MARSH

Energy Practice

RISK ENGINEERING POSITION PAPER – 01

PROCESS HAZARD ANALYSIS (PHA)

SOLUTIONS...DEFINED, DESIGNED, AND DELIVERED.

MARSH & McLENNAN COMPANIES

CONTENTS

1. BACKGROUND

Major accidents on energy sites have the potential to result in hundreds of millions of dollars of physical damage, present a danger to employees and the local population, and can lead to significant business interruption.

However, there are steps that can be taken to address major accident hazard (MAH) threats and minimize the risk of a serious incident as part of a comprehensive process safety management (PSM) program. A fundamental element of PSM, alongside others, such as mechanical integrity or management of change (MOC), is process hazard analysis, a key tool for understanding MAHs.

PHA encompasses several techniques to evaluate and control hazards and risk levels respective to process operations to assess the suitability and effectiveness of existing safety barriers, and to help determine whether additional barriers or risk mitigation measures are needed. Therefore, the ineffective application or absence of PHA can significantly increase overall risk levels, and as outlined in Appendix A of this paper, the lack of a rigorous PHA program has been identified as a key contributing factor in several major recent loss events within the energy industry.

Many of the PHA techniques discussed in this paper are considered to be well-established within the industry, and have been standardized with templates developed for their execution in many organizations. Each technique will have its own level of suitability and applicability, depending on a site's process maturity and complexity, as well as its overall PSM philosophy and objectives. Yet, no two PHAs are the same. The fact that a PHA is a team effort can lead to different outcomes depending on the PHA technique used and the skills and experience of the PHA Leader and team members.

2. OBJECTIVE

The objective of this position paper is to define the key attributes that would be rated by Marsh as "very good" for a PHA process in the oil, gas, and petrochemical industry. These attributes reflect those in the Marsh energy risk ranking criteria. They can be used to support and define risk improvement recommendations, and also to provide detailed advice to clients seeking to improve their management systems.

3. SCOPE

The scope of this position paper includes the development and application of a PHA process for carrying out periodic reviews of an operating asset's process safety studies, including those carried out as part of minor works or plant modifications. It is not intended to define the key attributes of a PHA or the risk assessment process as part of a larger engineering, procurement, and construction (EPC) project.

It should be noted that throughout this document, the term "site" is used to reference the part of the organization carrying out the PHA process. Depending on the nature of the organization, this could be a single plant, multiple plants on the same site, or multiple sites.

Although this document describes techniques that can be used by a site to carry out a PHA, it is not within its scope to provide detailed technique methodologies.

4. SPECIFIC REQUIREMENTS

There should be a comprehensive written policy and procedure governing the PHA process for each site as part of the site's policy for the management of major hazards. Any corporate expectations for the PHA process should communicated, made readily available to member sites, and incorporated as appropriate into the site's policy and procedures.

The policy and procedure for the PHA process should define the following elements:

- Objectives for carrying out a PHA.
- The scope of the PHA.
- The PHA technique to be adopted.
- The key roles, responsibilities, and competence requirements for those involved in the PHA process.
- Managing the PHA schedule.
- The required documentation infrastructure to enable the PHA process to operate effectively.
- The preparation required for the PHA.
- The key steps in the PHA process.

SCOPE OF PHA STUDY

A PHA study should evaluate the following:

- The process hazards.
- The identification of any previous incidents that had the potential for catastrophic consequences.
- Engineering and administrative controls applicable to the hazards and their interrelationships.
- Consequences of the failure of these controls.
- The broader considerations of facility siting.
- Human factors that apply to the effective application of barriers or controls.
- A qualitative evaluation of the effect of control failure on the safety and health of site employees.

According to the US Occupational Safety and Health Administration (OSHA), "The key provision of PSM is process hazard analysis (PHA) – a careful review of what could go wrong and what safeguards must be implemented to prevent releases of hazardous chemicals." In the EU, the scope of the PHA study will be influenced by the Seveso Directive, the main legislation addressing the control of onshore MAH threats involving dangerous substances, and by the Safety of Offshore Oil and Gas Operations Directive.[1]

THE PHA TECHNIQUE TO BE ADOPTED

Within this paper, the following definitions are used, recognizing that different organizations may have different interpretations of the techniques discussed (refer to Appendix B for further detail on these and other commonly used PHA techniques).

