

Avoiding Quality Pitfalls for HAZOP/LOPA Sessions and Documentation

Steven T. Maher, PE CSP
Risk Management Professionals
Steve.Maher@RMPCorp.com

Carine M. Black
Risk Management Professionals
Carine.Black@RMPCorp.com

Morgan T. McVey
Risk Management Professionals
Morgan.McVey@RMPCorp.com

Prepared for Presentation at
American Institute of Chemical Engineers
2019 Spring Meeting and 15th Global Congress on Process Safety
New Orleans, Louisiana
March 31 – April 3, 2019

AIChE shall not be responsible for statements or opinions contained
in papers or printed in its publications

Avoiding Quality Pitfalls for HAZOP/LOPA Sessions and Documentation

Steven T. Maher, PE CSP
Carine M. Black
Morgan T. McVey

Risk Management Professionals

Keywords: PSM, RMP, CalARP, SMS, Process Safety, PHA, HAZOP, LOPA, Quality

Abstract

Although Process Safety Management (PSM), requiring a high-quality Process Hazard Analysis (PHA), was promulgated in the United States in 1992, and HAZOP Study techniques date back to the mid-1970's, the HAZOP Methodology (and companion techniques such as LOPA) can still present challenges in consistently applying PHA in a high-quality fashion. Many challenges can exist for the implementation of PHA, and each PHA is unique due to variables such as team composition, the HAZOP/LOPA facilitator, process unit history and past incidents, regulatory environment, safety culture, and available and accurate process safety information. These variables can have a significant impact on the HAZOP/LOPA results; however, the value of HAZOP/LOPA sessions and quality/usability of resultant HAZOP/LOPA documentation is a critical objective. The primary responsibility for achieving this objective must fall on the shoulders of the facilitator to provide streamlined support to navigate through the PHA process while accurately capturing team discussions with the necessary level of detail. Key topics addressed within the paper include:

- Quality objectives, including content and structure conducive to subsequent HAZOP/LOPA usage/updates
- Need for uniform, high-quality application
- Experienced-based tips for driving high-value sessions and for developing high-quality HAZOP/LOPA documentation
- Checklist for assessing the quality of individual HAZOP/LOPA Studies
- Key indicators that a reviewer can use to validate the acceptability of the HAZOP Study
- Structuring HAZOP/LOPA to support other PSM elements and safe plant operation

It is not the intent of this paper to provide basic PHA training, but to focus on key tips to address commonly-observed, and readily-rectified, PHA deficiencies. We have attempted to list the most common quality challenges observed from the work of even experienced HAZOP/LOPA Facilitators, and this can also provide a basis for characteristics to look for by a Quality Assurance Reviewer.

1. Focus on Objectives – Why is a Quality Process Hazard Analysis (PHA) Important?

Most people attempt to avoid undesirable outcomes and organize their actions to minimize risk; however, very few of us apply a structured evaluation of potential undesired outcomes to avoid. Whereas this may be a personal decision for the individual, this is unacceptable for a complex process system like a refinery, where the undesired events can have impacts well-beyond the individuals directly involved. These events may be rare and involve a complex set of initiating events and failure of safety/mitigation systems; thus, it is necessary to perform periodic and thorough evaluations.



FIGURE 1.1 – Tragedies to Avoid

The December 2, 1984 Methyl Isocyanate (MIC) release from the Union Carbide Bhopal Facility is considered a pivotal event in catalyzing the application of Safety Management Systems (SMS) approaches to enhance process safety. The MIC release and the magnitude of the tragedy drew the attention of industry, the public, and the regulatory community to the potential consequences associated with process safety events (Figure 1.1). Industry's response was swift and definitive. The American Institute of Chemical Engineers (AIChE) founded the Center for Chemical Process Safety (CCPS) in 1985, recognizing that the most effective mechanism for addressing process safety was not the application of additional prescriptive mechanisms, or by addressing any specific action, but by effecting fundamental business (i.e., safety culture and management systems). CCPS Guidebooks are currently considered key references in conveying the technologies needed for process safety, and the first CCPS Guidebook ("Guidelines for Technical Management of Chemical Process Safety"[2]), published in 1987, was designed to address this pressing need.

A key part of managing process safety has always been the identification and understanding of potential hazards and their consequences. This need pushed practical techniques for hazard identification, i.e., the Hazard and Operability (HAZOP) Study, developed in the decades prior to the Bhopal tragedy, to the front lines in the effort to manage process safety.

