Business Case for PHA of Procedures (to Find the Accident Scenarios that are Otherwise Missed)

William Bridges
Process Improvement Institute, Inc.
Tennessee, USA
wbridges@piii.com

Matias Massello
Process Improvement Institute, Inc.
La Plata, ARG
mmassello@piii.com

Stephen Bridges
Process Improvement Institute, Inc.
Tennessee, USA
sbridges@piii.com

Prepared for Presentation at
American Institute of Chemical Engineers
2023 Spring Meeting and 19th Global Congress on Process Safety
Houston, TX
March 12-16, 2023

BUSINESS CASE FOR PHA OF PROCEDURES

(TO FIND THE ACCIDENT SCENARIOS THAT ARE OTHERWISE MISSED)

Authors

William Bridges – President
Process Improvement Institute, Inc. (PII)
e-mail: wbridges@piii.com

Matías A. Massello – Process Safety Engineer
Process Improvement Institute, Inc. (PII)
e-mail: mmassello@piii.com

Stephen Bridges – Senior Process Safety Engineer
Process Improvement Institute, Inc. (PII)
e-mail: sbridges@piii.com

Abstract

Hazard evaluations, also called process hazard analysis (PHAs) have been performed formally in gradually improving fashion for more than five decades. Methods such as HAZOP and What-If analysis have been developed and honed during this time. Some weaknesses identified 30 years ago still exist in the majority of PHAs performed around the world. Critically, most PHAs do not thoroughly analyze the errors that can occur during startup, shutdown, and other non-routine (non-normal) modes of operations; sadly, the commonly used approaches for PHA of continuous mode of operation only find about 5 - 10% of the accident scenarios that may occur during startup, shutdown, and online maintenance. This is true even though about 80% of major accidents occur during non-routine operations. Instead of focusing on the most hazardous modes of operation, most PHAs focus on normal operations (e.g., HAZOP of equipment nodes). In a majority (perhaps more than 80%) of both older operations and new plants/projects, the non-routine modes of operations are not analyzed at all. This means that perhaps 70% of the accident scenarios during non-routine operations are being missed by those PHAs. If the hazard evaluation does not find the scenarios that can likely occur during these non-routine operations, the organization will not know what safeguards are needed against these scenarios.

This presentation focuses on the business case for doing PHA of Procedures, based on hundreds of PHA. Data from PHAs/HAZOPs show that 50 to 85% of the risk reduction opportunities are found during PHA of procedures, **resulting in $100,000,000 USD or more in risk reduction savings per week of PHA/HAZOP of procedures**. The return on investment for PHA of procedures (the savings in risk avoidance by implementing doing PHA of procedure) is more than 1000 times the cost of the PHA of procedures.

Introduction

There are several reasons that human errors are both more likely and more devastating in abnormal modes of operation. First, the close interaction between humans and the process equipment adds opportunities to introduce errors that are normally not possible during normal operation, effectively raising the chances for error by sheer increased exposure and input from the operators (especially during startup). Second, during modes of operation such as shutdown, startup, or online maintenance the level of contribution from Human Factors that drive error frequency are multiplied, making human error more likely per interaction/input. Lastly, during abnormal operation, some or perhaps all the critical Independent Protection Layers (IPLs) for an accident scenario are not available (were never included in design to account for certain scenarios possible in these modes).

The Goal of the PHA of Procedures is NOT to improve the procedures and not to identify new administrative controls. Instead, the goal is to find the Independent Protection Layers (IPLs), such as increasing the size of a relief valve or adding an SIF or adding a check valve, to protect against the unique scenarios that occur during startup, shutdown, and online maintenance.

Following several large industrial catastrophes, the US government through OSHA established regulations requiring companies to perform Process Hazard Analysis (PHAs) as part of their Process Safety Management (PSM) system. OSHA intended that PHAs cover hazards and accident scenarios during all modes of operation.

Over the past 3 decades since these regulations were established, performing PHAs has become commonplace in chemical plants, gas plants, oil refineries, and related processing plants around the world. Though the US PSM regulation requires PHA of all modes of operation, only a minority of companies invests time in meetings for analysis of these non-routine modes of operation (apart from normal HAZOP brainstorming: analyzing deviation of level, pressure, flow, and other parameters). Most companies consider the PHA complete and within compliance if they cover the standard 'Deviation during startup, shutdown or maintenance' as topics during the HAZOP of continuous nodes of equipment to satisfy the requirement of the PHA to include all modes of operation. Unfortunately, this type of brainstorming is not adequate to identify most of the scenarios that can occur during non-continuous modes, catching only 5-10% of the unique scenarios that can occur during these modes of operation.[1, 2, 3]

Studies performed by regulators and industry analysts have shown more than 70% of major accidents occur during non-routine/abnormal mode operations (startup, shutdown, online maintenance primarily)(Figure 1).