TECHNIQUE	COMMENT
Hazard identification (HAZID)	Identification of significant hazards to ensure that there are appropriate measures in place to eliminate or reduce the risks to tolerable levels. Can be carried out once the basic process engineering design of a project or modification is known.
Hazard and operability study (HAZOP)	A rigorous line-by-line review, this requires the piping and instrumentation diagrams (P&ID) to be finalized with a good understanding of the safety barriers that need to be adopted as part of the project, or those already installed when restudying an existing plant. If done too early in the development of the P&ID, the HAZOP can quickly degenerate into a design review.
Process hazard review (PHR)	A rigorous system-by-system review designed to operate at a higher level than a HAZOP, applying learning gained during site operation to previous versions of the PHA or HAZOP.
Safety integrity level (SIL) analysis	An assurance assessment that safety instrumented functions (SIF) provide the required safety performance and integrity. Typically carried out in parallel with a HAZOP or PHR.
Hazard analysis (HAZAN)	A quantitative analysis of a known hazard, including equipment reliability and hazard frequency data. It is most effectively done on an operating plant with known performance data, rather than using data that is either theoretical or implied. A tool also often used for SIL analysis.
Layer of protection analysis (LOPA)	A semi-quantitative tool for analyzing and assessing risk. The timing would be similar to that for a HAZOP. Like HAZAN, it is a tool also often used for SIL analysis.
Bowtie analysis	Primarily a qualitative technique, this can be carried out once details of the safety barriers to be adopted/already employed are known, even though operating data, including that for human factors, may not yet be available.
Failure mode and effect analysis (FMEA)	A systematic, typically qualitative, and methodical tabular technique for evaluating and documenting the causes and effects of known types of component failures.
"What if"	A simple-yet-structured brainstorming technique for determining likely hazards and judging the likelihood and consequences of those hazards occurring.

The PHA technique to be adopted should be the most appropriate to the potential severity of the site's MAH threats. As such, the selection of the PHA technique should consider the following criteria:

- The age and maturity of plant operations.
- The technical complexity of the site.
- The quality of available information.
- The experience and competence resident at site with using the various PHA techniques available.

Therefore, while it would be typical for a refinery or complex petrochemicals plant to conduct a HAZOP and SIL assessment every five years, a PHR with accompanying SIL may be deemed more appropriate for a chemicals facility, while a "what if" study would be more suitable for a less complex operation, such as a distribution terminal.

For a multi-unit site, it is also worth considering whether the same approach is necessary across all units. For example, it may be appropriate for less complex process operations to be studied qualitatively, while a more structured or quantitative approach is used to study those unit operations where failure of a safety instrumented system (SIS) could escalate to a major accident hazard.

The choice of the PHA technique will also depend on whether a site is seeking to carry out an update or a revalidation of an existing PHA, or whether a completely new PHA is to be carried out for an existing asset. This will depend on:

- The quality of the initial PHA (for example, if there are any deficiencies in supporting documentation or study scope, or if recent process safety information (PSI) casts doubt on the thoroughness of the initial study).

- How extensive changes to the process have been since the initial PHA. Note that the IEC 61882 HAZOP studies - Application guide refers to the need for periodic studies to "counteract the effects of creeping change."[2]
- The effectiveness of the site's management of change (MOC) program in analyzing and documenting changes carried out on the site since the last PHA (for example, plant uprating, changes to P&IDs or control/trip logic, or changes to staff training or shift coverage).
- Any recent regulatory changes.
- Company PSM standards and major accident management policy.

As noted earlier, it is the responsibility of the site to clearly state the criteria for the approach or technique taken in its PHA policy and procedure.

ROLES, RESPONSIBILITIES, AND COMPETENCE REQUIREMENTS

The PHA is best performed by a team with expertise in engineering and process operations, including at least one employee who has experience with and knowledge of the operation of the process being evaluated. Therefore, although it may be appropriate for the team to be led by an external specialist knowledgeable in the specific analysis technique(s) being used, it is not appropriate to outsource the PHA process to be managed and executed exclusively by a third party.

Each site will likely have its own organizational structure and may have different titles for the key PHA team roles within that organization. It should also be acknowledged that there is likely to be a "core team" for the duration of the study process, with specialists brought in for individual sessions to answer specific points.

It is expected that, for all key roles, the competence expectations for carrying out the PHA are defined by the site and documented within the individual job descriptions and associated competence matrices.

ROLE	COMMENT
PHA process owner	The person who takes overall ownership for implementing and managing the PHA process locally, while taking cognizance of any corporate procedures and policies. This person will typically: • Produce a written proposal for initial approval. • Ensure that the key people are involved at the right times. • Ensure that the process has been followed properly. • Ensure that all actions arising from the process are effectively managed to completion. The most common process owners will likely be the process safety managers, or senior engineers associated with the technical or safety functions.
PHA leader	An experienced PHA practitioner who has attended specific formal training in leading process hazard analyses. The PHA leader may be from inside the site, corporate organization, or from a recognized third-party specialist organization. If third parties are employed to lead PHAs, the site should fully verify the third party's experience and competence. They will need to be familiar with a range of hazard identification, hazard and risk assessment, and quantification techniques. The leader will advise on the selection of the PHA team and ensure the adequacy of the information recorded for the study. They will also need to ensure that the validity of declared safety barriers is thoroughly tested as part of the PHA process.
PHA scribe	The PHA leader will often appoint a separate person to facilitate note taking during the PHA process.

