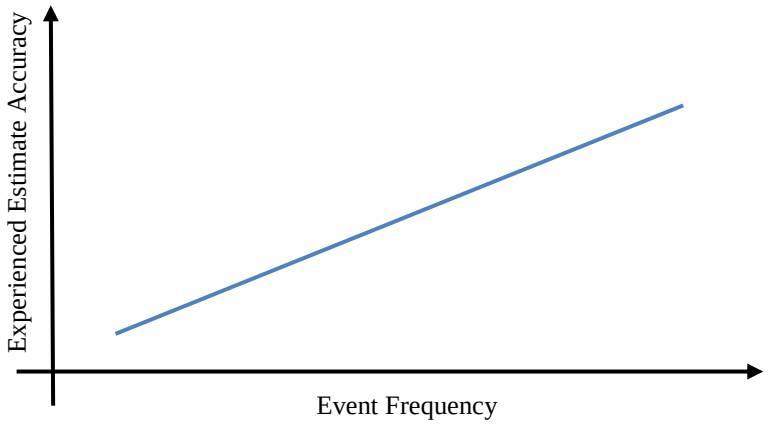

Figure 6: Event frequency versus experienced estimate accuracy

Therefore, if the auditor finds out that the team relied on their experience to estimate the risk of most rare events without relying on any generic or historical data, then quality of their estimates should be deemed inadequate.

6.4. Risk Acceptance Criteria

It is essential that the risk acceptance criteria and tools used to evaluate risk against them are well defined and established prior to performing a PHA. Some of the less than adequate practices seen in the PHA field include the following:

1) Some facilities do not provide any risk acceptance criteria or tools to the PHA team, asking them only to identify hazardous initiating events and safeguards. This is grossly inadequate unless the initiating events identified and safe guards proposed by the team are evaluated later by a competent risk assessment team against risk acceptance criteria. This approach has some advantages and

disadvantages. It can lead to increased focus and efficiency on what the team does best, identifying initiating events. In most cases, not all team members have adequate experience/knowledge in assessing risk against a defined criteria, which may lead to disagreement and long discussions that may delay or reduce the accuracy of risk assessment, especially if the tool used is qualitative (*e.g.*, risk matrix). However, this approach is incomplete by itself and has to be supplemented by a separate risk assessment exercise by a competent team.

2) Some facilities do not provide any risk acceptance criteria or tools to the PHA team and asks them to use their own (if PHA is conducted by a contractor) or use one from the internet. Unfortunately, this practice is common and has many issues that makes it a completely unacceptable practice, chief among which:

   (a) This practice leads to a high probability of variability in assessment of risk in each PHA study. An initiating event might be deemed acceptable in one tool but unacceptable in another. A safeguard prescribed might also be deemed adequate in one tool but inadequate in another.

   (b) This practice increases the responsibility on the PHA team and dilutes the responsibility of facility management to develop their risk acceptance criteria. Facility management should develop risk acceptance criteria that suit their risk acceptance profile and they should be aware of the consequences of the criteria they decide on, especially since they have a significant leadership role in dealing directly with the consequences of an incident.

Therefore, it is essential for facility management to develop/approve proper risk acceptance criteria that ensures profitability without compromising the environment and human life. The risk tolerance criteria should include at least the following [26]:

1) Maximum allowable risk per initiating event.
2) Maximum allowable risk per node or area.

The defined risk tolerance criteria should include all relevant types of risk (*e.g.*, human life, assets, health, environment), and differentiate between voluntary and involuntary risk (employee risk vs. community risk). The maximum allowable risk defined for the community or facility surroundings should be much more conservative when compared to allowable employee risk. The decided upon risk tolerance criteria should be approved and signed by facility management to ensure their involvement, commitment, and ownership. The auditor should also make sure that the maximum allowable risk threshold defined is reasonable. As a general rule, an employee should not be exposed to more risk at work than voluntary risk taken during activities off work [27]. For societal risk, the risk is considered generally acceptable by the public if the risk of fatality is less than 10^{-6} fatality per person/year, which is the risk of fatal injury from natural hazards [28]. The risk is considered generally unacceptable to the public if the risk of fatality is higher than 10^{-3} fatality per person/year, which is the risk of fatal injury from disease [28]. So, usually the maximum allowable societal risk is between 10^{-6} and 10^{-3} fatality per person/year. UK's Health and Safety Executive stipulates that the risk of death from an industrial incident to the public should not exceed 50 fatalities in 5,000 years per annum [29].

Facility management is also expected to assign the responsibility of designing and customizing their risk assessment tools (*e.g.*, risk matrix) to a competent team and review/approve them. The design goals of the risk assessment tool should include the following:

1) Limit subjectivity.
2) Reduce user errors.
3) Assist user/s in accurately assessing the risk of an initiating event and comparing it to the risk acceptance criteria.
4) Assist user/s in ranking risks in order to prioritize proposed PHA recommendation implementation.
5) Assist user/s in accurately assessing the effect of proposed safeguards on identified hazardous scenarios and its adequacy to reduce the risk to ALARP.

If the tool used in the PHA was found to deviate from these design goals, the tool should be deemed substandard. For example, signs of a less than adequate risk matrix include:

1) Descriptions of consequence categories do not include either loss of life, financial loss, or environmental loss. The team should consider loss in all consequence types.
2) Quantitative descriptions are not available to define probability and consequence categories. Using quantitative descriptions, such as anchor points and ranges, to

describe a probability or consequence category would greatly assist in reducing subjectivity and bias among the PHA team [30].

3) Resolution of matrix is too small (*e.g.,* 3x3) and does not cover the range of credible scenario probability and consequence. The resolution of the risk matrix should consider the range of consequence (from the maximum to the minimum credible scenario) and probability (range relevant to the PHA) [30].
4) Ranges of frequency and consequence are not adequate. For example, major incidents consequences should range from loss time injury to multiple fatalities. For likelihood, the range should be from 1 per year to at least 1/10000 per year. [1]
5) Coloring of risk matrix is not defined. Each color should be clearly defined in terms of risk acceptability, and the ALARP region should be identified [30].
6) Risk acceptance criteria are not defined quantitatively. Reliance on coloring only in a risk matrix will lead to risk evaluation ties and prevent the team from properly ranking hazardous scenarios [30].

6.5. Initiation Criteria for more Quantitative Methodologies

At the other end of the spectrum, establishing criteria that triggers the need for more quantitative risk assessment methodologies is even more important than deciding on the risk acceptance criteria. When the potential consequences are huge, methodologies that lack accuracy are unacceptable because small errors still translate to significant consequences. Therefore, it is essential that corporate requirements stipulate

the initiation criteria for more quantitative risk assessment methodologies when performing a PHA. Examples for such triggers can be estimated consequences (*e.g.*, major injury, fatality, societal injury, environmental toxic release), risk, complexity of the process, type of material/chemical processed, or a combination [11]. In addition, corporate requirements should stipulate the methodologies accepted for the established triggers and the level of detail required [11]. For example, if during the PHA a hazardous scenario identified was estimated to cause major injuries to the surrounding community, the team would have to perform a separate QRA study for that specific scenario. This would help in accurately estimating the risk and in deciding on adequate safeguards that would reduce the likelihood of the scenario and reduce the risk to an acceptable level.

The auditor should first ensure that corporate requirements stipulate the initiation criteria for more quantitative risk assessment methodologies while performing PHAs, and the accepted methodologies suitable for the specific initiation criterion. The auditor should then verify implementation of these requirements in the PHA. It is not uncommon that the PHA team specifies a recommendation to perform a more quantitative methodology (*e.g.,* QRA, LOPA) for a specific scenario instead of performing the methodology themselves during the PHA. This can be due to time factors, and lack of qualifications required to perform such studies due to its complexity. This is acceptable. However, it is not acceptable that the recommendation is closed by performing the quantitative study only. The auditor should ensure that these types of recommendations are only closed if the specified recommendations in the resulting quantitative study are performed, and not by merely conducting the study. This is

essential because of two important factors. PHA recommendations are usually high level items that are tracked by upper management and given high priority. Closing the recommendation to perform additional studies by merely performing the study may lead to the resulting recommendations of the additional study being untracked or having lower priority.

6.6. Inaccurate Assessment of Safeguards Effect

One of the crucial steps of a HAZOP study is the reevaluation of risk with existing safeguards or ones that are recommended by the team. Several HAZOP teams skip this step entirely due to the time consuming discussions it takes for the team to agree on the effects. Yet without performing this step, the team cannot determine or demonstrate whether the introduced or existing safeguards are sufficient to reduce the risk of the hazard identified to the ALARP region in the risk matrix. Sometimes two, three or even more safeguards are needed to mitigate a hazard.