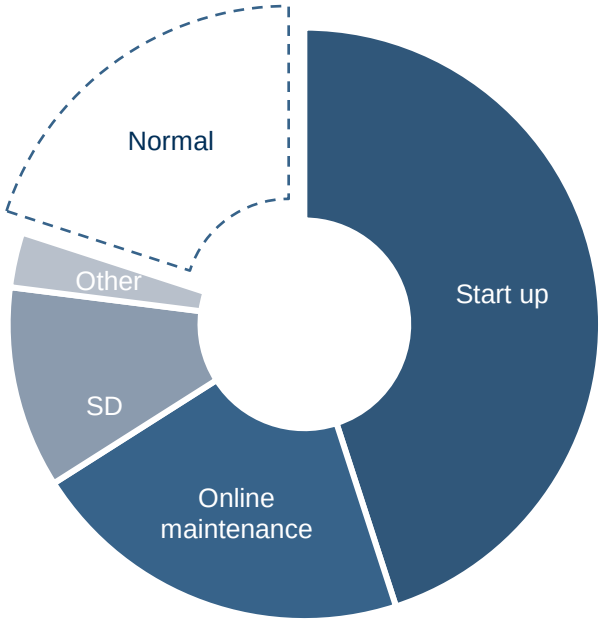
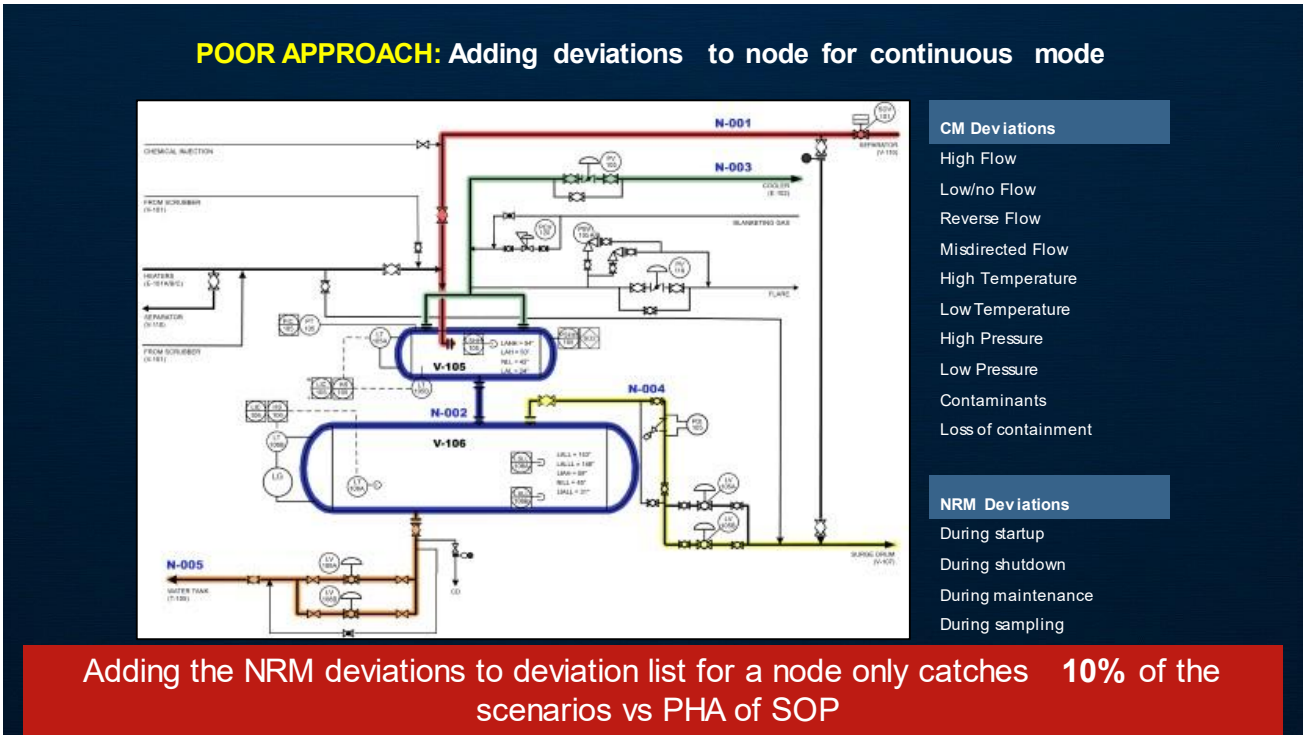


Figure 1. Distribution by Operating Mode of the 47 Largest Process Safety Accidents between 1987 and 2010 [3]

This paper gives examples of several scenarios that would have been missed by the typical method of HAZOP of nodes plus 'Deviation during…' used by most companies during their PHAs (about 80% of companies use this analysis, according to estimates by PII).



The value of identifying and protecting for scenarios found as part of abnormal mode PHAs (accounting for costs of extra meeting time) will be shown through these examples. According to statistics from PII and other PHA data, additional savings from avoided incidents from recommendations generated in

PHA of abnormal modes/Procedure often provide 5 times the risk reduction compared to the recommendations found from PHA of normal mode of operation.

One reason for processes being at higher risk during these operating modes is many of the safeguards (IPLs) are bypassed or may not be fully capable in these modes. A hazard evaluation is necessary to help a company identify the layers of protection necessary to lower the risk to acceptable levels. To fulfill this need, a company operating a continuous process should **fully** evaluate the hazards during **all** modes of operation. Unfortunately, in the first 5 decades of wide-spread hazard evaluation use (beginning after the Flixborough disaster in the UK in 1974 – an accident that occurred during startup in a temporary, poorly engineered configuration), many companies have done a poor job of identifying and evaluating accident scenarios during startup, shutdown, and online maintenance modes of operation, while usually doing a good job of evaluating hazards of normal modes (continuous or normal batch modes) of operation.

Most of the observations and statements above are from the definitive papers on PHA of procedures and Chapter 9 of *Guidelines for Hazard Evaluation Procedures*, 3rd Edition [1, 2, 3, 4, 5, 6], as are the descriptions of the approach to PHA of Procedures provided below.

Overview of Approach for PHA of Non-Continuous Modes of Operation

Figure 2 shows the typical usage of the three methods described above for a typical set of operations procedures within a complex chemical plant or refinery or other process/ operation. Most of the procedures are simple enough or have low severity hazards to warrant using the What-if method. Currently, the 7-8 Guide Word approach is used infrequently, since most tasks do not require that level of scrutiny to find the accident scenarios during non-routine modes of operations.