Discipline engineers	Several specialist engineering disciplines (for example, plant process engineer or distributed control system (DCS) engineer) will input into the PHA process. However, they may come in and out to address specific technical issues. They may need their input to be checked or verified by the corresponding technical authorities on site, depending on their level of seniority or experience.
Operations representative	An effective PHA process requires detailed understanding of the plant process and equipment being studied. It also requires contributions from people who are directly involved with the plant operations and understand what actions are required to be taken in the first instance following plant abnormal operation. To that end, the operations representative attending the PHA will typically be an experienced operator or operations shift supervisor. The representative will advise on site operating and maintenance preparation requirements and validate any assumptions made in hazard analyses on the suitability, validity, or applicability of safety barriers, including operating methods, proof testing of instruments, repair times for equipment, etc.
Technology specialists	The PHA may require input from specialists such as process chemists, catalysis experts, or corrosion engineers. This will likely only be required for the assessment of specific sections of the process.
PHA auditors	The site should identify and appoint suitably competent and experienced personnel to audit the PHA process to ascertain compliance and identify areas of improvement. For large multi-site organizations, these may be corporately-appointed.

It is important that all of the key personnel involved in the operation of the site's PHA process understand its importance within the site or corporate PSM structure, as well as their individual and team responsibilities. All PHA participants should receive an appropriate level of training, dependent on their responsibilities within the PHA. This may include general training for discipline engineers and operations representatives in advance of a PHA to ensure that they have an outline understanding of the PHA process and procedures. Appropriate training should also be given to those taking part in a PHA for the first time, and consideration should be given to the need for regular refresher training, particularly for infrequent PHA attendees. If the site has a role within the organization that takes overall responsibility for the PHA process, this individual should lead the training for the other participants.

MANAGING THE PHA SCHEDULE

The time period between the first PHA and subsequent revalidation reviews will typically be influenced by overall site process complexity, the magnitude of potential MAH, and local regulatory requirements. Because of the significant resource requirements for carrying out a PHA, five years is typically seen as the maximum time before a revalidation review or new PHA should be carried out. This is the review period enforced in the US by the OSHA PSM standard 29 CFR 1910.119.[3,4,5]

The site should also identify and document the order for studying its plants or process units. This will typically be based on hazard severity, the number of potentially affected employees, the age of the process, and the operating history of the process.

The requirement to review the suitability of the site's wider PHA studies should be included in the site's change management program, such that the potential knock-on effects of any change or project on the site's risk profile is examined. This is particularly relevant for significant plant modifications that could have far-reaching effects beyond the immediate vicinity of the modification, and may mean a process unit-specific or site-wide PHA revalidation review will need to be conducted earlier than would otherwise be mandated by the site's PHA policy and procedure.

DOCUMENTATION INFRASTRUCTURE REQUIREMENTS

An appropriate system is required to record the inputs to and outputs from the PHA, including the management of action items.

MANAGING THE PHA INPUTS

The documentation system for managing inputs can take various forms, but must be designed for the following inputs to be appropriately documented:

- Overview information of the plant or process being studied.
- Key individuals involved in the PHA study.
- Evidence generated during the process defining the existing risk mitigation measures, layers of protection, and safety barriers such as loss control elements, safety critical equipment, critical procedures, and critical tasks.
- Where there are known gaps within the current layers of protection and the actions required to close them.

During the PHA process, the PHA leader should use his/her judgement on how long to debate a topic before an action is assigned. Once a discussion has gone beyond a certain time limit (for example, 10 minutes) then the process should move to the next point and an action generated.

MANAGING THE PHA OUTPUTS

The PHA can generate a significant number of actions, particularly in the first revalidation cycle or complete re-study, although subsequent revalidations will typically generate fewer and fewer actions.

All of these actions need to be effectively managed, and this can only be done if they are SMART – that is, specific, measurable, achievable, relevant, and time-bound. The documentation system chosen to manage the actions must take the following into consideration:

- The PHA outcomes, findings, and associated actions can be effectively communicated to all personnel impacted by the PHA, for example, process operators.
- Each action is assigned a unique identifier number, with a defined date and a clear expectation of requirements for closure.
- The status of each action can be tracked, meaning any overdue can be easily identified.
- The required action approval authority is defined.
- The evidence associated with action closure is documented, or, if the action is rejected by the approval authority, the reasons why, and what further action is required to permit closure has been noted.
- Any modification, such as an extension to the closure date, is clearly documented.

Where the site's PHA process extends across several units or plants, the process for recording actions should be consistent across all plants, and ideally, the documentation system should allow for an overview of all site actions.