In addition, an inexperienced team could introduce invalid safeguards. Examples of invalid safeguards are the following [18]:

1) A safeguard that requires a rushed operator intervention unfeasible by the operator due to a lack of time or inaccessibility (*e.g.*, isolation valve located very close to a leak/fire, or isolation valve which requires a scaffold to access);
2) "Operator Awareness;"
3) "Never had a problem with it to-date;"

4) Using a vessel sight glass with a media that causes fouling of glass, making it difficult to determine the true level;
5) Using a component from the same failed loop/system as a safe guard.

Furthermore, some may inaccurately reevaluate the risk with proposed/existing safeguards. One of the most common signs which reveal lack of knowledge in risk assessment is the reduction of risk in both the probability and consequence axes when evaluating the effect of a safeguard. Risk is rarely reduced in both probability and consequence [31].A safeguard such as a level alarm will reduce the likelihood, not the consequence. A dike constructed to limit the size of spillage area would reduce the consequence, not the probability. If inaccurate assessment of safeguards exists throughout the report, this would be a clear sign that the team is not fully competent. Therefore, even if the team/leader had substantial evidence of training and long experience, misestimating the effect of safeguards on risk is a clear sign that they still lack some of the necessary competence. Inaccurate assessment of safeguard effects on risk calls into question the credibility of the PHA significantly since it would most probably lead to substantial underestimation of real risk, which means that facility employees are less safe than they think they are.

6.6.1. Considering Operator Action

Operator actions are often relied on to reduce risk in two types of responses. The first is the initiation and implementation of emergency response activities if the process could not be controlled after exceeding the process safety parameters. The second

response is controlling the process to return it to its safe state after exceeding the process safety parameters. [32]

If the auditor notices that the PHA team did consider operator action to reduce risk, then he/she has to examine two factors:

1) The direction in which risk is reduced (*i.e.*, along the probability axis or the consequence axis).
2) The magnitude of reduction along the axis.

In the first type of response where the operator is relied on to initiate and implement emergency response activities, reduction is only expected in the consequence axis since loss of containment has already occurred at this stage and any possible reduction can be in the consequences (*e.g.*, community evacuation, cooling nearby structures, taking the injured to nearby medical facilities). The magnitude of reduction will depend on several factors (*e.g.*, type of consequence, resources, access, and communication) and should be looked at on a case-by-case basis. So, if auditors discover that the PHA team reduced risk on the probability axis on this type of response, quality score of PHA should be reduced.

In the second type of response where the operator is relied on to control the process and return it to its safe parameters after exceeding them, risk reduction should only be expected on the probability axis. As for the magnitude of reduction, the team should not reduce the probability of failure by more than a factor of 10 (10^{-1} probability of failure on demand), unless the team demonstrates that this particular operator response is reliable enough to exceed a reduction factor of 10 using Layer of Protection

Analysis (LOPA) or an equivalent methodology. In this analysis, the operator action has to meet the intended safety instrumented function (SIF) criteria. In addition, the analysis has to demonstrate that the operator can respond correctly to the alarm or process indication within the available time to return the process to a safe state. The probability of human error for each specific case has to be estimated using sound human error evaluation techniques such as the Technique for Human Error Rate Prediction (THERP) and the Accident Sequence Evaluation Program Human Reliability Analysis Procedure (ASEP HRA Procedure). In addition, environmental factors (*e.g.*, access, control area environment, control layout and quality of displays), stress factors (*e.g.,* shift schedules, response time pressure), and personnel factors (*e.g.*, experience, training) has to be considered in the analysis to reduce or increase/decrease the nominal human error rates estimated through the human error evaluation technique. Using a checklist similar to Table 1 could also help demonstrate adequacy of operator action for probability of failure reduction of more than a factor of 10. [32]

Table 1: Considering Human Factors for Operator Response. Adapted from [32].

Human Factor Related Engineering Issues	**Yes**	**No**	**N/A**
Can the operator action be completed within the required time for the SIF?			
Do operators have immediate access to a specific alarm response procedure?			
Do operators have sufficient training to complete the required response?			
Do operators receive periodic competency evaluations in the required action?			
Do operators have the physical ability required to complete the required SIF?			
Are operators provided with adequate controls and displays required to complete the required action?			
Does the operator action meet company requirements and procedures and is it suitable for the operator experience?			
If separate displays exist, do they provide consistent information?			
Does the display action match the actual control movement?			
Does the display provide direct, complete, concise, usable information with the required precision without the need for any extra steps?			
Is enough information provided to the operator about normal vs. abnormal conditions?			
Is there a clear indication for any display failure?			
Are displays and controls required for the SIF located/positioned within the reach limits of the operators?			
Are the alarms required to complete the SIF directly obvious to operators?			
Are the required alarms and controls grouped together for the operator?			
Does the design of the SIF controls ensure minimal human error?			
Is the SIS operator interface located in an area that ensures immediate operator attention?			
Does the display provided for the operator show that required actions are completed (*e.g.*, valve closed, pump turned off)?			

6.7. PHA Team Competence

Other major sources of variation and inaccuracy are the PHA team composition, expertise, and personal attributes. The PHA team can literally make or break the whole PHA. PHA team members with inadequate experience, meager qualifications, and poor personal attributes will fail to identify all credible hazard scenarios, inaccurately estimate risks for hazardous scenarios, and prescribe poor safeguards [33]. In fact, an incompetent team will identify more non-credible and more low consequence hazards when compared to a competent team [23]. In addition, an incomplete PHA team could lead to similar undesirable results. Some PHA experts insist that the whole PHA is redone if the team is not qualified [18]. Having an incomplete team would also lead to time delays and reduction in quality since the input of the non-present member would have to be added and reviewed by the team at a later stage. Therefore, it is crucial to assess the PHA team composition and competency.

6.7.1. OSHA Requirements for PHA Teams

In order to adequately audit the competency of a PHA team, it is vital to take into account the governmental requirements for the team. OSHA requires the PHA team leader to be [34]:

1) Knowledgeable in the PHA methodology;
2) Impartial to the plant or project;
3) Competent in managing the team.

OSHA also requires the team to have certain characteristics [34]:

1) Possess expertise in the following areas or disciplines: “process technology; process design; operating procedures and practices; alarms; emergency procedures; instrumentation; maintenance procedures, both routine and non-routine tasks, including how the tasks are authorized; procurement of parts and supplies; safety and health; and any other relevant subjects”;
2) Fully knowledgeable of current “standards, codes, specifications, and regulations applicable to the process being studied”;
3) Compatibility with each other and team leader;
4) Some members will be full-time members while others can be part-time members only.

In addition, a letter of interpretation of the PSM standard by OSHA indicated that an OSHA representative may elect to interview team members and/or leader and review their training history, whether formal, informal, or on-the-job training, to verify their competence based on the aforementioned requirements [35]. So, although the PSM standard does not specifically require training for the PHA team members and leader, OSHA certainly expects it.

6.7.2. PHA Team Composition

Verifying the completeness of the PHA team is essential to ensure thoroughness and effectiveness of the PHA team in identifying hazardous scenarios. Having members with different disciplines, expertise, perspectives, and opinions will contribute to a successful PHA analysis. There are many PHA guidelines that recommend different

team structures but most agree that there should be some core, and temporary team members in a team. It is crucial that the facility defines the minimum PHA team composition, and monitor implementation of these requirements. Of course, the team structure will depend on the type of industry and process being analyzed and whether it is a new project or a PHA revalidation of an existing process. Generally, the team composition would be as follows [13]:

1) PHA Leader;
2) Scribe;
3) Process Engineer or Designer;
4) Project Engineer;
5) Experienced Operator;
6) Safety, Health, Environment Expert (as required);
7) Instrument/control Engineer/Safety Instrumented Systems (SIS) Engineer (as required);
8) Mechanical/maintenance engineer knowledgeable in routine and non-routine maintenance procedures and tasks (as required)*;
9) Corrosion inspector/engineer representative (as required)*;
10) Instrument technician;*
11) Maintenance/mechanical technician;*
12) Other specialist/experts in other relevant disciplines (*e.g.*, process technology; operating procedures and practices; alarms; emergency procedures; procurement

of parts and supplies) as required (Process safety management guidelines for compliance. 1994 (Reprinted), 1994).