2. Brief History of Key PHA Techniques and Regulatory Requirements

Although there are quite a few tools in the PHA toolkit, the team-oriented, patterned-brainstorming sessions associated with HAZOP Studies[3] are generally considered the workhorse of the industry (Figure 2.1). Layer of Protection Analysis (LOPA)[4], frequently integral with the HAZOP Study, is a complementary tool that provides additional details on failure probabilities and conditional

modifiers. HAZOP Studies provide a foundation for scenario identification and high level development, while LOPA provides a consistent and more quantitative framework for further analysis of applicable high-risk scenarios to reveal additional insights, some of which can be directly used for identifying appropriate reliability targets for key safety features. Although HAZOP Studies have been a core part of an acceptable hazard evaluation process referenced in various industry guidelines[2,3], as well as regulatory requirements such as Process Safety Management (PSM)[5] and Risk Management Programs (RMP)[6] for onshore facilities in the United States, LOPA is a relatively new tool that simplifies Quantitative Risk Assessment (QRA) techniques to a manageable level to facilitate usage. LOPA applications are gradually becoming best practice for addressing higher consequence/risk events and are especially useful for an initial assessment of the reliability needed for key safety systems. As well as LOPA being an industry-accepted practice for important applications, for California Refineries, PSM[7] and the California Accidental Release Prevention (CalARP) Program[8] require the development of Safeguard Protection Analysis (SPA), with LOPA as an acceptable tool.

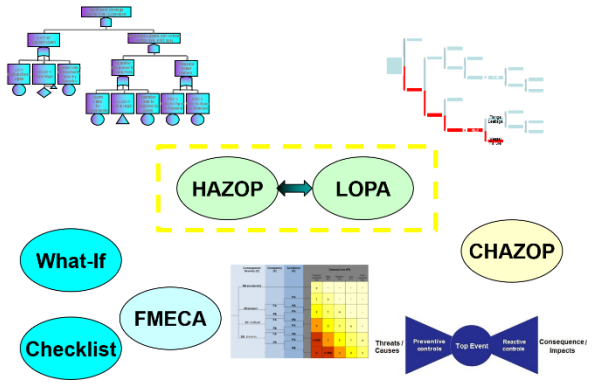

FIGURE 2.1 – HAZOP & LOPA are Core Elements of Hazard Evaluation

Although the core HAZOP has been relatively constant, HAZOP and LOPA applications have been evolving to accommodate higher expectations of both regulators and industry practitioners with respect to quality and level-of-detail. There are fundamental quality requirements that must be met to achieve regulatory compliance, but just as "beauty is in the eye of the beholder," some quality parameters pivot on the objectives of the potential applications anticipated for the HAZOP/LOPA.

Thus, the first step before convening the team and starting on the first scenario is to outline a clear definition of objectives.

3. Defining Objectives

The core objectives of all hazard identification exercises (e.g., HAZOP/LOPA) are to uncover potential weaknesses/vulnerabilities in system design/operation that could result in an undesired outcome (e.g., injury, environmental impact, equipment damage, operational impact, or compromised company reputation). Part of this analysis is to challenge the reliability of applicable safeguards to ensure adequate mitigation for potential process upsets. A quality PHA can address a variety of objectives supportive of successful plant operation:

- Protecting plant personnel, the nearby community, and the environment
- Addressing SMS regulatory requirements

- Providing insight regarding safety/operational/financial advantages/disadvantages of design and operations options
- Facilitating Management-of-Change (MOC) evaluations
- Prioritizing Mechanical Integrity (MI) Program elements and covered equipment
- Formulating Safety Integrity Level (SIL) requirements for Safety Instrumented Functions
- Providing input/verification of operating limits and Operating Procedures with respect to consequences of deviation
- Providing training to inexperienced personnel in the design intentions, expected operation, and potential hazards of the facility
- Supporting safety system design bases and required safety functions
- Providing a strong foundation for future PHA updates
- For capital projects, optimizing the design while minimizing associated costs

The value-add benefits listed above are just some of the ways in which a high quality PHA can streamline independent but related PSM efforts. All too often, the mentality of "checking the box" for a regulatory requirement leads to a poor-quality PHA, which greatly limits its potential future usability, resulting in lost opportunity costs, not to mention, potential regulatory deficiencies.

4. Planning and Preparation Essentials for Supporting a Quality PHA

Success in the development of a quality PHA can be compromised even before the PHA Team Session begins due to poor planning and/or inadequate preparation. Reference 10 can be accessed for additional planning and preparation tips (and timing) that includes the following key elements:

- **Ensure attendance of key personnel during PHA Team Sessions** – Qualified, experienced, knowledgeable, and prepared technical experts (Engineering & Operations) who participate in all phases of the PHA are critical. Ensure Team Member availability for the entire duration of the study for consistency. Table 4.1 identifies the key disciplines useful for any HAZOP/LOPA Team. Don't wait to the last-minute to schedule necessary personnel. Sometimes the best contributors for the PHA are some of the busiest individuals at the plant.
- **Venue logistics conducive to teamwork** – HAZOP/LOPA sessions may be best conducted offsite to facilitate focus. The meeting room layout should be supportive of constructive interaction.
- **Completeness-verification and, as appropriate, field-verification of key design information made available to the PHA Team (e.g., P&IDs, PFDs, Cause & Effect Matrices, Electrical Area Classification Drawings)** – Table 4.2 provides a checklist of key information requirements for a HAZOP/LOPA.
- **Software preparation, including population of key causes, is contributory towards:**
  - PHA Completeness and Organization

- Streamlined Session Time: Causes Prepopulated from P&IDs for Quick Location of Relevant Scenarios During the Session
- Sensible Grouping of Causes for Effective Future Use and Update

Populating key causes can also provide a vehicle for sending a "preview" of key issues to be evaluated during the HAZOP Study to participants, so they can be better prepared to provide definitive feedback.