PREPARATION FOR THE PHA

ENSURE UP-TO-DATE PROCESS SAFETY INFORMATION (PSI)

Good quality PSI is the foundation of a good PHA study, and the site should ensure that its written PSI is up to date before conducting a PHA, particularly that for P&IDs. Once the quality of the information is confirmed, the site may need to update this information prior to carrying out the PHA, or adjust its preferred approach to the study if it is clear that the PSI is not of the desired quality. In this case, a site can still get value from its preferred PHA technique, but must consider adjusting the technique by adding additional experienced personnel to the process, or giving extra time and consideration to critical areas where the data is incomplete.

Access to quality PSI will help the site identify and understand the hazards posed by processes and technologies involving highly hazardous chemicals. The site should have ready access to the following:

TYPE OF PSI	EXAMPLES
Information on chemical hazards	• Toxicity and permissible exposure limits. • Physical, reactivity, and corrosivity data. • Thermal and chemical stability data. • The hazardous effects of inadvertent mixing of different materials, that is, potential chemical interactions.
Process and technology information	• Up-to-date P&ID and electrical classification drawings. • A block flow diagram or simplified process flow diagram. • Material and energy balances. • Process chemistry. • Process inventory and design operating conditions. • Materials of construction. • Design codes and standards employed. • Up-to-date standard operating procedures (SOP) and emergency operating procedures (EOP), for describing operator response to normal and abnormal operations. • Understanding of the process's corrosion and damage mechanisms. • Safe upper and lower limits for process parameters (for example, temperature, pressure, flow, pH, or composition). • Relief system design and design basis. • Emergency depressuring and shutdown system design. • Other safety systems (for example, gas detection or fire suppression systems).
Other	• Management of change (MOC) documents for changes carried out since the last PHA study. • Incident investigation reports for process safety-related incidents and near-misses since the last PHA study. • Previous PHA studies (this may include studies from other similar units).

SETTING THE ENVIRONMENT

Setting the right environment for any PHA is paramount to enable the process to run as efficiently as possible and to get the most out of the people attending.

Studies can take a considerable period of time, so should be scheduled in an appropriate location to ensure that attendees are distracted as little as possible. The program of PHA meetings should include sufficient breaks and opportunities for refreshment.

KEY STEPS IN THE PHA PROCESS

The PHA revalidation process for each site will be different, depending on local regulatory and compliance requirements, as well as the maturity of the operating plant. However, the process should broadly follow these key steps:

REVIEW ALL MODIFICATIONS MADE TO THE PROCESS SINCE THE PREVIOUS PHA

To make sure the PHA revalidation accurately reflects the hazards of the site's current processes, the revalidation team should review all modifications since the previous PHA and determine if an additional analysis is needed. This should include reviewing records of implemented recommendations from the previous PHA and any incident reports and compare these to the MOCs.

If the hazard evaluation performed during a modification was either inadequate or uncertain, then the team should review this change as part of the wider PHA process.

In instances where the process identifies several modifications that do not have corresponding MOC documentation, this may be an indication that the MOC process has not been implemented effectively and the team may need to consider redoing the PHA rather than updating or revalidating it.

Depending on how human factors have been addressed in the previous PHAs, the team should review any assumptions made in the past and consider how these might have been affected by site changes and modifications. These include:

- Operator training, for example, in response to abnormal operating scenarios.
- The suitability of SOPs and EOPs and the application of critical task analysis.
- Control room ergonomic factors.
- Personnel workload/stress.
- Labelling/housekeeping.

REVIEW PREVIOUS PROCESS SAFETY INCIDENTS

The PHA revalidation team should also review the site's process safety incidents and near misses since the previous PHA, as well as learnings from relevant external incidents (for example, from sites using similar processes or technology), in order to ensure that potential hazards are identified, as well as the adequacy of existing safety barriers.

REVIEW THE STATUS/RESOLUTION OF PREVIOUS PHA RECOMMENDATIONS

The team should make sure all previous recommendations have been closed out. It would be good practice for the team to review a sample of past responses to ensure that the closure process has been robust. Any recommendations or actions not closed out should be further reviewed to make sure that the recommendation is still valid in light of the current PHA process.

ADDRESS HAZARDS ASSOCIATED WITH ABNORMAL OPERATING MODES

The PHA process should include a systematic means of assessing both normal and abnormal operating modes. The hazards involved during start-up, shutdown, maintenance, sampling, etc. in a process unit should be evaluated to help identify procedural or equipment deficiencies that could contribute to human errors.

It is not unusual for initial PHAs or hazard studies to incompletely address hazards during non-routine operation. As a result, the PHA revalidation team may need to augment the previous PHA by performing this task, either as a standalone hazard analysis, or by incorporating guidewords within the revalidation PHA to include abnormal operation such as start-up, shutdown, etc.