* Most PHA guidelines and best practices generally agree on the general composition of the PHA team. However, it is rare that you find a guideline that requires the presence of a corrosion inspector, maintenance/mechanical technician, and instrument technician. The value of these members is evident especially when validating the frequency of failure when using generic data if actual equipment failure data is not properly monitored or documented. They would also be able to shed some light on the reliability of proposed safeguards. For example, a corrosion inspector would know how often a leak would occur and what type of failure usually happen (*e.g.*, pinhole leak, hydrogen induced cracking, or microbial corrosion). So, not only would he/she be able to affirm the frequency of failure and credible consequence, but he/she would also be able to assist in steering the team in the right direction when proposing a suitable safeguard (*e.g.*, corrosion inhibitor, or maybe reducing water content). In addition, involving these team members in the PHA enhances their awareness of the credible hazardous scenarios and consequences in their facility which makes them more mindful of the criticality of some safeguards over others, which would subconsciously make them ensure that preventive maintenance is performed at an acceptable level. Of course, it is understandable that some of these team members are usually very busy and having them as permanent members of the team is very difficult or even impractical, so at least they are expected to be partial team members in PHAs.

6.7.3. PHA Team Qualifications

As can be deduced from the OSHA requirements mentioned above, the mandatory regulations set by the government are limited. The level of expertise and knowledge which defines the competency of the team is not clearly stipulated. Safety and risk specialists in process safety and human factors recognize the legislation's limitations and recommend more detailed requirements that match the level of importance of a PHA team qualifications [33].

Ideally, the competency of the team should be verified by reviewing the plant's competency management program [33]. Although this guide mainly focuses on auditing implementation of the PHA element, it is necessary to review other elements to properly assess implementation of the PHA element. Having a properly established and implemented competency management program ensures competency of the team, thus allowing quality and consistent PHAs to be produced. It would enable plant managers to make informed decisions when choosing team members and produce evidence of PHA team qualifications on demand for government auditors and investigators. The absence of a competency management program will hinder the verification of the PHA team competency and may consequently discredit the whole PHA study. Therefore, it is essential to verify that a competency management program is established by the plant in the first place. This program would be part of the plant's PSM training element. The program should adequately specify competency requirements and monitor them.

The competency management program should specify the roles and responsibilities of the PHA team members and plant managers, stipulate the level of

expertise required for team members depending on the complexity of the process being analyzed, and training and expertise required to reach the level of competency desired for each PHA team member (classroom or on the job) [21]. In addition, the program should specify the required frequency or criteria for refresher training [33], measure, monitor, and document the competency of members [33], have the ability to track training history of individuals [33], and provide a snapshot of the team members' competency status at the time of the report. The latter is crucial in order to verify that the team members were fully qualified at the time of the report and not at a later stage. It is also crucial that the assigned competency assessor is also thoroughly competent, credible, consistent, and independent [33].

6.7.3.1. PHA Team Leader Suggested Competency Criteria:

A PHA team leader must be thoroughly knowledgeable in the PHA methodology and possess exceptional facilitating skills. Table 2 describes suggested traits for a PHA team leader.

6.7.3.2. PHA Scribe Suggested Competency Criteria:

A PHA scribe must be knowledgeable in the PHA methodology, not just a recorder, fluent in the language being used, typing, grammar, spelling and familiar with the software being used to record the PHA if used. Table 3 describes suggested traits for a PHA scribe.

6.7.3.3. PHA Team Member Suggested Competency Criteria:

PHA team members must be sufficiently knowledgeable in their areas of expertise depending on the complexity of the process being analyzed. They should also

receive training on the PHA methodology being used. Table 4 describes suggested traits for a PHA team member.

Table 2: Suggested traits for PHA team leader. Adapted from [33] [36]

Technical	*Personal*
Essential	
▪ Formal PHA leadership training. ▪ Extensive knowledge* in the PHA methodology used and experience* as a team member. ▪ Extensive knowledge* and experience* utilizing risk assessment tools. ▪ Full knowledge of current PHA regulations, and company requirements. ▪ Understanding of process analyzed. ▪ Technical ability to read technical drawings, specification sheets and other technical documentations.	▪ Impartial to the facility. ▪ High Endurance. ▪ Possess two-way communication skills. ▪ Respected. ▪ Can control teams and make them reach consensus without force. ▪ Can keep the meeting on track
Optional	
▪ Experience as a scribe. ▪ Relieved from other work responsibilities that can distract from the PHA.	▪ Patient with team members ▪ Organized and focused ▪ Quick and open-minded thinker ▪ Cooperative and friendly ▪ Able to read people ▪ Diplomatic

Note: If the PHA team leader is a contractor. It is essential that his/her qualifications are verified to meet the minimum requirements set by the competency management program.

* The company's competency management program should specify exactly what constitutes having "extensive knowledge and experience" for the PHA team leader. This thesis cannot stipulate specifically what constitutes having "extensive knowledge and experience" for the PHA team leader because each process has varying levels of complexity and risk in different companies and environments. However, the established company's competency management program should specify exactly what having extensive knowledge means for the PHA team leader. This could be the number of PHA studies participated in as a team member, years of experience, training, tasks completed, certification or combination of all. For example, the company's competency management program could specify that the team leader shall have participated in at least four PHA studies as a team member and one as a scribe, in addition to having appropriate academic background, and PHA leadership training in order to become eligible for PHA leadership.

Table 3: Suggested traits for a PHA scribe. Adapted from [33] [36].

Technical	*Personal*
Essential *	
▪ Knowledgeable in the PHA methodology used. ▪ Experience in recording PHA sessions whether by utilizing a specific software or otherwise. ▪ Fluent typing skills with adequate spelling and grammar accuracy.	▪ Attention to detail. ▪ High Endurance. ▪ Compatible with team leader. ▪ High comprehension of speech
Optional	
▪ Understanding of process analyzed. ▪ Knowledge of technical terminology used. ▪ Relieved from other work responsibilities that can distract from the PHA.	▪ Capable of being an assistant to the team leader and not just a recorder. ▪ High level of response

* If the PHA scribe is a contractor. It is essential that his/her qualifications are verified to meet the minimum requirements set by the competency management program.

Table 4: Suggested traits for a PHA team member

Technical	*Personal*
Essential	
▪ Sufficiently* proficient in their respective area of expertise. ▪ Knowledgeable in applicable standards, regulations, and best practices applicable to their respective areas of expertise. ▪ Able to read technical drawings and understand process documentation. ▪ Received formal training in risk assessment and utilizing risk assessment tools.	▪ Communicate technical issues clearly to team members. ▪ Committed to spend the required time to participate in the PHA with no distractions.
Optional	
▪ Knowledgeable in the PHA methodology used (received formal training). ▪ Understanding of process analyzed (mandatory if member is a process engineer or operator)	▪ Focused. ▪ Able to express his/her opinion without fear of criticism. ▪ Able to work in a team.

* The company's competency management program should specify exactly what constitute being "sufficiently proficient" for each PHA team member. This thesis cannot stipulate specifically what

constitutes being “sufficiently proficient” for each team member because each process has varying levels of complexity and risk in different companies and environments. However, the established company’s competency management program should specify exactly what being sufficiently proficient mean for each team member participating in this study. This could be a position, years of experience, tasks completed, training, certification or combination of all. For example, the company’s competency management program could specify that the operator shall have at least 5 years of experience, or should be at least a shift supervisor.

6.8. Time Allocated for PHA Team

Another significant contributing factor to PHA quality is the time allocated for the PHA team to conduct the PHA. You can have the best PHA team in the world, but giving them a lot less time than what they require will tremendously reduce the quality of their analysis. Industry safety leaders such as William Ralph [37] and Professor Sam Mannan, members of Mary Kay O'Connor Process Safety Center Steering Committee, emphasize the importance of giving enough time for the PHA team to produce quality PHAs. Professor Sam Mannan also advocates the need to provide the team with sufficient breaks as well to reduce fatigue and maintain the team’s focus [36]. Therefore, it is exceedingly important that the auditor determines and evaluate the actual time it took the team to complete the actual PHA exercise, not including preparation and report writing, and compare it to a reasonable estimate. The number of days it took to complete the PHA study can be obtained by interviewing some of the team members with reasonable accuracy if it is backed up by emails exchanged between the team. The average number of hours per day, as well as the number/length of breaks could be

obtained in the same way. It is even better if company guidelines would require this information to be logged in the PHA report itself to make it easier for future audits. An estimate of the time required to complete a HAZOP can be obtained using chapter 13 (*Estimation of Time Needed for PHAs*) of the *Guidelines for Process Hazards Analysis (PHA, HAZOP), Hazards Identification, and Risk Analysis* developed by Nigel Hyatt [18]. An estimate of the time required to complete a What if/Checklist can also be obtained using Hyatt's guidelines.