- **Qualified, experienced, and prepared PHA Facilitator** – Having a competent PHA Facilitator can make or break a HAZOP/LOPA Study. The following characteristics are essential:
  - Understanding engineering first principles and the HAZOP/LOPA Methodology in order to provide effective guidance to the team
  - Understanding when the team has reached the limits of what they can accomplish
  - Managing team dynamics and challenging personalities
  - Motivating the Team Member contribution and promoting creativity
  - Clarity in translation of the phenomenology of process upsets into a HAZOP/LOPA scenario framework

TABLE 4.1[10]
CHECKLIST OF KEY DISCIPLINES USEFUL FOR A HAZOP/LOPA
(R = Required by PSM/RMP)

- Facilitation/Leadership (R)
- Team Scribe/Recorder
- Process/Project Engineering (R)
- Operations (R)
- Maintenance (R)
- Control/Protection Instrumentation Engineer
- HSE Engineering
- Rotating Equipment Specialists
- Specialists to Address Unique Requirements, e.g., Damage Mechanism Review (DMR), Safeguard Protection Analysis (SPA), Hierarchy of Hazard Control Analysis (HCA)

Note that an optimal team size for an Operating Facility HAZOP/LOPA is 6-8 individuals.

TABLE 4.2[10] – GENERAL INFORMATION REQUIREMENTS FOR A HAZOP/LOPA

- **Process Flow Diagrams**
- **Piping & Instrumentation Diagrams (with changes identifiable from any previous HAZOP Studies)**
- **Cause & Effect Diagrams**
- **Alarm & PSV Setpoints**
- **Site Layout / Platform Location Drawings**
- **Accident/Incident History & Reports**
- **Management of Change (MOC) & Pre-Startup Safety Review (PSSR) Documentation**
- **Previous HA/PHA Recommendation Status**
- Equipment Data Books
- Operating & Emergency Procedures
- Maintenance Records
- System Descriptions
- Previous HA/PHA Reports
- Toxic, Chemical, and Physical Properties
- Prevention Program Compliance Audits

Bold items in the list above are generally more important.

  - Streamlining progress and maintaining team focus on important issues
- **Qualified, experienced, & prepared PHA Scribe** – The right scribe can:
  - Streamline team time, saving significant cost
  - Allow the Facilitator to more effectively interact with the team, improving team focus and PHA completeness/quality
  - Boost documentation quality and report turnaround time
  - This is an important issue, so Section 4.1 contains key elements from Reference 1.

4.1 Scribe Support

Scribing skills include typing, software usage, and computer interfaces with equipment such as displays. The Facilitator can be tasked with both facilitation and scribing duties depending on various parameters of the HAZOP/LOPA, such as system complexity and team composition. So, for a relatively small, manageable group, a Facilitator might be able to also accommodate scribe duties. The pivotal decision-making parameter is whether the additional cost of a Scribe outweighs the money saved by shortening the HAZOP/LOPA Sessions and the subsequent documentation time.

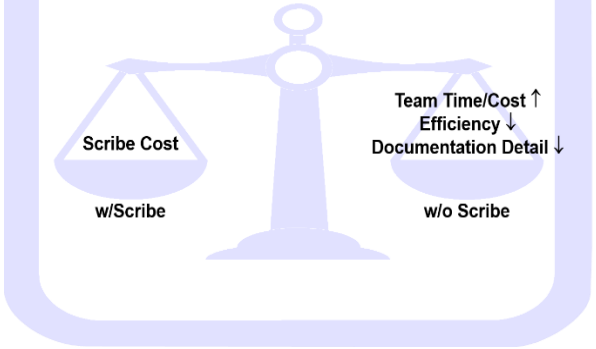

FIGURE 4.1 – Weighing Your Scribe Options

Many professionals, especially in a large company, tend to underestimate the value of their time and that of their peers. The employee time cost can be substantial and shortening the HAZOP/LOPA sessions could have a significant financial benefit. In most cases, this financial threshold is reached once the team size (excluding Facilitator and Scribe) exceeds 3-4 individuals for local projects and possibly 4-5 individuals if travel costs for the Facilitator and the lower-cost Scribe are considered. As another benchmark, Reference 1 recommends to "use a dedicated Scribe, for meetings longer than 4-total hours" and "Use a well-trained scribe to take the documentation load off of the team. This rule can save 30-50% of meeting time and increases brainstorming (because the team is not daydreaming as they wait for Leader to complete the notes)." Along with tangible savings, the Scribe can provide an improvement in the quality of the documentation by capturing more Team discussions and detail than could be accomplished otherwise, and the session itself, by allowing the Facilitator to better focus on engineering issues and maintain an optimal "pace" of the HAZOP/LOPA (too fast, the team gets lost, and too slow, the team tires quickly of watching a Facilitator type and shifts their attention to checking e-mail on their cellphone).