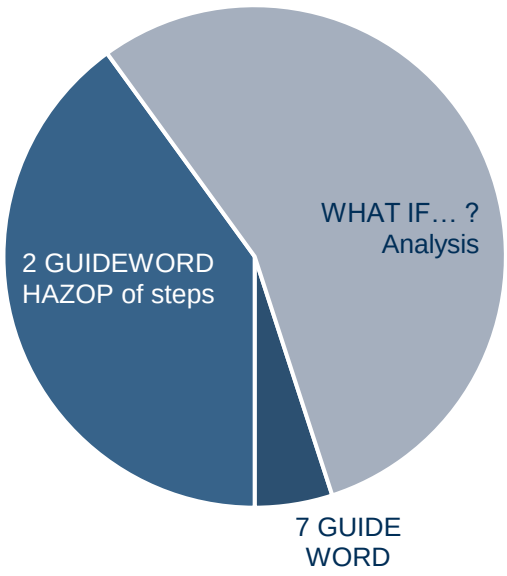


Figure 2. Relative Usage of Methods for Analysis of Procedure-Based Modes of Operation (essentially 2/3rd using What-if and 1/3rd using 2 Guideword HAZOP)

The experience of the leader or the team plays a major part in selecting the method to use for each task/procedure to be analyzed. However, the first decision will always be "Are these procedures ready to be evaluated to determine risk?" If the procedures are up-to-date, complete, clear, and used by operators, then the best approach for completing a complete hazard evaluation of All modes of operation, including routine modes of operation, is shown in Figure 3 and Figure 4 below.

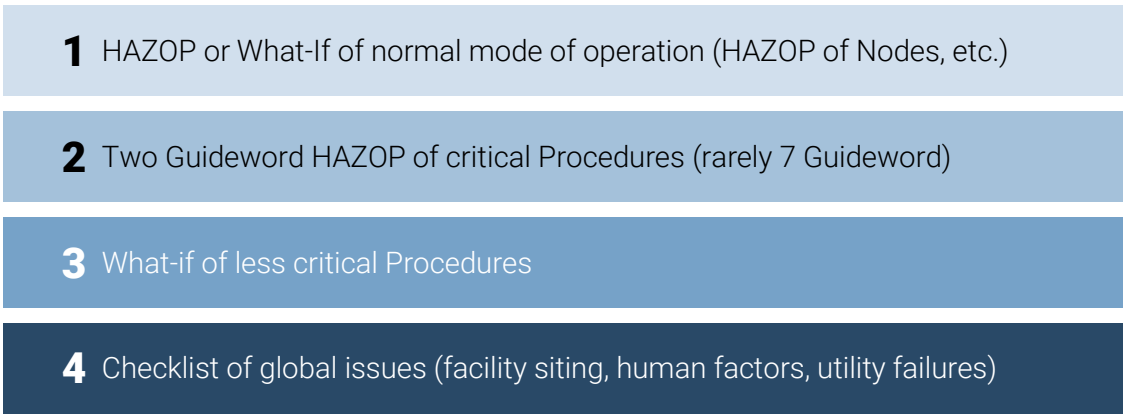


Figure 3. PHA of ALL Modes of Operation for a CONTINUOUS process

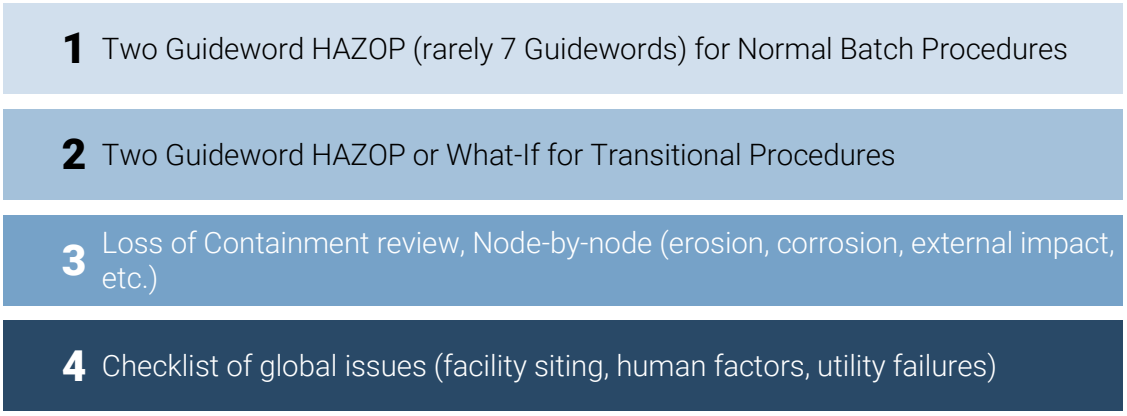


Figure 4. PHA of ALL Modes of Operation for a BATCH process

If procedures are not at least 90% accurate (with 95% accuracy being the target), then the best approach is to develop accurate and up-to-date procedures as quickly as possible and afterwards do a PHA of the newly issued procedures.

Using the approaches above, a company doing a complete hazard evaluation of an existing unit will invest about 65% of their time to evaluate normal (e.g., continuous mode) operation and 35% of their time for evaluating the risks of non-routine modes of operation.

Note that some companies believe that PHA of Procedures is not necessary to find the unique scenarios for errors during startup, shutdown, and online maintenance. They instead believe that adding the following 4 deviations to the list of topics for each equipment node will accomplish the same task:

- Deviation during startup
- Deviation during shutdown or emergency shutdown
- Deviation during online maintenance
- Deviation during sampling

However, from experiments conducted in actual PHAs with highly experienced leaders, PII has found that this approach only finds 10% of the missing scenarios, when compared to PHA of deviations from the steps in the procedures [1, 3, 4, 5. 6]. See Chapter 9 of *Guidelines for Hazard Evaluation Procedures*, 3rd Edition [2] for more details on these experiments.