However, the auditor must bear in mind that these estimates are not accurate and in reality many other factors can affect the actual time it takes the team to complete a PHA, which means that deviating from the estimate is acceptable if the deviation is not too high. So, the PHA quality would not necessarily take a significant hit unless the team was given less than 70% of the estimated time. For example, if the team was only given 165 hours compared to an estimate of 180 hours, there should not be any concern given the inherent inaccuracy of the estimate. However, if the team was only given 100 hours to complete a HAZOP which was estimated to require 180 hours, then it would be significantly probable that the HAZOP quality has suffered. Of course, more time deviation below 70% of the estimate should translate to more reduction in quality. So, 80 hours given to the team would have more negative effects on quality compared to 100 hours out of 180, and this should be reflected in the audit score given.

7. PHA SCOPE COMPREHENSIVENESS

7.1. Non-Routine Mode of Operation

Perhaps the biggest and most dangerous gap in PHA performance is the failure to include non-routine mode of operation. More than 80% of process facilities do not perform PHAs for non-routine mode of operation [38]. Yet, a paper published by the Process Improvement Institute (PII) which reviewed 47 major process safety incidents occurring from 1987 to 2010 revealed that almost 70% of all moderate to major incidents occurred during non-routine mode of operation [2]. This figure was even confirmed by a poll sent to over 50 of PII's clients [38]. Discussing this issue with another safety consulting company, which leads PHAs on a regular basis, also confirmed that this is a major issue in most process facilities [39], despite the fact that performing PHAs for all modes of operation is an OSHA PSM requirement according to OSHA's 29 CFR 1910.119. What makes this issue even more dangerous, is that common PHA methodologies employed for continuous mode of operation only identifies 5-10% of the potential hazardous scenarios for non-routine mode of operation [38]. This risk becomes even more evident when factoring the number of shutdown/startups performed by each facility each year, the fact that during startup/shutdown operations most safeguards proposed to reduce risk during continuous operation are bypassed, and that the reliance on operator actions is substantially increased greatly increasing human error and reducing reliability. This results in the increased probability of a major incident occurring by 30-50 times [38].

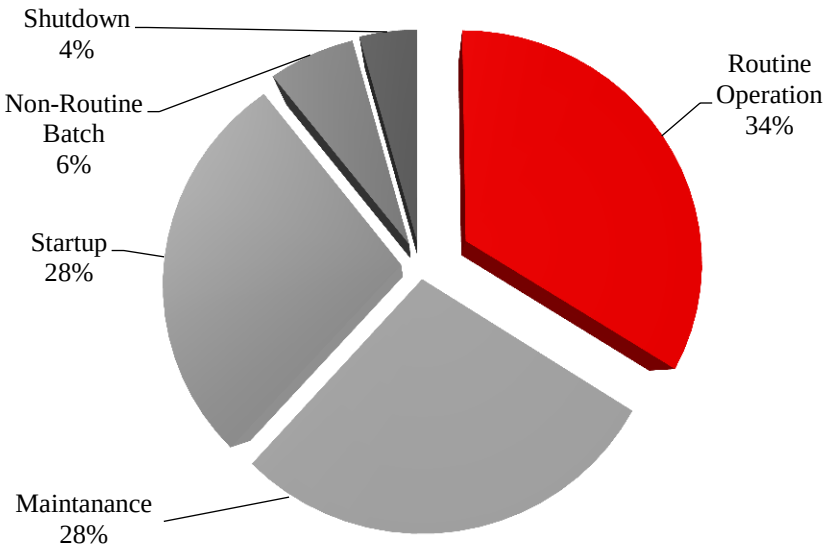

Figure 7: Incidents during different modes of operation (47 major incidents between 1987-2010). Adapted from [2].

The auditor should verify that PHAs were conducted for non-routine modes of operation and should evaluate them against the same quality standards discussed throughout the proposed guidelines in Appendix A. There are a few points that the auditor should note:

1) For evaluating time required to complete non-routine mode of operation PHAs, time estimated using Hyatt's guidelines discussed in Section 6.8 must be multiplied by a factor of 54%. This is due to the fact non-routine modes of operation HAZOPs require less guidewords and therefore less time. According to William Bridges in his paper titled "*How to efficiently perform the hazard evaluation (PHA) required for non-routine modes of operation (startup, shutdown, online maintenance)*", the total amount of meeting time spent to

perform routine and non-routine mode of operation PHAs is split 65% and 35%, respectively.

2) The auditor should verify that appropriate PHA methodologies are utilized. Qualitative PHA methodologies typically used for non-routine modes of operations are [38]:
   (a) The 7 to 8 guidewords HAZOP, typically used for high risk/complexity procedures.
   (b) The 2 guidewords HAZOP, typically used for lower risk/complexity procedures.
   (c) The What-if method utilized or low risk/complexity procedures with well understood tasks and hazards.
3) Triggers to initiate more quantitative methodologies (*e.g.,* LOPA) for specific procedures should be established in corporate requirements and implemented during PHAs for non-routine modes of operation similar to their routine counterparts as discussed in section 6.5.

7.2. Facility Siting

Another common gap shared by many companies is also failing to include or consider facility siting (*i.e.,* effect of potential explosions and toxic releases on nearby occupied buildings) in their PHA. Most facilities will do a good job in including all process nodes. However, they might fail to assess facility siting entirely. Addressing facility siting is a requirement in the USA and is driven by OSHA and EPA. Yet, some

facilities perform this task separately without incorporating its findings in the facility's PHA studies. Auditors should verify incorporation of facility siting assessment findings in PHA recommendations. In addition, since facility siting assessment should be part of the PHA, auditors should ensure that facility siting studies are performed at least every 5 years and incorporated in PHA revalidations [20]. This is extremely important not only because it reduces residual risk that went unidentified in previous PHAs, but also because building occupancy indices may change as well, which may result in significant change in the consequences and the level of risk assessed in the previous PHA studies. Auditors should also verify that temporary structures, such as portable buildings or trailers used during turnaround and inspection (T&I) for contractor occupancy, are only placed in safe zones defined in the facility siting assessment. During the BP Texas city incident, 15 contractors were fatally injured in trailers that were not placed in safe zones [8].

7.3. Chemical Inventory

Chemicals stored in the process are not subject to being overlooked in a PHA study. However, chemicals used for maintenance usually are overlooked. Improper storage of flammable or toxic chemicals stored in warehouses and sheds can lead to major incidents. A well-known one is the incident that occurred in Tianjin, China 2015. The explosions which originated from chemicals stored in a storage warehouse had a power which exceeded 20 tons of TNT [15]. So, depending on the quantity and nature of

the stored chemicals, a facility might be completely wiped out. Had a quality PHA been performed on this chemical warehouse, the risk would have been greatly reduced.

Auditors should not only ensure that all chemical storage warehouses/buildings have been included in the PHA, but also maximum inventory reached for these chemicals should be verified through site verifications, inventory reports, and/or employee interviews. It is also vital to ensure that maximum chemical inventories are accounted for in PHA revalidations as well. A change in inventory may slip through existing gaps in the facility's MOC process, especially if the chemical inventory is managed by a different department which may not have an engineer or qualified person. This is often seen in big companies where material/chemical warehouses are managed independently. Furthermore, in general warehouses are often perceived as low risk and have poor PSM implementation monitoring.

7.4. Shared Processes

Special attention must be given to shared processes and connected boundaries between different units in a given facility. Performing PHAs on processes like utility lines and flare headers that are shared among several units in a facility can be neglected unintentionally. When ownership of process units is segregated and the responsibility of performing PHAs is assigned to several PHA teams, the teams might neglect performing PHAs on shared processes or miss sections as a result of differently defined boundaries between units [39]. The auditor should verify first if references in PHA do in fact link to a performed PHA on the shared process. In addition, the auditor should verify that the

boundaries of connecting process units are similarly defined and no section of the facility is overlooked.

7.5. Inherently Safer Design (ISD)

Utilizing the ISD principals to reduce risk should be a critical step in any PHA study. Although it is most effective during conceptual design and front end engineering design (FEED) [1], it should also be applied to reduce consequence severity for high consequence hazardous scenarios identified during initial PHA studies [31]. Although ISD can be applied at any time during the facility's lifecycle, it makes more sense practically and financially to apply them during the design stage of the process [1]. By now, ISD awareness should not be an issue and auditors should pursue and verify implementation of ISD principals.

An auditor should verify that the ISD principals were applied during the design stage for identified hazardous scenarios with severe consequences [31]. The hierarchy followed should be in accordance with Figure 8 shown below.