Of course, the decision to involve a Scribe pivots on the Scribe's capabilities. Some key characteristics to seek in a Scribe include:

- Familiarity with HAZOP/LOPA techniques and documentation

- Familiarity with reading engineering drawings and documentation
- Familiarity with the HAZOP/LOPA documentation software and computer skills

For a HAZOP/LOPA, avoid assigning an untrained scribe, or one that is not committed to professional-quality PHAs. Unless properly trained, and motivated, a poor scribe can compromise quality and team progress. Typically, a younger engineer that may be undergoing training to become a Facilitator works best.

5. Tips for Conducting a Quality HAZOP/LOPA

A key variable in the quality and usefulness of a PHA are the session dynamics. Section 4 identifies key personnel and other resource needs, but effective utilization during the PHA is critical. The following are key PHA Session characteristics that are conducive to creating a high-quality and useful outcome. Most of these characteristics must be driven by the PHA Facilitator:

Process Design/Limits and Response to Upset Conditions – It is important for the PHA Team to clearly articulate the process dynamics associated with the upset condition, and for the PHA Scribe to document the maximum unmitigated pressures/temperatures and associated design limits, so that it is clear that the PHA Team's discussions are focused on the same potential hazard scenario, and to ensure that the application of LOPA (if needed) is targeted to the potential hazard scenario.

Overpressure Ratios – Various interpretations of API RP 581[9] are used in industry to characterize the probable worst-case of an event as either a non-leakage event, a flange leakage event, or a credible potential for piping/vessel failure. Although the PHA Team should always be looking at the specific process conditions and equipment, defining a typical consequence for the PHA Team limits the potential for a gross misapplication.

For each overpressure scenario, an overpressure ratio can be calculated and documented allowing the Team to identify a more realistic severity based on whether the scenario is a catastrophic rupture event or a flange leak.

$$\textit{Overpressure Ratio} = \textit{maximum pressure} / \textit{MAWP}$$

Where maximum pressure is the highest pressure that can be reached without taking into consideration pressure relief valves.

Consequence Documentation – To help ensure proper convergence by the PHA Team, it is typically helpful to detail the sequence of events when documenting the consequence.

For example: Potential blocked-in discharge of the pump, leading to increased discharge pressure up to 250 psig, leading to no potential to overpressure the 300# discharge piping as it is rated for the pressure. Potential pump deadhead, seal failure, loss of containment of flammables below

the autoignition temperature (low H2S), resulting in a pool fire with potential personnel impact/exposure.

This level of detail ensures that all Team members are on the same page and are evaluating the same scenario. Furthermore, it provides sufficient information where anyone can read the scenario and know exactly what was analyzed.

Instrumentation and Setpoints – This may be a little more challenging for a system under design, but in general, specific alarm and protection system setpoints should be discussed (and documented) to ensure that the PHA Team can clearly gauge the ability of a safeguard/Independent Protection Layer (IPL) to be effective, especially considering time for Operator diagnosis and response. Furthermore, documenting setpoints of alarms, PSV's, interlocks, etc. allows the Team to verify that the layers of protection will activate as intended. For example, if an interlock setpoint is higher than a PSV setpoint, this may raise a red flag that warrants further investigation.

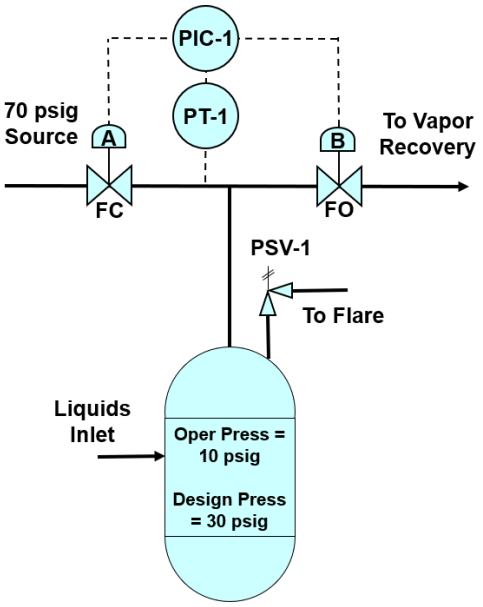

FIGURE 5.1A – Typical "Push-Pull" Blanket Gas Pressure Control System
(control station block and bypass valves removed)

Control and Protection System Actions – Similar to clear discussions on instrumentation & setpoints, clear specification of the action of control & protection system can avoid erroneous credit of an ineffective safeguard.