Guidelines for ranking Procedures for the PHA

Together with an operator before the meeting or with the entire PHA team during the meeting, identify the sections of the procedures that warrant use of:

- **7-8 Guide Words:** For procedures that could lead to extremely large consequences can happen if deviations occur. Typically, in a chemical plant, petrochemical plant, gas plant, or refinery, no procedure will have hazards and complexity. (High Complexity; Very High Hazards, such as explosives)
- **Two (2) Guide Words:** For procedures in which the system is high to moderately complex, mistakes are costly, or severe consequences could occur. (High Complexity; High Hazards)
- **What-If (no guide words or guide phrases)**: For hazardous but simpler, less complex tasks. (Moderate to High Complexity; Moderate Hazards)
- **No detailed analysis:** No further analysis for low hazard tasks (Low Hazards)

This is usually done by risk ranking the procedures High (H), Medium (M), and Low (L) using the concepts of **Hazard level** of the task and **Complexity level** of the task. See Table 1 for an example scoring. Once the ranking is done, the PHA team then makes plans to do a PHA of the high-risk procedures first, and then do the PHA of Medium ranked procedures. After some experience is gain, most PHA leaders find that 7-8 Guide Words is unnecessarily arduous and so the 2 Guide Word method is used to analyze the risk of deviations of steps of High-risk tasks; and What-if is used for medium-risk tasks. The ones ranked low are not analyzed further as the PHA team feels these tasks cannot likely lead to process safety scenarios (note that these procedures still need to have its standalone PHA prior to being issued or if involved in an MOC).

Table 1. Example of Risk Ranking of the Procedures for Startup, Shutdown, and Online Maintenance

SOP Num.	Title	Rev.	Risk Rank
BUT900	VAPORIZER PREPARATION FOR MAINTENANCE	2	HIGH
BUT901	COMMISSIONING PROCESS TO VAPORIZER	5	MEDIUM
BUT902	PROPANE REFRIG. COMPRESSOR MOTOR LUBE OIL SYSTEM	0	LOW
BUT903	PROPANE REFRIG. COMPRESSOR STARTUP	9	MEDIUM
BUT904	PROPANE REFRIG.COMPRERSSOR NORMAL SHUTDOWN	2	LOW
BUT905	INSTRUMENT AND LOGIC SYSTEM FOR CHILLED WATER	0	LOW
BUT908	REFRIG. COMPRESSOR EMERGENCY PROCEDURE. LOSS OF COOLING WATER / INSTRUMENT AIR AND ELECTRIC POWER	1	LOW
BUT911	C6 TRANSFER TO DE-ETHANIZER BOTTOM STEAM STRIPPER	6	LOW

On average we find that an optimum faction of procedures to review is about 20 to 30% of the total number of titles. Another rule of thumb is to invest about half of the time spent on continuous mode PHA in analyzing SOPs to find the unique scenarios that occur during startup, shutdown, and online maintenance. [5, 6]

If the PHA of continuous mode required 10 days of meetings, then PHA of the High and Medium ranked SOPs for startup, shutdown, and online maintenance will require about 4 or 5 days of meetings.

Time requirements

Many companies do **not** perform a thorough analysis of the risk for startup, shutdown, and on-line maintenance modes of operation; the reason normally given is that the analysis of these modes of operation takes "too long." Yet, the hazard evaluation of the normal mode is taking too long and so the organization feels it has no time left for the analysis of procedures for startup and shutdown modes of operation. But, if these hazard evaluations for the normal mode of operation are **optimized** (such as using rules presented elsewhere [7]), the organization will have time for thoroughly analyzing the non-routine modes (typically discontinuous modes) of operation and the organization will still have a net savings overall. This point is critical since about 80% of catastrophic accidents occur during non-routine modes of operation. Figure 5 illustrates (for a continuous process unit) the typical split of meeting time for analysis of routine mode of operation versus non-routine modes of operation.

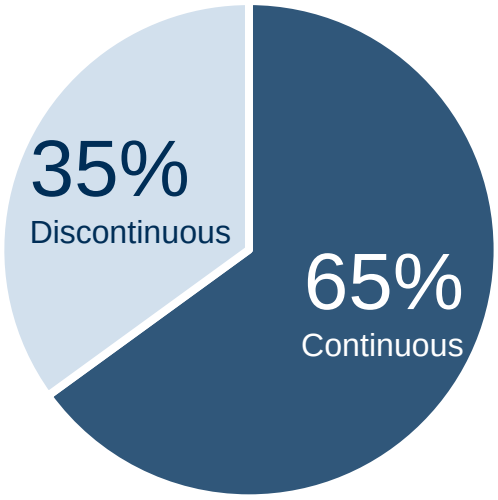


Figure 5. Relative Amount of Meeting Time Spent for Analysis of Routine and Non-routine Modes of Operation for a Continuous Process [1, 2, 3, 4]

Table 2 shows some PHAs performed by PII to illustrate the meeting time distribution (continuous mode vs. non-routine modes) and also the percentage of procedures that were considered to have High/Medium risk by the PHA Teams.

Table 2. Examples of meeting time distribution between Continuous mode and Non-routine modes

Plant	Country	SOPs		Continuous		Non-routine	
		Total	% High/Med.	Days	%	Days	%
2EH	KSA	87	23 %	14	70 %	6	30 %
Urea	KSA	141	33 %	9.5	72 %	3.5	28 %
PDH	KSA	84	25 %	10	71 %	4	29 %
Coker	USA	33	30 %	10	67 %	5	33 %
PP	KSA	174	27 %	10	62 %	6	38 %

Increasing regulatory pressure

Industry has taken some initiatives on resolving this problem. One initiative was to improve the focus on PHA of non-routine procedures as part of the update to "Guidelines for Hazard Evaluation"[2]. A new Chapter 9, Section 1 was added that necessitates hazard evaluations of all hazards of the process during all modes of operation. This textbook also explains why, when, and how to perform such analysis of step-by-step procedures.

Many companies have taken the initiatives to do the same, including about 20% of the largest chemical, petrochemical, and refining companies. But most companies who should be analyzing step-by-step deviations are not; and the major accidents continue to occur partly because of this. As a result, US regulators are beginning to increase pressure on regulated companies to perform PHA's of All modes of operation.

US OSHA Regulation and Enforcement [3]

The US OSHA PSM regulation requires PHA of all hazards during all modes of operation as well, and several key citations since 1990 have focused on PHA of non-normal modes.