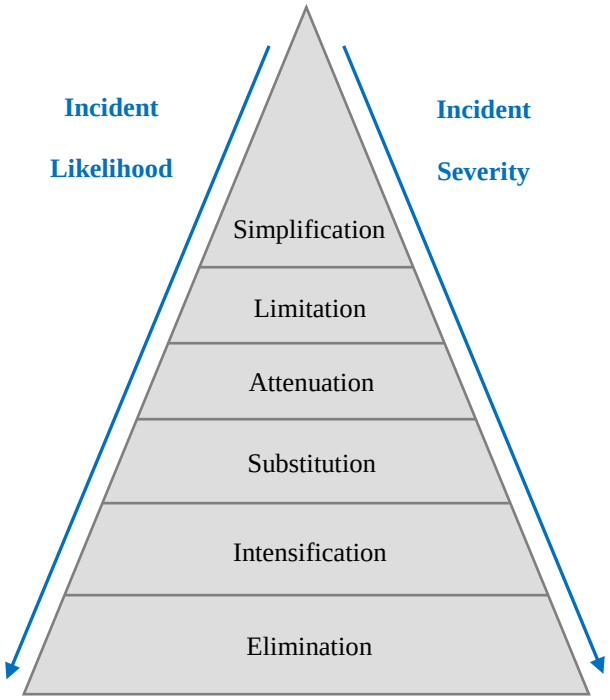

Figure 8: Inherently Safer Design (ISD) principals' hierarchy. Reprinted from [1]

Elimination: Elimination of hazard.

Intensification: Reduction in inventory of hazardous chemicals and/or process/equipment size (*e.g.* pipe diameter, vessel size).

Substitution: Substitution of hazardous chemical with a safer one (*e.g.*, higher flash point, less reactive chemicals).

Attenuation: Reduction of hazardous conditions (*e.g.*, pressure, temperature if flammable, dilution).

Limitation: Reduction of consequence (*e.g.*, reducing leak volume, reducing explosion impact)

Simplification: Reduction of probability of error/failure.

8. CONCLUSIONS AND RECOMMENDATIONS

As implied throughout the thesis, it is critical that the audit team use guidelines similar to the ones proposed in this study as part of an overall PSM audit. Focusing on auditing the quality of the PHA element alone will unquestionably assist in identifying gaps in implementation and company policies/standards. However, solving these identified gaps will require looking at the bigger picture, which only can be attained from auditing the whole safety management system (SMS). Implementation deficiencies in process safety information, incident investigation, training, and mechanical integrity for example, will definitely have cascading effects on PHA implementation. In addition, implementation deficiencies in PHA quality will also have cascading effects on other PSM elements such as mechanical integrity, operating procedures, emergency planning and response. Therefore, it is highly recommended that the user/s of these proposed guidelines incorporate them as part of an overall PSM audit. It is also highly recommended that user/s of these guidelines also use their findings to propose recommendations that focus on improving the SMS, eliminating the identified gaps, and updating the internal standards and procedures of the facility to ensure continuous improvement. It is most frustrating to find out that all the man-hours, money, and effort that went into performing the monumental task of auditing the whole SMS just to find that the audit report merely became a document hidden on a shelf collecting dust. Spending the time and money to perform this audit and use its findings to close the

company's SMS gaps should be seen as an investment by the facility's executives. It will unquestionably save a lot of money and ensure business continuity on the long run.

9. FUTURE WORK

The next step that follows developing these guidelines would be of course to test them in a pilot exercise at a chemical/hydrocarbon facility. Multiple pilots will help complete and refine these guidelines, and make them more practical to use. The natural step following those pilot exercises and improvement of guidelines is to use them to enhance the facility's internal standards and procedures in order to help close identified gaps, develop systems that assist in making the PHA element easier to audit and monitor with the goal of steering the facility for continuous improvement of PHA element implementation.

REFERENCES

1. Cameron, I.T. and R. Raman, *Process Systems Risk Management*. Vol. 6. 2005: Academic Press.

2. Bridges, W. and T. Clark. *How to efficiently perform the hazard evaluation (PHA) required for non-routine modes of operation (startup, shutdown, online maintenance)*. in *7th Global Congress on Process Safety*. 2011.

3. U. S. Chemical Safety and Hazard Investigation Board, *Williams Geismar Olefins Plant: Reboiler Rupture and Fire: Geismar, Louisiana: Incident Date: June 13, 2013: Two Fatalities, 167 Reported Injuries:*. 2016.

4. U. S. Chemical Safety and Hazard Investigation Board, *Chlorine release (16 medically evaluated, community evacuated): DPC Enterprises, L.P., Glendale, Arizona, November 17, 2003*. 2003: Washington, D.C. p. 55.

5. U. S. Chemical Safety and Hazard Investigation Board, *Chlorine release, July 20, 2003 (7 injured): contaminated antimony pentachloride exposure, July 29, 2003 (1 killed): hydrogen fluoride release, August 13, 2003 (1 exposed, 1 injured): Honeywell International, Inc., Baton Rouge, Louisiana* 2005. p. 106.

6. Mannan, M.S., J. Makris, and H.J. Overman, *Process Safety and Risk Management Regulations: Impact on Process Industry*. Supplement 1 ed. Encyclopedia of Chemical Processing and Design, ed. R.G.A.a.J.J. McKetta. Vol. 69. 2002, New York: Marcel Dekker, Inc.

7. Litvak, A., *Energy companies study the role of human behavior in safety*. Pittsburgh Post-Gazette, 2014.

8. *BP Texas City Final Investigation Report*. 2007, U.S. Chemical Safety and Hazard Investigation Board.

9. *Process safety management guidelines for compliance*. 1992: [Washington, D.C.]: U.S. Dept. of Labor, Occupational Safety and Health Administration, 1992.

10. Kaszniak, M., *Oversights and omissions in process hazard analyses: Lessons learned from CSB investigations.* Process Safety Progress, 2010. **29**(3): p. 264-269.

11. Center for Chemical Process Safety, *Guidelines for Auditing Process Safety Management Systems*. 1993: Center for Chemical Process Safety/AIChE.

12. Moss, T., *Auditing Offshore Safety Risk Assessments.* Journal of Petroleum Technology, 1990. **42**(10): p. 1241-1243.

13. Crawley, F. and B. Tyler, *HAZOP: Guide to Best Practice (Third Edition)*. 2015: Elsevier.

14. Center for Chemical Process Safety, *Guidelines for Risk Based Process Safety*. 2007, Center for Chemical Process Safety/AIChE.

15. BBC News, *China explosions: What we know about what happened in Tianjin - BBC News.* 2015.

16. Andrew Jacobs, J.C.H. and B. Chris, *Behind Deadly Tianjin Blast, Shortcuts and Lax Rules.* 2015.

17. Mortimer, C., *Tianjin explosion: Gigantic crater left by Chinese factory explosion revealed in this picture.* 2016.

18. Hyatt, N., *Guidelines for process hazards analysis (PHA, HAZOP), hazards identification, and risk analysis*. 2003: CRC press.

19. Dunjó, J., et al., *Conducting HAZOPs in continuous chemical processes: Part I. Criteria, tools and guidelines for selecting nodes.* Process Safety and Environmental Protection, 2011. **89**: p. 214-223.

20. Center for Chemical Process Safety, *Hazard Identification and Risk Analysis*, in *Guidelines for Auditing Process Safety Management Systems*. 2011, John Wiley & Sons, Inc. p. 307-360.

21. Center for Chemical Process Safety, *Guidelines for Defining Process Safety Competency Requirements*. 2015, New York, US: American Institute of Chemical Engineers.

22. Center for Chemical Process Safety, *Guidelines for Chemical Process Quantitative Risk Analysis*. 2nd ed ed. CCPS guidelines series. 2000: New York : The Center, [2000].

23. Rushton, A.G., *Quality Assurance of HAZOP*. 1996, U.K. Health and Safety Executive: Sheffield, UK.

24. Beerens, H.I., J.G. Post, and P.A. Uijt de Haag, *The use of generic failure frequencies in QRA: the quality and use of failure frequencies and how to bring them up-to-date.* J Hazard Mater, 2006. **130**(3): p. 265-70.

25. Moss, T.R. and J.E. Strutt, *Data Sources for Reliability Design Analysis.* Proceedings of the Institution of Mechanical Engineers, Part E: Journal of Process Mechanical Engineering, 1993. **207**(1): p. 13-19.

26. *LOPA – Layer of Protection Analysis.* Process and HSE Engineering, 2011.

27. Lowrance, W.W., *Of Acceptable Risk: Science and the Determination of Safety.* 1976.

28. Shortreed, J., K. Dinnie, and D. Belgue. *Risk criteria for public policy*. in *Proceedings of the First Biennial Conference on Process Safety and Loss Management*. 1995.