Importance of Instrumentation Failure Specificity – Transmitter failures, <u>and the failure direction for the causal event</u> (i.e., misreading high or misreading low), should be specifically identified. This is critical for the PHA Team to assess if any common-mode failures (between two credited safeguards or between the causal event and an associated safeguard) exist that could compromise safeguard effectiveness. Transmitters that have a failure mode that could impact multiple end-devices should typically be listed as an independent causal event, with end-devices being controlled clearly specified. Figure 5.1A is a typical "push-pull" blanket gas pressure control system, where a single valve failure may be a simple operational challenge, but the pressure transmitter misreading low could cause both a pressure excursion and disable an overpressurization protection feature. In contrast, Figure 5.1B illustrates a relatively

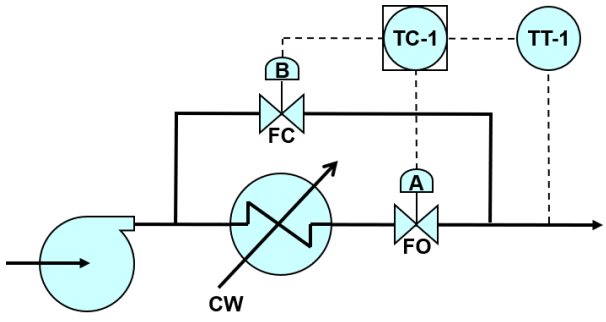

FIGURE 5.1B – Common Temperature Control System
(control station block and bypass valves removed)

common configuration, where a temperature transmitter failure may impact two devices, but which may only have a non-hazardous change in temperature profiles. For the system in Figure 5.1B, a more significant event may occur due to the failure closed of TV-1B, which would initiate a cooling effect that results in the control system commanding TV-1A to also close, resulting a complete blocked discharge potential hazard.

Instrumentation Transmitter vs. Controller Tag Numbers – Although Console Operators often refer to an alarm using the controller tag number (e.g., LC-XXX), to further minimize the potential for the PHA Team failing to identify potential common-mode failures, it is typically a better practice to reference the root transmitter (e.g., LT-XXX) in the causal event and safeguards.

Valve Failure Mode Clarity – As part of the causal event, if the cause clearly, and consistently, states for a fail-closed valve, "fails closed" or "malfunctions open," and for a fail-open valve, "fails open" or "malfunctions closed," the PHA Team is better able to assess the validity of the failure mode. For example, if the risk of a fail-open valve opening is much higher than its closing, it might be appropriate for the PHA Team to reassess the validity of the valve's failure mode. To further support the PHA Team's efforts in properly evaluating failure mode acceptability, incorporate a "Loss of Instrument Air" process deviation where 2-3 minutes are spent before moving onto the next node to list key control valves and their failure modes for each node to validate that the valve failure modes are appropriate.

Crediting Alarms as Safeguards – Does one alarm provide a definitive basis for diagnosis of the upset condition and possible cause to the Console Operator? Does two? Does twenty? Regardless of the number, there is still a common-mode dependency for any number of alarms of the Console Operator to make an effective diagnosis and use their training to identify and implement the appropriate corrective action. To ensure that the most important alarm functions are identified (in case the PHA is used as a basis for the Mechanical Integrity Program), a reasonable practice is to list the one or two alarms that will annunciate "first" and provide the most direct correlation with the process parameters (i.e., flow, pressure, temperature, level) that are driving the process upset. To further emphasize the common-mode dependency of the Console Operator, it may be beneficial to bundle the alarms as a single safeguard (IPL). Periodically, it is often valuable to remind the PHA Team that alarms should only be credited if sufficient time for response exists, given the considerations of:

- Someone present to hear the alarm (local alarms should typically not be credited)
- Alarm prioritization and diagnosis
- Deciding on the corrective action
- Permission for implementing the corrective action
- Initiating and completing the corrective action
- Time needed for the corrective action to mitigate the event (i.e., process safety time)

Failure of a Safeguard as a Causal Event – HAZOP/LOPA are scenario-based analyses. If a safeguard's failure is already implicit in the risk-ranking for a scenario, treating its failure as a separate causal event is unnecessary and potentially confusing. A minimum flow recirculation line is a common example: The action of the minimum flow recirculation valve opening would

typically be credited as a safeguard, with the failure to open implicit in the risk-ranking for that scenario. Therefore, evaluating a separate "malfunctions closed" or "fails to open" event for that minimum flow recirculation valve is unnecessary and potentially confusing.

Consistent Grouping of Scenario Consequences and Application of Safeguards Associated with the Scenario – Safeguards should have a clear correlation with the ability to ameliorate the scenario consequences. Characterizing each safeguard as an Independent Protection Layer (IPL) can facilitate segue to LOPA.