Before PSM regulation

Before there was a PSM regulation from US OSHA, the agency published CPL 2-2.45 (Systems Safety Evaluation of Operations with Catastrophic Potential) [8]. In this guidance document, OSHA stated that a human error analysis should address:

- Consequences of failure to perform a task.
- Consequences of incorrect performance of a task.
- Procedures and controls to minimize errors [8]

This approach is still the fundamental analysis method for PHA of non-normal modes of operation.

Phillips 66 "PHA" Citation

A citation with 566 instances was issued to Phillips 66 in Pasadena, TX, following their 1989 disaster that killed 23 workers [9]. The citation was related to a violation of the General Duty Clause (Section 5(a)(1) of OSH Act of 1970). US OSHA cited Phillips against the General Duty Clause, since the PSM standard (29 CFR 1910.119) had not yet been issued. OSHA cited Phillips for not protecting its workers from hazards of fire/explosion by, among others, not performing a PHA that should have included an evaluation of the effect of design modifications on operator performance, and the identification of the source of observed human error and the identification of human factors that could result in incident event sequences. The citation stated, "This review should result in a systematic listing of the (1) types of errors likely to be encountered during normal or emergency operation, (2) factors contributing to such errors, and (3) proposed system modifications to reduce the likelihood of such errors".

The settlement agreement [10] between US OSHA and Phillips included the following requirements for process hazard analyses (PHAs) of the rebuilt and surviving units:

- "Phillips will analyze each process…and will include human factors analysis … [and] will be …led by an independent consultant."
  - William Bridges (of JBF Associates at the time, now with PII) led these PHAs. Before these PHAs began, OSHA, Phillips, and Mr. Bridges decided that the best approach for finding all human error scenarios was to perform a HAZOP of deviations of the steps for the procedures governing activities for startup, shutdown, and particularly online maintenance.
- "Phillips will provide OSHA an independent consultant's evaluation of the adequacy of its settling leg maintenance procedures performed while the polyethylene reactors are in operation…"
  - As part of the settlement to meet this requirement, it was decided by JBFA, Phillips and OSHA to perform a Human Reliability Analysis (HRA) of the Setting Leg online maintenance procedure, to ensure that the statistical risk of the accident recurring is less than the background risk of driving to work.

The PHA and HRA resulting from the Phillips settlement agreement is presented as a Case Study later in this paper for sake of clarity.

OSHA regulation on PSM

Paragraph (e) of the US OSHA regulation on PSM, 29 CFR 1910.119, [11] and similar requirements in US EPA's rule for risk management programs (RMP), 40 CFR 68.24, [12] specifically require that PHAs consider and address hazards of the process, i.e., all hazards regardless of the mode of operation (routine or non-routine).

- 29 CFR 1910.119(e)(1) states that the PHA, *"shall identify, evaluate, and control the hazards involved in the process"*.
- 29 CFR 1910.119(e)(3)(i) states that the process hazard analysis shall address *"The hazards of the process"*.
- 29 CFR 1910.119(e)(3)(vi) states that the process hazard analysis shall address human factors.
- Appendix C to the OSHA PSM standard states that both routine and non-routine activities need to be addressed by the PHA of the covered process.

There is no qualifier that limits the OSHA PHA requirement to only perform a PHA on routine modes of operation. PSM requires that **all hazards** related to the process be addressed, regardless of the mode of operation or activity (routine or non-routine).

OSHA Inspection No. 103490306 (Nov 2, 1992) [13]

In the first major PSM inspection in 1992 using 29 CFR 1910.119, OSHA assessed a serious violation when the PHAs did not address "human factors such as board operator error, line breaking mistakes, and improper lockout and isolation of process equipment," all of which are errors originating from failure to either perform tasks or perform them correctly.

Internal document on Program Quality Verification of PHAs

US OSHA published an internal document on Program Quality Verification of Process Hazard Analysis in 1993 (by Henry Woodcock, of OSHA) [14]. This document states that a PHA should include analysis of the "procedures for the *operation* and *support* functions" and goes on to define a "procedure analysis" as evaluating the risk of "skipping steps and performing steps wrong." The authors concur and PII has found the same true in PHAs that we have performed using various methods; a 2 Guideword HAZOP approach is normally optimal for PHA of procedures.

OSHA Inspection No. 123807828 (Nov 18, 1993) [15]

Ashland Oil, Catlettsburg, KY. Several operators were preparing to ignite a 2-B-3 crude heater after a two week turnaround. The lead operator had two very inexperienced workers helping him light the heater. A large quantity of fuel gas entered the heater before the pilot light was ignited. The resulting explosion killed one employee, who received fatal injuries to the back of his head. The operators bypassed safety shutdown features; poor engineering allowed this to occur and should have been

discovered in the PHA. In addition, they did not check the firebox to ensure that it was gas-free before lighting the heater.

The Kentucky OSHA citation read: *"The PHA did not address all hazards of the #2 Crude unit…. The PHA did not address the hazards associated with the startup of the crude unit after a turnaround, …emergency shutdown…, emergency operations and normal shutdown of the unit. The process hazard analysis that was completed by the PHA team for the #2 Crude unit only evaluated the hazards associated with normal mode of operation of the #2 Crude unit"*.

Settlement: All procedures were re-written and all PHAs were redone to include a PHA of deviations from procedural steps for all non-continuous modes of operation.

PSM National Emphasis Programs

US OSHA PSM National Emphasis Programs for Chemical Processes [16] and also for Refineries [17] underscore the need for companies to identify potential accident scenarios during non-routine modes, and to reduce the frequency and consequences of such errors as part of an overall process safety management (PSM) program.

OSHA recognizes that CCPS/AIChE added Chapter 9.1 in the 3rd edition of *Guidelines for Hazard Evaluation [2]* to further emphasize the need for a PHA to include hazard evaluations of all modes of operation and that this chapter has added best-practice detail on the approach for doing the hazard evaluation of startup, shutdown, and online maintenance modes of operation. Despite the specific OSHA standard that requires PHAs of covered processes must address all hazards, many PHAs still do not address hazards during all modes of operation. Further, many of the regulated community have stated "Well, OSHA did not tell us to perform a PHA of procedures for non-routine modes of operation." On the other-hand, OSHA did not state to do only a hazard evaluation of normal mode of operation and stop there.