ENSURE COMPLIANCE WITH CURRENT PHA REGULATORY REQUIREMENTS

The revalidation team should look at the following, and determine what additional information needs to be added to any previous PHA to make it compliant; the team should also identify the tasks required in order to obtain that information:

- The effect of any new or existing regulatory requirements on the site's PHA.
- The effect of any new or existing industry standards.
- The effect of any new or existing internal company requirements.

5. STEWARDSHIP OF THE PHA PROCESS

The health and performance of the PHA process should be regularly monitored and assessed using both a routine review of key performance indicators (KPIs) and periodic audits. These steps will help assure the site management team that the system is being used in the way it is designed and intended.

KPIs

Each site should routinely produce both leading and lagging KPIs to monitor the performance and health of its PHA process. The KPIs should be produced at least once per month and be reviewed at an appropriate site management forum. Routine leading KPIs would typically include:

- The total number of planned PHAs completed/overdue as per plan.
- The number and proportion of open and overdue PHA actions, by severity/risk category.
- PHA procedure compliance as per audit.

Lagging indicators might include the number of process safety incidents on a plant where incomplete or inadequate PHA is identified as a contributing cause.

AUDITS

Each site should audit its PHA process periodically, typically annually. The audit should be performed by a small team knowledgeable in the application of the PHA process. Consideration should be given to including people from outside the immediate local site in the audit process. Findings from the audit should be reported to site management, possibly through forums such as the site process safety management committee.

An audit process would typically include:

AUDIT STAGE	QUESTIONS TO CONSIDER
Evaluating the PHA Process	• Is there a scheduled plan for ensuring all relevant plant areas are included in the PHA process, with defined timescales? • Has a competent PHA leader been identified and appointed? • Are all key personnel identified and invited to attend? Are there any key personnel (such as technology specialists) omitted? • Are key preparation requirements established and study preparation materials (such as process descriptions or standard and emergency operations procedures) distributed?
The PHA study	• Are the appropriate risk assessment and quantification processes being selected? • Are the processes being followed properly and thoroughly? • Is there an appropriate level of documentation for risk mitigation measures? • Are the actions raised SMART (specific, measurable, achievable, relevant, and time-bound)? Do they address the risk gaps identified?
Managing the actions	• Are actions being closed out by the appropriate approval authorities? • Are actions being completed in a timely manner? • Is the action documentation sufficient to give a full account of either why the additional risk reduction measures presented are appropriate, or why no further action is required?
Personnel related	• Do the key personnel understand the process? • Do they understand their roles and responsibilities? • Have they been trained?

5. REFERENCES

1. EU Safety of Offshore Oil and Gas Operations Directive, Document 32013L0030, Directive 2013/30/EU of the European Parliament and of the Council of 12 June 2013.

2. BSI, 2016, Hazard and Operability Studies – HAZOP Studies – Application Guide, BS IEC 61882:2016, British Standards Institution.

3. United States Department of Labor Occupational Safety and Health Administration (OSHA) standard 29 CFR 1910.119 - Occupational Safety and Health Standards.

4. Process Safety Management - U.S. Department of Labor Occupational Safety and Health Administration OSHA 3132.

5. Process Safety Management Guidelines for Compliance - U.S. Department of Labor Occupational Safety and Health Administration OSHA 3133.

6. The Report, The BP U.S. Refineries Independent Safety Review Panel, January 2007.

7. State of California. *Department of Industrial Relations, Notice of Citation*, available at https://www.dir.ca.gov/dosh/citations/ExxonMobil.Signed-Citation-Documents.1042440.pdf, accessed 1 February 2018.

8. US Department of Labor. *Occupational Safety and Health Administration, Stipulation and Settlement Agreement*, available at https://www.osha.gov/enforcement/cwsa/phillips-66-company-08221991, accessed 1 February 2018.

9. US Chemical Safety Board. Final Report: Williams Olefins Case Study, available at http://www.csb.gov/williams-olefinsplant-explosion-and-fire-/, accessed 1 February 2018.

10. IEC 61508, Functional Safety of Electrical / Electronic / Programmable Electronic Safety-related Systems.

11. The Report, The BP U.S. Refineries Independent Safety Review Panel, January 2007.

12. Ibid.

6. APPENDICES

APPENDIX A: INDUSTRY LOSSES

Examples of industry losses where the lack of a rigorous PHA program has been identified as a key contributing factor:

INDUSTRY LOSS	LOSS	COMMENT
Pasadena, US, 1989	23 fatalities following a polyethylene plant explosion and fire.	Following the incident, the operator agreed with OSHA to conduct a PHA utilizing a methodology that would best address the hazards of the particular process at issue.[8]
Longford , Australia, 1998	A US$1.3 billion, major property and business interruption loss.	One of the root causes was that a retrospective HAZOP planned for Gas Plant 1 for several years had not been completed. Further, that a 1992 modification had only been completed with a HAZOP which had limited scope. The Royal Commission viewed it as inconceivable that a HAZOP study would not have revealed factors which contributed to the incident.
Texas City, US, 2005	15 fatalities, major property and business interruption loss.	The Baker report[6] into the loss recommended that the site management "should not rely solely on audits, rather also on PHA, near misses, high potential incidents, MOC reviews, inspections."
Point Comfort, US, 2005	Property damage of US$85 million, plus five months' shutdown.	Vehicle impact (a primary cause of the loss) was not picked up as part of the site's hazard review process.
Jaipur, India, 2009	11 fatalities, the tank fire burned for 11 days.	The investigation committee into the incident stated that "loss of containment in terms of time and quantity was never considered a credible event and accordingly not taken into account in hazard identification. Also that "...only one HAZOP study has been done on the installation...The report, though titled "HAZOP study," does not include any HAZOP work but contains "consequence analysis."
Geismar, US, 2013	Two fatalities following an olefins plant explosion, giving US$110 million property damage plus extensive business interruption loss.	Following the incident, the US Chemical Safety Board concluded that "...deficiencies in implementing the site's process safety management programs include...poor implementation of PHA action items.... Those deficiencies ultimately contributed to the reboiler rupture and the deaths of two employees."[9]
Torrance, US, 2015	Fluidized catalytic cracker explosion giving major property and business interruption loss and a US$566,600 fine.	Citation 11 Item 1 by the State of California states: "On and prior to February 18, 2015, the employer failed to perform a Process Hazard Analysis PHA for identifying, evaluating, and controlling hazards in the electrostatic precipitator (ESP) operating with broken and bypassed safety critical devices.....during the FCC emergency shutdown."[7]

APPENDIX B: COMMON PHA TECHNIQUES

HAZARD IDENTIFICATION (HAZID)

The HAZID is designed to identify significant hazards present within the unit, and ensure that there are appropriate measures to eliminate the risk or reduce the risk to tolerable levels (ALARP).

This is typically a hazard-based top-down approach, designed to either revalidate major accident scenarios, initiating events and safeguards, or to identify potential new exposures following a site-initiated change. Identification of the hazards provides the opportunity for unit or equipment redesign to eliminate or significantly reduce the risk, but, where the risk cannot be reduced to tolerable levels by practicable redesign, additional protective measures may need to be incorporated to meet the relevant criteria.

By its nature, the HAZID will identify any new scenarios or MAHs that need to be documented and would prompt a revision of the site's hazard register.

HAZARD AND OPERABILITY STUDY (HAZOP)

The HAZOP is probably the most common rigorous technique used for carrying out a PHA within the energy industry. This is often because it is a process which would likely (depending on asset age) have been carried out during the initial site design stage. It uses fully developed P&IDs to identify hazards and operability problems, and process deviation guidewords to stimulate creative thinking about possible deviations and their effects. Within an EPC project, a HAZOP would typically follow a HAZID in the project timeline.

This is a rigorous deviation-based bottom-up approach, in which the site will likely have its own trained HAZOP leaders. However, because it is highly structured, caution must be used when using this to revalidate an existing study to ensure that in following the existing guidewords, the process does not result in merely repeating the previous study, but is also able to identify new hazards or exposures.

The HAZOP structure will support parallel SIL studies, the review and update of site P&IDs, and the identification of opportunities for further site risk reduction. However, HAZOPs are invariably time consuming, and can present a major resource challenge for an operational plant. As discussed earlier in this report, it is important that non routine activities, such as start-up or shutdown, are included in a HAZOP, alongside normal operation.

PROCESS HAZARD REVIEW (PHR)

The PHR technique is a systematic and comprehensive study of hazardous events. But, where the HAZOP is a line by-line approach, the PHR operates at the higher system-by-system level, using hazardous event guidewords, showing some similarities in this respect to the HAZID approach.
It is typically a hazard-based top-down approach, and while it not as rigorous as a HAZOP, its higher-level view of the process offers considerable time savings and does not require detailed P&IDs. A unit flowsheet or process flow diagram will often suffice.