29. Health and Safety Executive, *Initial briefing to Societal Risk Technical Advisory Group*. 2009, Research Report, RR703.

30. Duijm, N.J., *Recommendations on the use and design of risk matrices.* Safety Science, 2015. **76**: p. 21-31.

31. Mannan, M.S., *Personal Communication*. 2017.

32. Suttinger, L.T. and C.L. Sossman, *Operator Actions Within a Safety Instrumented Function*. Conference: ISA 2002, Chicago, IL (US), 10/21/2002--10/24/2002; Other Information: PBD: 6 Sep 2002. 2002: ; Savannah River Site (US). Medium: ED; Size: vp.

33. Baybutt, P., *Competency requirements for process hazard analysis (PHA) teams.* Journal of Loss Prevention in the Process Industries, 2015. **33**: p. 151-158.

34. *Process safety management guidelines for compliance. 1994 (Reprinted)*. 1994: [Washington, D.C.] : U.S. Dept. of Labor, Occupational Safety and Health Administration, [1994].

35. Occupational Safety and Health Administration, *OSHA Letter of Interpretation of PSM Standard*, T.N.C. Robert Summers, Inc., Editor. 2001.

36. Mannan, M.S., *Chemical Process Safety Lecture: HAZOPs*. 2015.

37. Ralph, W., *Personal Communication*. 2017.

38. Bridges, W. and M. Marshall, *Necessity of Performing Hazard Evaluations (PHAs) of Non-normal Modes of Operation (Startup, Shutdown, & Online Maintenance).* 2016.

39. Nguyen, G., *Personal Communication*. 2017.

APPENDIX A: PHA QUALITY AUDITING GUIDELINES

No.	Question	Reference	Standard Status (MC/NI/DNE)	Score (0-5)	NF	Notes/Comments
1	**Sources of Quality Variance**					
1.1	**Comprehensiveness of PHA Inputs**					
1.1.1	Has the facility/company established requirements to include all applicable PHA inputs listed in (a) through (m)? (a) Piping and Instrumentation Diagrams (P&IDs), (b) Process Flow Diagrams (PFDs) with material/energy balances, (c) Layout drawings, (d) Equipment specifications sheets, (e) Process description, (f) Incident and near miss investigation reports, (g) Maximum chemical inventory in storage facilities, (h) Previous PHA reports*, (i) Emergency work orders*, (j) Corrosion inspection worksheets*, (k) MOCs*, (l) Drill critiques*, (m) Pre-startup safety reviews action items*. * Required only during PHA revalidation.	Sections 3 & 6.1				

No.	Question	Reference	Standard Status (MC/NI/DNE)	Score (0-5)	NF	Notes/Comments
1.1.2	Did the PHA/s consider all applicable input sources listed in (a) through (e)? (a) Piping and Instrumentation Diagrams (P&IDs), (b) Process Flow Diagrams (PFDs) with material/energy balances, (c) Layout drawings, (d) Equipment specifications sheets, (e) Process description, Auditor should review: ▪ PHA report and verify that all applicable sources for input were considered in the report. ▪ Shared processes with connected boundaries between different units (*e.g.*, utility lines, flare headers) and verify: o If PHA references for shared processes do in fact reference to a performed PHA. o If PHA process node boundaries are identical in connecting process units and no section of the facility is overlooked.	Sections 6.1 & 7.4			1	

No.	Question	Reference	Standard Status (MC/NI/DNE)	Score (0-5)	NF	Notes/Comments
1.1.3	Did the PHA/s consider all related incidents and near misses with medium to high risk potential listed in (a) through (c)? (a) Incidents and near misses which occurred at the same facility, (b) Incidents and near misses at other facilities with similar processes in the same company? (c) Incidents at other facilities with similar processes in other companies? Merely attaching incident reports do not qualify as adequate consideration. Auditor should also: ▪ Review emergency maintenance work orders (EMWO), identify the ones that were issued following an incident, and verify that all incidents have been considered in the PHA. EMWOs would capture the occurrence of incidents that were not properly reported or investigated. ▪ Review process trips/upsets investigation reports and verify that the ones with medium to high risk potential were considered in the PHA. Some companies do not report these as near misses.	Section 6.1			7	

No.	Question	Reference	Standard Status (MC/NI/DNE)	Score (0-5)	NF	Notes/Comments
1.1.4	Did the PHA team review and consider critical issues identified in emergency maintenance work orders (EMWO) during revalidation? Auditor should verify if the PHA team used actual equipment premature failure information identified in EMWOs to impact their estimation of risk.	Section 6.1			1	
1.1.5	Did the PHA/s consider the maximum chemical inventory in nearby storage facilities? Auditor should verify: ▪ The actual maximum chemical inventory reached through site verifications previous inventory records, future plans of increase, and employee interviews. ▪ If maximum chemical inventory impacted potential consequences when estimating risk. ▪ If facility siting analysis considered nearby hazardous chemical inventory in nearby storage warehouses? ▪ If storage warehouses with high inventory of hazardous material have been included in the PHA as potential sources of hazard and not been overlooked.	Sections 6.1 & 7.3			2	

No.	Question	Reference	Standard Status (MC/NI/DNE)	Score (0-5)	NF	Notes/Comments
1.1.6	Did the PHA/s consider previous PHA reports during revalidation? Auditor should verify if issues identified during previous PHAs (*e.g.* outdated P&IDs, missing information, operating procedures, startup procedures, shutdown procedures, inventory discrepancy) have been rectified before performing the audited PHA.	Sections 6.1 and 6.2			1	
1.1.7	Did the PHA/s consider corrosion inspection worksheets during revalidation? Auditor should verify if critical corrosion inspection worksheet findings such as current thickness of pipe or vessel impacted risk estimation.	Section 6.1			1	
1.1.8	Did the PHA team review previous MOCs to account for any residual intolerable risk during revalidation?	Section 6.1			1	

No.	Question	Reference	Standard Status (MC/NI/DNE)	Score (0-5)	NF	Notes/Comments
1.1.9	Did the PHA team review past drill critiques and considered their findings (*e.g.*, emergency response time, fire truck access, manual isolation valve access) in the report during revalidation? Auditor should verify if the team used drill critique findings in risk estimation and design.	Section 6.1			1	
1.1.10	Did the PHA team review pre-startup safety reviews and consider unresolved action items? Auditor should verify if unresolved action items [*e.g.* incomplete transfer of process information, incomplete training of maintenance personal to properly maintain a safety instrumented system (SIS), and incomplete installation of SIS] have impacted the report. Verification should include field verification and/or interviews.	Sections 6.1 & 6.2			1	

No.	Question	Reference	Standard Status (MC/NI/DNE)	Score (0-5)	NF	Notes/Comments
1.2	**Quality of PHA Inputs**					
1.2.1	Has the facility/company established systems, including items (a) through (m), which ensure quality of all applicable PHA inputs listed in question 1.1.1? (a) Process Safety Information (PSI) (b) Training and Competency Management (c) Mechanical Integrity (d) Management of Change (MOC) (e) Incident Reporting and Investigation (f) Emergency Planning and Response If these systems exist and have been audited as part of an overall PSM audit, scores should be used to influence the overall score of PHA quality.	Section 6.2				

No.	Question	Reference	Standard Status (MC/NI/DNE)	Score (0-5)	NF	Notes/Comments
1.2.2	Did the facility provide accurate and up-to-date PSI to the PHA team? Auditor should verify the question through the following: ▪ Checking previous PHA reports for any comments regarding missing/inaccurate PSI and verifying if these were rectified prior to performing the audited PHA. ▪ Interviewing PHA team members and inquiring about any missing information or inaccuracies identified during the PHA. ▪ Interviewing process engineers, plant operators, and maintenance engineers and inquire about any missing information or inaccuracies they encounter regarding PSI. ▪ Checking completed MOCs which needed PSI updates and verifying if updates were performed prior to the PHA. ▪ Interviewing personnel and inquiring about any recent changes to the process and verifying that all these changes went through the MOC process and associated PSI were updated as necessary. ▪ Reviewing any recent third party audit reports which audited PSI.	Section 6.2			8	

No.	Question	Reference	Standard Status (MC/NI/DNE)	Score (0-5)	NF	Notes/Comments
1.3	**Risk Assessment Accuracy**					
1.3.1	Has the facility/company established requirements to ensure accuracy of risk assessments during PHA? Auditor should verify if the company established/adopted guidelines for using historical data, generic failure data, and experience to ensure accuracy of risk estimation.	Sections 6.3.1 & 6.3.3				
1.3.2	Has the facility/company established and maintained an equipment failure database in order to use it to estimate risk to high levels of accuracy? Auditor should verify that the facility/company has developed their own database based on the facility's equipment failure data. If other sources of data (*i.e.* historical data from other facilities, or generic data) were used to develop the database, the auditor should ensure that they were reviewed and modified to cater for differences in operational and environmental conditions (*e.g.*, fluid aggressiveness, temperature, pressure, and vibration).	Section 6.3.1.1			2	