To highlight the importance that PHAs address hazards during all modes of operation and activities (routine and non-routine), OSHA is considering issuing a Hazard Alert that would incorporate the concepts in Chapter 9.1 of *Guidelines for Hazard Evaluation Procedures, 2008, CCPS/AIChE. [2]* Also, as stated above, OSHA has an enforcement initiative, CHEM NEP, that utilizes a list of dynamic questions that OSHA compliance officers use to evaluate compliance at facilities covered by the program. **It is possible that future dynamic list questions could address PHAs of all modes of operation, and is further possible that this CHEM NEP update is drafted and waiting for release.**

US Chemical Safety and Hazard Investigation Board (US CSB)

The CSB has commented on the need for PHAs to address all hazards of the process during all modes of operation. Their clearest statements are in "Bayer CropScience Pesticide Waste Tank Explosion" and "Husky Energy Superior Refinery Explosion and Fire" investigations reports. [18], [19]

Bayer CropScience Pesticide Waste Tank Explosion (2008)

- *2008-08-I-WV-R1:* Revise the corporate PHA policies and procedures to require:
  - Validation of all PHA assumptions to ensure that risk analysis of each PHA scenario specifically examines the risk(s) of intentional bypassing or other nullifications of safeguards,
  - **Addressing all phases of operation and special topics including those cited in chapter 9 of "Guidelines for Hazard Evaluation Procedures"** (CCPS, 2008),
  - Training all PHA facilitators on the revised policies and procedures prior to assigning the facilitator to a PHA team, and
  - Ensure all PHAs are updated to conform to the revised procedures.

Husky Energy Superior Refinery Explosion and Fire (2018)

- *2018-02-I-WI-1:* **Establish safeguards to prevent explosions in the FCC unit during transient operation (including startup, shutdown, standby, and emergency procedures)**. Incorporate these safeguards into written operating procedures. At a minimum establish the following specific safeguards:

  a) Implementation of the reactor steam barrier, or a similar inert gas flow, to maintain an inert barrier at an elevated pressure between the main column (containing hydrocarbon) and the regenerator (containing air);
  b) Purging the main column with a non-condensable gas as needed to prevent a dangerous accumulation of oxygen in the main column overhead receiver;
  c) Monitoring to ensure that there is a sufficient non-condensable gas purge of the main column to prevent a dangerous accumulation of oxygen in the main column overhead receiver (either through direct measurement of the oxygen concentration and/or through engineering calculation);
  d) Monitoring of critical operating parameters for flows, pressures, pressure differences, and catalyst levels;
  e) Documentation of consequences of deviating from the transient operation safe operating limits and of predetermined corrective actions; and

f) Inclusion of the above items in the appropriate FCC operator training curricula.

- *2018-02-I-WI-5:* **Develop guidance for analyzing operating procedures to improve transient operation hazard evaluations during PHAs**. Refer to section Chapter 9.1 in the CCPS publication *Guidelines for Hazard Evaluation Procedures, 3rd Ed*. or an appropriate equivalent resource to develop the guidance. Incorporate the guidance into the appropriate Cenovus Superior Refinery PHA procedural documents and policies.
- *2018-02-I-WI-11:* **Develop guidance documents for performing process hazard analysis on operating procedures** to address transient operation hazards in facilities with Process Safety Management (PSM) covered processes.

US EPA's RMP Regulation

In the Risk Management Program rule (40 CFR 68) [12] EPA also recognizes the importance of procedural analysis, however; it is expressed in a more explicit way for Program 2 facilities than Program 3 facilities.

Program 2 (No offsite receptors – Not covered by OSHA PSM/NAICS)

- *Hazards Review - 68.50.(a):* "The owner or operator shall conduct a review of the hazards associated with the regulated substances, process, **and procedures**".
- *EPA General RMP Guidance, Chapter 6:* "The next step may be to conduct a simplified "What If" process, where your technical staff ask "What if it stops or fails?" for each piece of equipment and "**What if the operator fails to do this?**" **for each procedure.**" [22]

Program 3 (Offsite receptors – Covered by OSHA PSM/NAICS)

- *Process hazard analysis – 68.67.(c):* "The process hazard analysis shall address: (1) The **hazards** of the process".

Like in OSHA PSM, there is no qualifier that limits the EPA RMP requirement to only review routine modes of operation. It requires that **all hazards** related to the process are addressed, regardless of the mode of operation or activity (routine or non-routine).

Contra Costa County Hazard Materials Program (Local regulation)

The counties in California are the implementation and enforcement agencies for the US EPA RMP regulation, which in California is termed, California Accidental Release Prevention (CalARP) regulations. One premier implementer is Contra Costa County (CCC). In addition to the standard requirements found in EPA's RMP regulation (which has requirements essentially identical to OSHA PSM), CCHMP has also added their own initiatives to improve how the 10 major facilities in CCC address human factors and PHAs of all modes of operation.

The Industrial Safety Ordinance (ISO) [20] specifically requires that each site perform a PHA of procedures, just to be certain PHAs of all modes of operation are performed. One question in the county's auditing protocol is: *"Did the Stationary Source perform Procedural PHAs to evaluate potential active*

failures or unsafe acts in the procedure such as missed or out of sequence steps and including raising questions regarding the availability of personnel to perform a task as specified in the procedure?" [Section B: Chapter 4.3 of the CCHMP Safety Program Guidance Document].

Conclusions on Regulatory Pressure

Clearly, the regulatory pressure is increasing for industry to perform a PHA that thoroughly addresses hazards during all modes of operation, including deviations from steps in startup, shutdown, and online maintenance procedures.