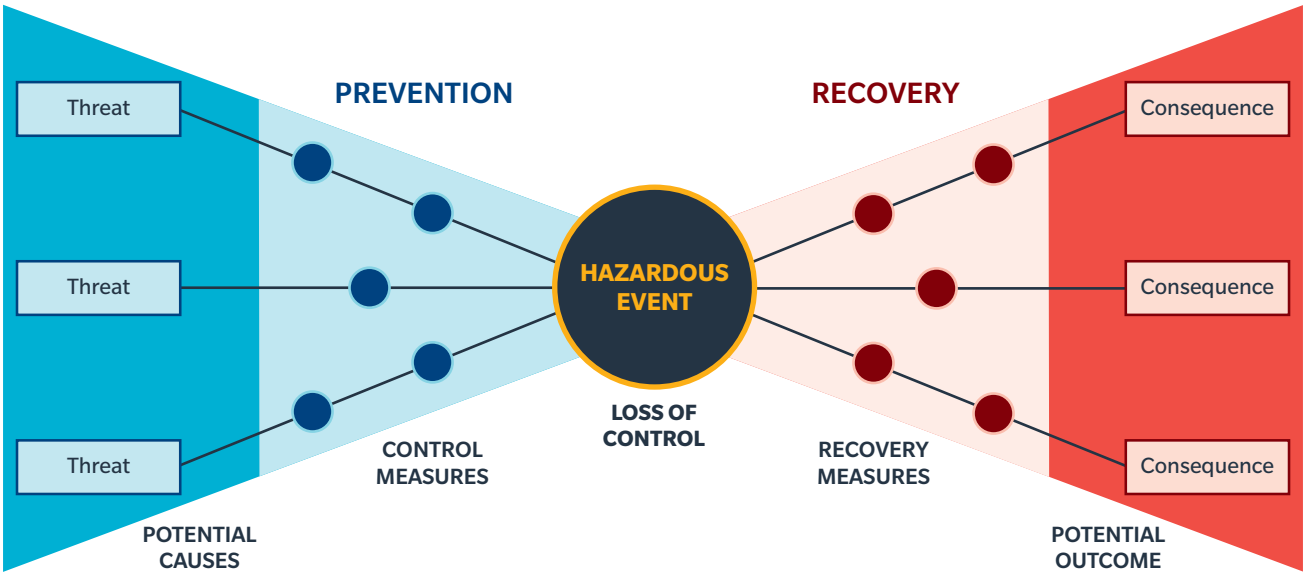
The PHR technique, therefore, will typically develop what had already been documented through the site's original hazard studies, adding what has been learnt since, such as learning from incidents, or changes made upstream or downstream of the original studies.

BOWTIE ANALYSIS

The bowtie technique is typically a structured qualitative analysis, used where a quantitative approach is neither possible (for example, through a lack of data), nor desirable. We are, however, seeing more examples of this approach being used quantitatively as sites become more familiar with the methodology and gain access to data on barrier and control performance. When used qualitatively, the process gives a visual presentation of the number of barriers or controls for MAH prevention and mitigation, as shown in the following example:

The hazardous event to be studied would typically be identified in a HAZID, therefore, this technique is most powerful once the site's MAHs are known and understood. The bowtie diagram then combines a study of the threats that can cause the event (that is, the fault tree, typically drawn on the left hand side) with a study of the consequences (that is, the event tree, typically drawn on the right hand). The process then continues to identify protecting barriers, as either controls which look to prevent the threats from occurring, or as recovery or mitigation measures which look to reduce the potential impact.

One of the strengths of the bowtie analysis is that it can show the site's overall response to an MAH scenario, combining hardware (such as SIS), software (such as the operator's response to an initiating event), and emergency response and recovery measures in a single process illustration.



SAFETY INTEGRITY LEVEL (SIL) ANALYSIS

Safety instrumented systems are often used to provide a level of risk reduction in relation to one or more hazardous events. If instrumentation is to be effectively used in this capacity, it is essential that it achieves appropriate standards of reliability and performance. The setting of standards and performance levels is formalized in the International Standards IEC 61508[10] and IEC 61511[11] IEC 61511 requires that in addition to providing risk reduction for hazardous events with a consequence associated with the protection of people, the SIL assessment procedure should also be used where it involves protection of the environment. The procedure may also be used for other applications involving asset protection or other business loss.

SIL analysis can be carried out by various techniques and is often done alongside a HAZOP or PHR, as it usually requires the same disciplines to be present. The techniques of hazard analysis (HAZAN) and layer of protection analysis (LOPA) are discussed in greater detail below. Although risk graphs are commonly used for SIL analysis, they are typically only recommended for initial "risk screening", and therefore they are not discussed further in this paper.

FEATURE	RISK GRAPHS	LOPA	HAZAN
Level of complexity and sophistication.	Low	Medium	High – requires experienced, specified practitioners.
Use for initial screening?	Yes – very quick	Yes	No – too complex
Typical study time, per instrumented loop.	A few minutes	One hour	One day
Suitable for detailed analysis?	No	Yes – up to a point	Yes
Identifies potential dependency between barriers?	No	Yes – identifies but does not quantify	Yes
Able to include specific human factors aspects?	No	Yes	Yes
Output	SIL	PFDa[1]	PFDa[1]
Further comment	Technique does not lend itself to recording the basis of any decisions.	See below.	See below.

1. Probability of Failure on Demand, average value.

HAZAN

This technique is the most rigorous and most flexible of the SIL methodologies available. It can, however, be the most time consuming, and requires considerable training and experience to be used effectively.