No.	Question	Reference	Standard Status (MC/NI/DNE)	Score (0-5)	NF	Notes/Comments
1.3.3	If historical data was utilized from other facilities with similar processes to estimate probability of failure, has the team reviewed and modified the data to cater for differences in operational and environmental conditions (*e.g.*, fluid aggressiveness, temperature, pressure, and vibration)?	Section 6.3.1.1			1	
1.3.4	Were generic failure databases utilized to estimate probability of failure only where no historical data existed?	Section 6.3.1.2			1	
1.3.5	If generic data were used to estimate probability of failure, was it reviewed and/or modified to suit the facility's operational and environmental conditions (*e.g.*, fluid aggressiveness, temperature, pressure, and vibration)?	Section 6.3.1.2			1	

No.	Question	Reference	Standard Status (MC/NI/DNE)	Score (0-5)	NF	Notes/Comments
1.3.6	Was probability of failure estimates revalidated by the PHA team using actual failure data of the facility equipment during PHA revalidations?	Section 6.3.1.2			1	
1.3.7	Did the PHA team initially estimate the risk using the worst-case credible consequence for a given scenario without considering the effects of any safeguards (*e.g.* relief valve, level alarm, emergency isolation valve)?	Section 6.3.2			1	

No.	Question	Reference	Standard Status (MC/NI/DNE)	Score (0-5)	NF	Notes/Comments
1.3.8	If the team relied solely on their experience to estimate the risk of some given scenarios, was it limited to high frequency scenarios which several team members witnessed during their experience? The probability of rare events should not be estimated using the team's experience only without relying on any other sources of data.	Section 6.3.2			1	

No.	Question	Reference	Standard Status (MC/NI/DNE)	Score (0-5)	NF	Notes/Comments
1.4	**Risk Acceptance Criteria**					
1.4.1	Has the facility/company developed adequate risk acceptance criteria for all relevant types of risk (*e.g.*, human life, health, environment, and assets) which includes items (a) and (b)? (a) Maximum allowable risk per initiating event. (b) Maximum allowable risk per node or area Auditor should verify if: ▪ The criteria differentiate between employee and societal risk (*i.e.*, societal risk should not be higher than employee risk). ▪ The criteria are approved and signed by facility/company executives. ▪ The criteria are reasonable (*e.g.*, societal risk should be between 10^{-6} and 10^{-3} fatality per person/year.	Section 6.4				

No.	Question	Reference	Standard Status (MC/NI/DNE)	Score (0-5)	NF	Notes/Comments
1.4.2	Did the facility/company develop an adequate risk assessment tool (*e.g.*, risk matrix) which incorporates the approved risk acceptance criteria that meets the requirements of question 1.4.1? Auditor should verify that: ▪ Descriptions of consequence categories includes at least loss of life, financial loss, and environmental loss. ▪ Quantitative description is used to define probability and consequence categories. ▪ Resolution of matrix is at least 4x4. ▪ Ranges of frequency and consequence are adequate. For example, major incidents consequences should range from loss time injury to multiple fatalities. For likelihood, the range should be from 1 per year to at least 10^{-4} per year. ▪ Coloring of risk matrix is clearly defined in terms of risk acceptability, and the ALARP region is identified. ▪ Risk acceptance criteria is defined quantitatively in addition to coloring. ▪ The tool is approved by facility/company executives.	Section 6.4			2	

No.	Question	Reference	Standard Status (MC/NI/DNE)	Score (0-5)	NF	Notes/Comments
1.4.3	Did the PHA team utilize an adequate risk assessment tool (*e.g.*, risk matrix) which meets the requirements of question 1.4.2?	Section 6.4			3	
1.5	**Initiation For More Quantitative Methodologies**					
1.5.1	Has the facility/company developed criteria for initiating more quantitative studies, and specified suitable quantitative risk assessment methodologies for the specific initiation criterion? Auditor should verify that initiation triggers used are based on estimated consequences (major injury, fatality, societal injury, environmental toxic release, etc.), risk, complexity of the process, type of material/chemical processed, or a combination.	Section 6.5				
1.5.2	Did the PHA team perform a study with a suitable quantitative risk assessement methodology based on facility/company initiation criteria?	Section 6.5			2	

No.	Question	Reference	Standard Status (MC/NI/DNE)	Score (0-5)	NF	Notes/Comments
1.5.3	If the PHA team recommended performing a study with a suitable quantitative risk assessement methodology based on facility/company initiation criteria, was the recommendation closed only after recommnedations of the resulting study were implimented?	Section 6.5			2	

No.	Question	Reference	Standard Status (MC/NI/DNE)	Score (0-5)	NF	Notes/Comments
1.6	**Safeguard Risk Effect Estimation**					
1.6.1	Did the team accurately reevaluate the risk of each hazardous scenario identified with recommended/installed safeguards to determine/demonstrate that the proposed safeguards are sufficient to reduce the risk to as low as reasonably practicable (ALARP)? Auditor should verify that: ▪ The PHA team did not introduce invalid safeguards such as: (a) A safeguard that requires a rushed operator intervention unfeasible by the operator due to a lack of time or inaccessibility (*e.g.*, isolation valve located very close to a leak/fire, or isolation valve which requires a scaffold to access); (b) "Operator Awareness;" (c) "Never had a problem with it to date;" (d) Using a vessel site glass with a media that causes fouling of glass making it difficult to tell true level; (e) Using a component from the same failed loop/system as a safe guard.	Section 6.6			3	

No.	Question	Reference	Standard Status (MC/NI/DNE)	Score (0-5)	NF	Notes/Comments
	▪ The PHA team did not reduce the risk in both the probability and consequence axes. A safeguard such as a level alarm would only reduce the probability, while a dike would reduce the consequence.					
1.6.2	Did the PHA team accurately consider operator action as a safeguard to implement emergency response procedures? Auditor should verify that risk was only reduced along the consequence axis.	Section 6.6.1			1	

No.	Question	Reference	Standard Status (MC/NI/DNE)	Score (0-5)	NF	Notes/Comments
1.6.3	If the PHA team considered operator action as a safeguard to control the process and return it to its safe parameter, have they accurately determined its effect on risk? Auditor should verify that: ▪ Risk was only reduced along the probability axis. ▪ Magnitude of reduction along the probability axis did not exceed a factor of 10 unless the team demonstrated the following: (a) This particular operator response is reliable enough to exceed a factor of 10 by performing LOPA or equivalent methodology proving that the operator action meets the intended safety instrumented function (SIF). (b) The operator can respond correctly to the alarm within the available time to return the process to a safe state. (c) The probability of human error for each specific case is estimated using sound human error evaluation techniques such as the Technique for human Error Rate Prediction (THERP) and the Accident Sequence Evaluation Program Human Reliability Analysis Procedure (ASEP HRA Procedure).	Section 6.6.1			3	

No.	Question	Reference	Standard Status (MC/NI/DNE)	Score (0-5)	NF	Notes/Comments
	(d) Environmental factors (e.g., access, control area environment, control layout and quality of displays), stress factors (e.g., shift schedules, response time pressure), and personnel factors (e.g. experience, training) are considered in the analysis to reduce or increase/decrease the nominal human error rates estimated through the human error evaluation technique.					