Subcomponent Failure Modes – Grouping subcomponent failures should be done with caution. For example, a blocked turbine exhaust may be a cause of a loss of flow from the pump being driven by the turbine; however, a blocked turbine exhaust could also cause an overpressurization event, requiring safety systems to function in order to ameliorate a serious potential personnel hazard.

Operations and Maintenance Modes – Facilitators need to routinely challenge the PHA Team on how the system is operated (i.e., for control systems, always in "auto," or frequently in "manual") and if there have been reliability problems that could affect the initiating event frequency of the causal event or the effectiveness of the safeguards.

PHA Team Training – In addition to PHA Team Training offered at the beginning of a PHA, consider providing a short "daily briefing" to enhance team alignment of key PHA principles.

Consideration of All Salient Perspectives and Input – Everyone on a PHA Team has an important perspective to offer to support the quality of the PHA, and the Facilitator needs to drive participation, involvement, and cooperation.

Session Length Reflecting Process Complexity – Consistent with the importance of Management Commitment previously identified, without adequate time for properly considering whether credible failures have an appropriate level of protection, PHA results will be incomplete or erroneous. Of course, giving the PHA Team too much time results in disengaged team members, which is also a deterrent to PHA quality. It is important to keep the PHA Team engaged.

Consistent Risk-Ranking – Challenges in the PHA Team's understanding of the process dynamics, scenario consequences, or proper application of the facility's risk-ranking matrix can manifest themselves in inconsistent risk-ranking. The Facilitator needs to be looking for inconsistencies that are indicative of quality problems.

Recommendation Basis – Recommendation significance and priority should be consistently driven by the magnitude of the "gap" to an acceptable risk threshold.



FIGURE 5.2 – Ensure Drawing Updates are Manageable

Manageable Drawing Updates – There are many occasions, especially during a design HAZOP/LOPA, where changes to the design information are applied during the course of the study. The Facilitator needs to skip over (and come back to, as appropriate) portions of the process where the design information is insufficient.

Manageable Information Gaps – In the same way that information gaps due to inadequate drawings must be managed, so must gaps in the knowledge-base of the PHA Team participants. PHA Team participants should be encouraged to expeditiously identify when they don't have definitive information, such that other "subject matter experts" can be summoned, as necessary.

Node Completeness Checks – A technique that generally works well for a HAZOP Study is, after each node, take 10-15 minutes to "step through" the equipment, from the beginning of the node to the end, and verify with the HAZOP Study Team that appropriate equipment and failure modes have been addressed. At that time, double-checking piping specification adequacy, appropriate protection of equipment design limits, reviewing the need for heat tracing, identifying potential dead legs that may require demolition or enhanced mechanical integrity inspections, and the appropriateness of the failure positions of instrument-air-controlled valves can be accomplished. The Completion Check allows the Facilitator to verify that key failure modes have been covered and gives the Team a chance to step back and verify that key issues haven't been missed.

PHA Revalidation vs. Re-do – At most, regulatory guidance for "a hazard review [being] revalidated only once between full hazard reviews" only applies to certain RMP Program 2 processes, and not most PSM-covered processes. For situations when past studies cannot be readily revalidated, a new complete hazard review or PHA may be warranted; however, a technical concern with an arbitrary re-do is that if a good Facilitator and Highly-Qualified Team did a high-quality PHA, and the PHA is arbitrarily discarded and replaced with a re-do by a less capable/experienced Facilitator and/or Team, the result can be a decreased thoroughness in the baseline hazard identification process that forms a foundation for the Safety Management System Program. There may also be a liability issue if a past high-quality PHA that properly evaluated a hazard was discarded, the poor-quality replacement didn't properly evaluate a hazard, and an injury accident occurs. Thus, unless the previous PHA is completely unusable, a re-do should take the form of starting with the "PHA of Record" and comprehensively reviewing/updating each-and-every PHA scenario. With this approach, insights from the previous effort would not be arbitrarily overlooked.

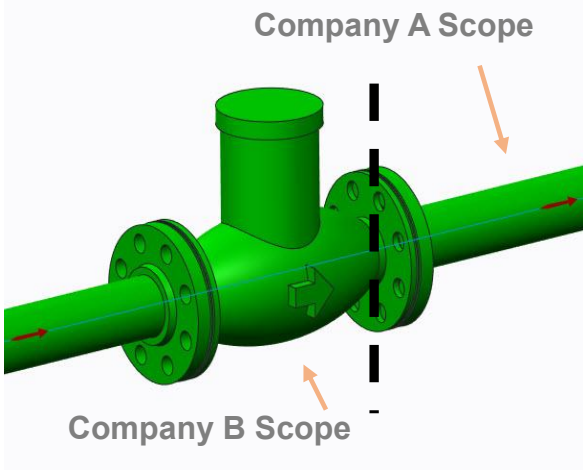

FIGURE 5.3 – Node Boundaries to Avoid

Node Boundaries – Avoid node boundaries in the middle of a flowpath (Figure 5.3). This

can originate from the interface from different vendors involved in the plant design, but inserting an arbitrary boundary in the middle of a flowpath can cause arbitrarily inconsistent results.