By the way, a similar focus is underway by the same government entities listed above to improve the coverage of all damage mechanism (corrosion, erosion, external impact, etc.) within a PHA (such as Cal OSHA's proposed rule for refineries). The 2008 update to the book *"Guidelines for Hazard Evaluation Procedures"* [2] was also to address weaknesses observed (across the industry) by US CSB (and others) in coverage of damage mechanisms within PHAs; US CSB requested these changes from CCPS.

Case Studies demonstrating the business case for PHA of Procedures

The following studies serve to provide a sample of errors types and consequences from recent PHAs performed by PII staff. This can be useful for those new to PSM, who may not be aware of certain types of mechanisms which are not found in normal operation which could potentially exist at their plants; scenarios that may have no protections currently.

The examples in the studies also provide grounds for those who already know they should be doing a more thorough analysis of non-continuous modes but need help justifying the extra time and monies required (beyond HAZOP of normal mode of operation); *though it should be noted again that for US companies and those covered by company standard, analysis of all modes is required, meaning compliance should be mandatory; not optional.*

Phillips Polyethylene Plant 6 (Pasadena, TX, USA)

In 1991-1992, a PHA was performed for the first of the rebuilt polyethylene plants at the Phillips 66 plant in Pasadena, TX. The accident there two years prior claimed 24 lives, injured hundreds of others, destroyed all three polyethylene plants, and cost Phillips an estimated $1.4 billion (in 1989 dollars). Following the investigation of the accident, one of the requirements of the settlement agreement between Phillips and the US government was to ensure the PHA of the rebuilt units addressed hazards during **all modes of operation.**

The PHA first covered the continuous mode of operation for the approximately 250 nodes of equipment (from feed stock through pellet handling) using the "parametric deviation" form of HAZOP (and some What-If). Then, to complete the analysis of all modes of operation, the PHA team performed a step-by-step analysis of all steps of all startup and shutdown and online maintenance procedures (about 700 steps changed the state of the system and each of these steps were analyzed) using the 7 Guide Word HAZOP method (2 Guide Word analysis was not known to the team at this time). For deviations such

as "operator skips a step," the causes identified by the team included "the operator doing this step miscommunicates with the operator who performed steps earlier in the day and went to the wrong reset panel/switch in the field". In this example, an "other-than" error led to the "skip" error; so two errors occurred at once: the wrong switch was flipped and the correct switch was not flipped. Other causes included: "label not distinct enough" or "thinking/believing the previous operator completed this step." The additional safeguards suggested by the PHA team sometimes lower the likelihood of the error by addressing a human factors weakness. But in many cases, the solution was a change to the hardware or instrumentation, including adding new interlocks (these would be called Safety Instrumented Functions today) and adding mechanical interlocks and installing larger relief valves. In a couple of cases, isolated sections of the process were redesigned to lower the inherent risk, such as adding error-proofing (Poke Yoke) features.

The 7 Guide Word HAZOP of non-routine modes of operation took 2.5 weeks of meetings, 40 hours a week. This was in addition to the 4 weeks of meetings to complete the parametric deviation analysis HAZOP of the continuous (normal) mode of operation (as mentioned before, 200 nodes of equipment); some all this the Normal PHA or Traditional PHA, but that is a misnomer. *Note that if the team had known of and been trained in 2 Guide Word HAZOP for procedure steps, they likely would have chosen that for many of the tasks and it is estimated that the meeting time for analysis of non-routine procedures would have been reduced to less than 2 weeks, with little or no loss of thoroughness.* The completed PHA report was submitted to US OSHA for review and was approved almost immediately; OSHA particularly reviewed the analysis of all modes of operation and coverage of human factors.

> **EXAMPLE:** From the PHA of startup, shutdown, and online maintenance, then team found a great many scenarios missed by the PHA of continuous mode of operation. For instance, the team recommended about 15% more safety instrumented functions only for startup, shutdown, and online maintenance. And the PHA team found scenarios unique to startup that led to resizing of 7% of the PSVs in the polyethylene plants because these PSVs were too small for the limit case accident scenario, which was unique to startup.

Summary of the Value of PHA of Procedures for Phillips:

1. **Demonstrate compliance of PHA requirements of US OSHA PSM standard by completion of a PHA of all modes of operation**
2. Found hundreds of new accident scenarios, many of which could lead to catastrophes similar in size to the 1989 accident; the risk of these scenarios was mitigated by the recommended improvement to the system.
3. **The risk reduction measures (all non-procedural IPLs) that were found missing during PHA of procedures of startup, shutdown, and online maintenance accounted for about 70% of the risk reduction from the entire PHA.**
4. Overall risk reduction was likely $500,000,000 USD.

UNITED – a SABIC affiliate (Jubail, Saudi Arabia)

In January 2019, a Redo PHA of the UNITED Ethylene Plant (Jubail, Saudi Arabia; a SABIC affiliate) was performed, which is to serve as that plant's new baseline PHA. This new hazard analysis included a PHA of Procedures, in compliance with SHEM 02.01, Rev 8, specifically section 5.12.2, which requires the PHA to consider all modes of operation, and section 5.12.2.9, that the PHA cover control system failures, including user interfaces and human factors [21]:

The meeting time was set at 19 days, with 14 days allocated for HAZOP of continuous/normal mode of operation and 5 days dedicated to PHA of Procedures (Step 3 of this paper) which was used to cover non-normal modes of operation: shutdown, startup, and online maintenance; and 3 hours for checklists reviews (such as Step 4 of this paper). For the continuous/normal mode of operation the plant was sectioned and analyzed in the typical HAZOP style, deviating each node's parameters as such as high and low deviations of level, flow, pressure, temperature, etc. as suitable for each node. The PHA of Procedures was done in the last 5 days, so the team was well aware of the major hazards and safeguards (at least for normal modes) relating to the equipment listed in each procedure. The procedure list was reviewed with the team on the first day to decide which procedures presented major process hazards (consequences of interest, in this case non-occupational hazards/serious injury or fatality consequences), so that more time could be focused on highest risks containing procedures. These procedures were typically more complex and usually longer in length. For these identified with significant process safety potential impact, the 2 Guideword Method was used and for those with less hazards, the What-If method was used. As usual, the goal was identifying specific scenarios of interest for those steps, capturing safeguards and safeguard steps in the documentation process. The few hours of the meetings included analysis using checklists to cover any hazards that weren't otherwise identified, and the team was given additional time outside of meeting to respond to the individual questions in both the Human Factors and Facility Siting Checklists, yielding an additional 3 recommendations deemed safety critical.