No.	Question	Reference	Standard Status (MC/NI/DNE)	Score (0-5)	NF	Notes/Comments
1.7	**Factors Affecting Team Performance**					
1.7.1	Has the facility/company established requirements to include at least disciplines listed in (a) through (l) in a PHA team? (a) PHA leader; (b) Scribe; (c) Process engineer or designer; (d) Project engineer; (e) Experienced Operator; (f) Safety, Health, Environment expert (as required); (g) Instrument/ Safety Instrumented Systems (SIS) engineer (as required); (h) Mechanical/maintenance engineer knowledgeable in routine and non-routine maintenance procedures and tasks (as required); (i) Corrosion inspector/engineer representative (as required); (j) Instrument technician; (k) Maintenance/mechanical technician; (l) Other specialist/experts in other relevant disciplines (*e.g.*, process technology; operating procedures; alarms; procedures; procurement) as required.	Section 6.7.2				

No.	Question	Reference	Standard Status (MC/NI/DNE)	Score (0-5)	NF	Notes/Comments
1.7.2	Did the PHA team cover all required disciplines to ensure all hazards are identified and evaluated against risk acceptability criteria? Auditor should verify that a corrosion inspector/engineer, instrument technician, and maintenance/mechanical technician were part of the team at least at some point during the PHA as required.	Section 6.7.2			3	

No.	Question	Reference	Standard Status (MC/NI/DNE)	Score (0-5)	NF	Notes/Comments
1.7.3	Has the facility/company established and implemented an adequate competency management program that ensures the competency of PHA team and covers items listed in (a) through (m)? (a) Specify the roles and responsibilities of the PHA team members and facility management. (b) Stipulate the level of expertise required for team members depending on the complexity of the process being analyzed, (c) Stipulate the training material and type of training (*e.g.*, classroom or on the job), (d) Specify the required frequency or criteria for refresher training, (e) Stipulate expertise required to reach the level of competency desired for each PHA team member (*e.g.* years of experience, number of PHA studies participated in, tasks completed, position, certifications, or combination of all), (f) Measure, monitor, and document competency of members, (g) Able to track training history of individuals, (h) Provide a snapshot of the team members' competency status at the time of the report.	Section 6.7.3			2	

No.	Question	Reference	Standard Status (MC/NI/DNE)	Score (0-5)	NF	Notes/Comments
1.7.4	Was the PHA team leader qualified per the requirements stipulated in the facility's competency management program? Auditor should review the PHA team leader competency requirements described in the competency management program and verify if he/she meets those requirements. Table 3 in section 6.7.3 can be used to verify team leader competency if facility requirements are deemed inadequate.	Section 6.7.3			4	
1.7.5	Were the PHA team members and scribe qualified per the requirements stipulated in the facility's competency management program? Auditor should review the PHA team members and scribe competency requirements described in the competency management program and verify if they meet those requirements. Tables 4 and 5 in section 6.7.3 can be used to verify team member and scribe competency if facility requirements are deemed inadequate.	Section 6.7.3			3	

No.	Question	Reference	Standard Status (MC/NI/DNE)	Score (0-5)	NF	Notes/Comments
1.7.6	Was the PHA team allocated sufficient time to complete the PHA while maintaining quality? Auditor should verify: ▪ How much time the team actually needed to complete the PHA while maintaining quality. This information could be obtained from interviewing the PHA team leader since it is his responsibility to estimate and ask for sufficient time for the team. If this information could not be obtained from the PHA team leader, refer to chapter 13 (*Estimation of Time Needed for PHAs*) of the *Guidelines for Process Hazards Analysis (PHA, HAZOP), Hazards Identification, and Risk Analysis* developed by Nigel Hyatt. His guidelines can be used to estimate the time required for meetings in a HAZOP study (not including preparation and report writing). Hyatt's estimation guidelines are mainly for routine modes of operation. HAZOPs and What if/checklist performed for non-routine mode of operation require 54% of the time estimated for routine mode of operation. ▪ The team was in fact allocated the time requested by the PHA team leader or at least 70% of the estimated time obtained Hyatt's guidelines.	Sections 6.8 and 7.1			4	

No.	Question	Reference	Standard Status (MC/NI/DNE)	Score (0-5)	NF	Notes/Comments
2	**PHA Scope Comprehensiveness**					
2.1	**Non-Routine Mode of Operation**					
2.1.1	Has the facility/company established a requirement to perform PHA studies for non-routine mode of operation?	Section 7.1				
2.1.2	Did the PHA team conduct PHAs for all non-routine modes of operation using appropriate PHA methodologies? Auditor should verify that: ▪ PHAs for performed for startup, shutdown, non-routine batch, and maintenance modes of operations. ▪ Appropriate PHA methodologies were utilized: (a) The 7 to 8 guidewords HAZOP, typically used for high risk/complexity procedures. (b) The 2 guidewords HAZOP, typically used for lower risk/complexity procedures. (c) The What-if method utilized or low risk/complexity procedures with well understood tasks and hazards. (d) More quantitative methodologies such as LOPA are utilized when triggered.	Section 7.1			20	

No.	Question	Reference	Standard Status (MC/NI/DNE)	Score (0-5)	NF	Notes/Comments
2.2	**Facility Siting**					
2.2.1	Has the facility/company established requirement to perform facility siting assessments as part of the PHA?	Section 7.2				
2.2.2	Was a facility siting assessment performed as part of the PHA study? Auditor should verify following: ▪ The facility siting assessment is not merely attached to the PHA report. Consequences estimated in the PHA report should be influenced by findings in the siting assessment. ▪ Facility siting assessment included storage facilities/warehouses.	Sections 7.2 & 7.3			2	

No.	Question	Reference	Standard Status (MC/NI/DNE)	Score (0-5)	NF	Notes/Comments
2.2.3	Were recommendations resulting from the facility siting assessment implemented completely? Auditor should verify the following: ▪ Recommendations of the siting assessment is part of the PHA report (to ensure same level of urgency and monitoring) ▪ If facility siting is performed separately as a PHA recommendation, the recommendation should not be closed until all facility siting assessment recommendations are closed. Site verification should be performed by the auditor to ensure that facility siting recommendations were implemented (*e.g.*, temporary structures, such as portable buildings or trailers used during turnaround and inspection (T&I) for contractor occupancy are only placed in safe zones defined in the facility siting assessment).	Section 7.2			2	

No.	Question	Reference	Standard Status (MC/NI/DNE)	Score (0-5)	NF	Notes/Comments
2.2.4	Were facility siting assessments revalidated every 5 years along with the PHA?	Section 7.2			1	
2.3	**Inherently Safer Design (ISD)**					
2.3.1	Has the facility/company established a requirement to utilize ISD principles to reduce risk during design stage PHA studies?	Section 7.5				

No.	Question	Reference	Standard Status (MC/NI/DNE)	Score (0-5)	NF	Notes/Comments
2.3.2	Did the PHA team utilize ISD principles to reduce severe consequences for identified hazardous scenarios during the design stage? Auditor should verify that ISD hierarchy is followed by the team in the correct order: 1- Elimination: elimination of hazard. 2- Intensification: Reduction in inventory of hazardous chemicals and/or process/equipment size (*e.g.* pipe diameter, vessel size). 3- Substitution: Substitution of hazardous chemical with a safer one (*e.g.*, higher flash point, less reactive chemicals). 4- Attenuation: Reduction of hazardous conditions (*e.g.*, pressure, temperature if flammable, dilution). 5- Limitation: Reduction of consequence (*e.g.*, reducing leak volume, reducing explosion impact) 6- Simplification: Reduction of probability of error/failure.	Section 7.5			3	

<table>
<tr>
<td>STANDARD STATUS:
Meets Criteria (MC): The requirement has been properly designed and established including communication, training, measurement, verification and feedback.
Needs Improvement (NI): Requirement does not meet criteria
Does Not Exist (DNE): Requirement is missing/absent</td>
<td colspan="2">NORMALIZATION FACTOR (NF)
is set to assign suitable weight for each aspect affecting PHA quality as some have more impact than others</td>
<td colspan="2">FACILITY/COMPANY REQUIRMENTS MEETING EXPECTATIONS
Number of standards that meet criteria:
Number of standards that need improvement:
Number of standards that do not exist:</td>
</tr>
<tr>
<td>Effectiveness: The extent of conformance to established criteria and documentation, quality of execution, degree of implementation and achievement of stated objective(s).
EFFECTIVENESS SCORE:
0 = No discernible or meaningful indication that requirements are even partially implemented
1 = Minimal evidence that requirements are even partially implemented (significant gaps and weaknesses)
2 = Some portion or aspect of the requirement is present, although major improvement is needed
3 = Significant portion of requirement is implemented, with some improvements needed
4 = Most of the requirement is implemented, with minor improvements needed
5 = Standard is fully implemented</td>
<td colspan="2">Summary</td>
<td colspan="2" rowspan="3">SCORECARD SCALE:
0 = No implementation
1 – 24 = Poor implementation
25 – 49 = Mediocre implementation
50 – 74 = Average implementation
75 – 89 = Above average implementation
90 – 100 = Excellent implementation</td>
</tr>
<tr>
<td>Total:</td>
<td colspan="2"></td>
</tr>
<tr>
<td>Total Possible = ∑(5 x NF) (Note: If a question is not applicable, then use NF = 0 for that specific question):</td>
<td></td>
<td rowspan="2"></td>
</tr>
<tr>
<td>Divide “Total” by “Total Possible” x 100:</td>
<td></td>
<td>OVERALL SCORE:</td>
<td></td>
</tr>
</table>