Avoid Repeating Scenarios – HAZOP Study Teams will often gravitate towards discussing "generalized" scenarios (e.g., no flow and high pressure resulting from the same cause) such that when the Facilitator guides the Team to "drill down" to the specific cause, it is clear that the Team is discussing different direct impacts from the same equipment failure causal event. Generalized scenarios should be avoided, and the Facilitator must continually drive towards causal event specificity. It is much better to do a thorough evaluation of a specific cause once, and thoroughly, to ensure that important nuances of the process dynamics are surfaced.

6. PHA Documentation Tips

Consistent with the objectives defined in Section 3, documentation quality should be tuned to be able to address all of the identified objectives. Typically, the following documentation characteristics support high-quality documentation that can be directly used to address project objectives, as well as providing sufficient information to support quality reviews.

Specific Causes, with Equipment Numbers Identified – Causes should be able to be correlated to a specific equipment failure or credible process conditions associated with valid operating modes. Tag numbers and P&ID references should be used to facilitate reader understanding of the scenario and quickly locate the equipment associated with the initiating event. A good rule-of-thumb is that if it takes more than ~20 seconds for someone who is familiar with the system to locate the equipment on the P&IDs, a P&ID reference is likely necessary. In addition, to avoid misinterpretation, equipment names should exactly match the name on the P&ID and be capitalized for ease of review and specificity.

Prolific Use of Equipment Tag Numbers and P&ID References – All the key PHA objectives identified in Section 3 are enhanced with specificity and the prolific use of equipment tag numbers. Taking just a few moments can greatly enhance the usability of the PHA documentation.

Block Valves Inadvertently Mispositioned – Any references to block valves should be descriptive regarding location. For example, if the block valve is not in the control valve station, there should generally be a reference to a line number and P&ID, or equivalent.

Probable Worst-Case Scenarios should be specific and able to be directly correlated to the causal event associated with the scenario. A qualified reviewer should be able to read the PHA documentation and clearly understand the sequence of events leading to the probable worst-case scenario.

Safeguards Should be Reliable, Active, and Have Sufficient Process Safety Time – Safeguards should also be specific to the cause/consequence scenario being examined. Ordering the safeguards by the progression of the event (i.e., the first safeguard to be encountered documented first) is a good documentation practice.

Recommendations (or gap acceptance) Whenever Clearly-Defined Acceptable Risk Level is Not Achieved – If there is a risk-gap, it should be addressed with an action item or documented as acceptable to the PHA Team.

Risk-Ranking – Consistent and Matched with Scenario – After the PHA, the Facilitator should carefully review risk-rankings for consistency and identify any inconsistencies to the PHA Team to effect a correction.

Level of Detail and Scenario Depth Pivoting on Importance and Complexity – All scenarios should be readily understandable to a qualified reviewer. As appropriate, details may need to be added to clarify process dynamics, especially if follow-up assessments need to be performed.

Recommendation Usability – Recommendations should be understandable, self-standing, logical, and complete. Actions should be clear, include definitive references to P&IDs and equipment numbers, and minimize the need for the assignee to review the HAZOP/LOPA Report (because the recipient of the action item is likely busy and many not have easy access to the HAZOP/LOPA Report).

Scenario Traceability – Scenarios should be logically-developed, complete, and understandable.

Clarifying Comments – Liberal use of clarifying comments should be made to support future usability and expansion of the PHA. The PHA Team's evaluation and basis for conclusions should be readily understood to support future revalidation efforts.

7. Priorities for a Quality Assurance Review

This paper has attempted to list the most common quality challenges observed from the work of even experienced HAZOP/LOPA Facilitators, and this can also provide a basis for characteristics to look for by a Quality Assurance (QA) Reviewer. A QA Reviewer will typically not have the time, resources, or the benefit of having worked with the PHA Team; however, the following represent our top seven characteristics for the QA Reviewer to examine that might reflect quality problems with the PHA or documentation:

- **Completeness Check** – Picking at least one node, have all key causal events been developed as definitive scenarios?
- **Probable Worst-Case Consequences** – Have they been clearly identified and used as the basis for risk-ranking?
- **Safeguards** – Are the identified safeguards clear barriers between the causal event and ultimate consequences? With the additional equipment and transmitter specificity, do IPLs appear independent, with no apparent common-mode failures missed? Are root transmitters for causes and safeguards clearly identified to reflect the PHA Team having clearly evaluated the potential for common-mode failures?
- **Scenarios** – Are they clearly interpretable? Scenarios should present an image of the event.
- **Risk-Ranking** – Consistent application?
- **Actions** – Clear, complete with focused basis, and self-standing?

- **Multiple HAZOP/LOPA Entries for the Same Causes** – Have these been avoided to decrease the potential for confusion and future misapplication?