It uses two complementary techniques: demand trees and fault trees. The technique of demand trees is a systematic way of identifying the potential initiating causes for a particular specific hazardous event. Fault tree analysis allows the initiating causes to be represented with their respective risk reduction measures. It also allows the identified dependencies to be included in an appropriate manner.

HAZAN therefore enables the risks associated with a particular hazard to be calculated, helping to clarify:

- Is the level of risk acceptable?
- Is a particular expenditure justified?
- What hazardous events present the greatest risk, and therefore should be prioritized?
- Which design is the safest or most reliable?

HAZAN provides a rational method of assessing risks so that decisions can be made with a greater element of certainty. It is typically the best technique for complicated SIS where there may be common cause failure and human factors issues.

LOPA

LOPA is the most common technique used for SIL analysis, as it strikes a balance between the time required for the analysis, the level of accuracy, and the documentation detail. Although it can be used in a relatively simplistic screening manner, it can also be used in a more quantitative manner, with a level of detail not dissimilar to a HAZAN using fault trees. Its format also lends itself to being used alongside a HAZOP or PHR.

The methodology for SIL analysis follows the broadly accepted approach as laid down in the standard IEC 61511.[12]
The principle steps are as follows:

- Identify the specific hazardous event.
- Determine the severity and target frequency.
- Identify the initiating causes.
- Scenario development.
- Protective measure and condition modifier listing.
- Completion of LOPA standard pro forma / spreadsheet.

However, care should be taken as it is generally not sophisticated enough by itself above SIL, or when studying catastrophic or very rare events, where a HAZAN would be more appropriate.

FAILURE MODE AND EFFECT ANALYSIS (FMEA)

This is a systematic, typically qualitative and methodical tabular technique for evaluating and documenting the causes and effects of known types of component failures, particularly those involving electrical and mechanical processes. As a top-down tool, it is less effective than fault tree analysis, but when used as a bottom-up tool, FMEA can augment or complement fault tree analysis and identify more causes and failure modes resulting in top-level symptoms.

However, it is not able to discover complex failure modes involving multiple failures within a process, and does not question the original design basis of the process.

As a PHA technique, it is perhaps most effective as a higher-level screening tool to rank potential scenarios, or for evaluating “one cause” events in low-complexity units.

“WHAT IF” ANALYSIS

“What if” analysis is a structured brainstorming technique for determining likely hazards, and judging the likelihood and consequences of those hazards occurring. It is a simple technique, relying heavily on the experience and intuition of the review team, and is more subjective and less detailed than a HAZOP. While it is relatively easy to use and can be an effective tool, the outcome will depend heavily on the quality of the questions asked.

As a PHA technique, this is perhaps most effective as a higher-level screening tool, or for evaluating well-understood events in low-complexity units.

APPENDIX C: SELF-ASSESSMENT CHECKLIST

The following checklist can be used to test a site's existing PHA process against industry good practice.

ITEM	Y	N	PARTIAL
SETUP AND APPLICABILITY			
Does the site have a formal, written procedure for carrying out PHAs?			
Does it clearly identify when a PHA should be carried out?			
Does it define the most appropriate processes for the assets covered?			
STAFFING			
Does the PHA process define the roles and responsibilities of the key people who operate the process:			
– Process owner?			
– PHA leader?			
– Discipline engineers?			
– Operations personnel? – Technology specialists? – PHA auditors?			
KEY STEPS			
Does the PHA process address the following:			
– The process hazards?			
– The identification of any previous incident that had the potential for catastrophic consequences?			
– Engineering and administrative controls applicable to the hazards and their interrelationships?			
– Consequences of the failure of these controls?			
– Facility siting?			
– Human factors?			
– A qualitative evaluation of the effect of control failure on the safety and health of site employees?			
– Ensure up-to-date process safety information?			
– A review of all modifications made to the process since the previous PHA?			
– A review of the status/resolution of previous PHA recommendations?			
– Address hazards associated with abnormal/transient operating modes?			
– Ensure that the PHA meets the requirements of any existing or new regulations, industry standards, or internal company requirements?			
SUPPORTING INFRASTRUCTURE			
Does the site have a structured way to document the PHA process?			
Does the site have a structured way to document and manage actions generated by the PHA process?			
Does training exist for the key people involved in operating the PHA process?			
Have all of the key people had this training, and are they still considered competent, or is refresher training required?			
STEWARDSHIP AND GOVERNANCE			
Are KPIs describing the operation of the PHA process routinely generated?			
Are they reviewed by senior level staff at an appropriate forum?			
Is an audit of the PHA procedure performed at least as frequently as the PHA process cycle?			
Are the outcomes of audits reviewed by senior level staff at an appropriate forum?			
Is there evidence of any corrective action being implemented following audit findings?			

MARSH