8. Emphasis Points for Maximizing the Future Usefulness of the PHA

As well as addressing immediate needs, there are a number of ways that the performance of the PHA and resultant documentation can be geared towards maximizing the ability to use and update the PHA.

Documentation Traceability – Application of the above tips on documentation quality can generally improve documentation traceability, also enhancing the PHA's ability to be updated.

Prolific Use of Equipment Tag Numbers and P&ID References – At the risk of being repetitive, this important characteristic is worth repeating for the documentation quality enhancement value achieved for a very small incremental effort.

Application of Risk-Ranking – It's tempting to only rank high-consequence scenarios; however, for a small incremental effort, ranking all scenarios reinforces the non-importance of low-consequence scenarios. This can be a significant aid to the design process, as well as MI Program prioritization.

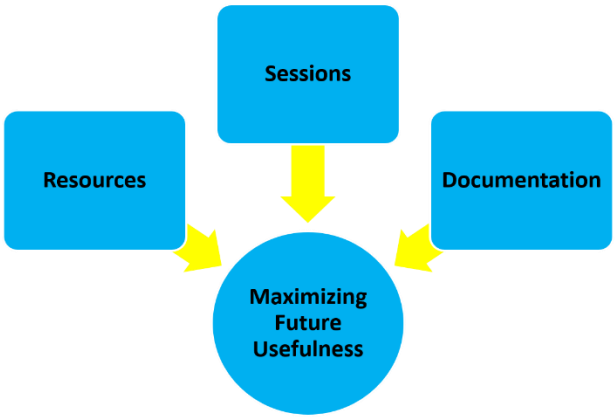

FIGURE 8.1 – Maximizing Future Usefulness

Consistent Scenario Grouping – Consistently placing certain types of scenarios under the same guideword such as "No Flow" or "High Level," etc. can help the reader locate types of events and facilitate future use and update.

Standardized PHA Approach – Although some owner/operators may use a PHA method tuned for their specific needs, standardizing the PHA technique to be consistent with industry best practices can facilitate its ability to be used in the future or updated. Use of a non-standard technique can be even more challenging if the facility changes ownership.

Large Nodes – Although sometimes daunting for a PHA Team, large nodes can allow for a more holistic approach to understanding process dynamics and facilitating scenario location and augmentation. Of course, node size and node complexity must be balanced.

Strive for "Evergreen" Approach – Although a small incremental effort may be required, focus PHA documentation on having an ability to readily update the PHA to address MOC and other future design/operations changes. Consider the long-term use of the PHA.

Software – Software should optimize usage, storage, and retrieval of the PHA. Consider long-term use and the potential for the owner/operator no longer supporting annual licensing fees. Save files in other machine-editable formats, as appropriate.

9. Summary

Implementation of the specific quality tips provided in this paper also require an environment supportive of the performance of high caliber work. Key underlying characteristics of the organization and the individuals involved in the HAZOP/LOPA are critical for supporting a program that emphasizes the importance of the performance of quality Process Hazard Analyses:

- Commitment from Management
- Commitment from the PHA Team
- Dedication of the Facilitator/Scribe in the Performance of Quality Work

These characteristics and the implementation of some of the key tips provided in this paper can provide a platform for the performance and creation of an efficient PHA that has current and future value, and can be used to address many of the objectives identified in Section 3.

10. References

[1] 2009 Global Congress on Process Safety, "Optimizing Qualitative Hazard Evaluations for Maximized Brainstorming (or “How to Complete A PHA/HAZOP Meetings in One-Third the Time Currently Required while Finding More Scenarios”)," http://www.process-improvement-institute.com/_downloads/Optimizing_PHA-HAZOP_While_Maximizing_Brainstorming.pdf.

[2] CCPS “Guidelines for Technical Management of Chemical Process Safety,” 1987.

[3] CCPS “Guidelines for Hazard Evaluation Procedures,” 1985.

[4] "Layer of Protection Analysis: Simplified Process Risk Assessment, " October 2001.

[5] PSM – 29 CFR 1910.119, “Process Safety Management (PSM) of Highly Hazardous Chemicals, Explosives and Blasting Agents,” 1992.

[6] RMP – 40 CFR Part 68, "Risk Management Programs (RMP) for Chemical Accidental Release Prevention," 1996.

[7] California Code of Regulations, Section 5189.1, “Process Safety Management for Petroleum Refineries,” October 1, 2017.

[8] “California Accidental Release Prevention (CalARP) Program,” October 1, 2017.

[9] API Recommended Practice 581, “Risk-Based Inspection Technology,” Second Edition, September 2008.

[10] Paper 513595, 2018 Global Congress on Process Safety, “Preparing for a Successful HAZOP/LOPA (Making or Breaking Quality & Efficiency),” Maher, Steven T., Carine M. Black, and John M. Johnson, April 22-26, 2018.

[11] http://www.RMPCorp.com/HAZOP-Study-series-module, HAZOP/LOPA Facilitation Best Practices Webinar Series.