The PHA team identified many hazards during the meeting in both the normal mode HAZOP and the PHA of Procedures, listing 115 Safety Critical Recommendations (as defined by UNITED) and 7 Operability Recommendations (not safety critical, note that effective operation reduces risk of safety incidents as well). Of these Recommendations, 42 (or 36% of total) were identified during the PHA of Procedures; and while many of these were simple fixes needed to step order or wording, **14 were in response to critical (high risk) consequences identified in the procedure analysis, requiring new or upgraded independent protection layers** to bring the risk to acceptable levels. The scenarios and related **recommendations found during PHA of procedures accounted for 80% of risk reduction from the entire PHA**, amounting to about $200 million USD in risk reduction.

> **EXAMPLE:** During the procedure analysis for the acetylene reactors, it was discovered that there were no adequate safeguards against run-away reaction during start up, meaning the reactor shell could reasonably be expected to fail at some point due to human error during startup, which would likely cause a large explosion with the potential for multiple fatalities. The startup process required an extremely slow ramp-up in temperature (1°C per

5 minutes) and was controlled entirely by control room operators (by manually changing set points as they monitored for temperature spikes). In this case, the team recommended new logic and safety instrumented functions to protect against the catastrophic reactor failure and explosion.

EXAMPLE: During the procedure analysis for the both the propylene nd ethylene refrigeration systems, it was discovered that there were no safeguards against charging liquid refrigerant too soon, before the system is pressurized first with vapors to 2.5 barg and 12 barg, respectively. Since the equipment was normal carbon steel which is suspectable to low temperature embrittlement below -29 C, if the systems are not first pressurized as stated in the procedure, the systems could reach temperatures of -40 C and -89 C, respectively. In this case, the team recommended installing one to two new automatic block valves (XVs) to prevent introduction of liquid refrigerant into these systems, unless multiple pressure transmitters first confirm the pressure is the system is above the target pressure. The ratings recommended were SIL 3, since there were no other protections available. The alternative recommendation was to change the materials of construction to be able to withstand the cryogenic temperatures possible.

Large OLEFIN Unit (Jubail, Saudi Arabia)

In the fall of 2019, a PHA was performed on one of the largest olefins unit in the world, located in Saudi Arabia. This was a large scope PHA, which spanned more than 10 weeks of meetings and over 420 nodes (about equal in size to the PHA performed of the rebuilt Phillips Polyethylene plant, mentioned above). The scope required analysis of both continuous (normal HAZOP) and non-continuous mode of operations. About 3 weeks were devoted to PHA of procedures, or ¼ of total meeting time. The procedures were analyzed for each sub-unit of Olefin plant, including bringing equipment experts as needed, such as for rotating equipment and DCS personnel.

Of the 282 safety related recommendations, 130 originated from PHA of procedures (46%). It is estimated that the **total savings achieved from implementing recommendations which originated from PHA of Procedures is about 70 to 80% of the risk reduction from the entire PHA**; and these recommendations were valued at more than $300 million USD in risk reduction. The PHA of procedures was clearly worth the cost of 3 weeks of additional PHA team meeting time. Many more Operational improvement recs and procedure re-writes were also generated from the PHA of Procedures, which will also affect a large amount in cost reduction/efficiency improvement (78% of the operational improvement recommendations and about 80% of the operational risk reduction came from PHA of Procedures).

EXAMPLE: Based on the team's estimation it is possible that a process gas drier shell can fail if cooling cycle/safe temperature is not reached before putting the dryer at operational pressure. The risk of this human-error-based accident scenario was too high by several orders of magnitude. Therefore, the team recommended additional hardware or instrumentation safeguards to prevent pressurizing the dryer before the temperature is low

enough (before the cooling cycle is completed) such as by installing a logic sequence that can't be bypassed, with a timer and temperature confirmation of shell/piping readiness for pressure, and count/duration of cooling volume.

EXAMPLE: The team recommended removing a line that is currently not in use (and is blinded) that runs from a benzene column reflux drum to the firebox of the fired heater upstream of the benzene catalytic reactor to prevent anyone from using the line in the future. Liquid is no longer burned in this heater and if the plant staff tried to burn this waste benzene in the heater in the future, it would introduce significant risk to the heater operation. It is better to remove the capability to use this line to eliminate this capability.

EXAMPLE: The team recommended venting the seal drain pot system continuously to the flare system. Currently, operations switches between venting to the flare and venting to the atmosphere, depending on the mode of operation, and there are multiple human errors that could leave the vent inadvertently open to the atmosphere when a highly volatile material is being drained to the system.

Formaldehyde Plant at CHEMANOL (Jubail, Saudi Arabia)

In the summer of 2019, a PHA was performed on one of the formaldehyde plants at CHEMANOL, in Saudi Arabia. The scope required analysis of both continuous (normal HAZOP) and non-continuous mode of operations, and PHA of procedures accounted for about 25% of total meeting time.

It is estimated that the **total savings achieved from implementing recommendations which originated from PHA of Procedures is about 50% of the risk reduction from the entire PHA.**

EXAMPLE: Based on PHA of procedures for startup of the plant, the team recommended adding an interlock/IPL to ensure that the Catalytic Incinerator is lined up correctly and at proper operating temperature, and ensure the vent line to atmosphere is closed, as a permissive for bringing the formaldehyde plant fully online. Otherwise there will be potential environmental concerns from Incinerator outlet gas to atmosphere, as well as risk of leaving the vent open before the Incinerator leading to a potential explosive atmosphere in the reactors. A captive key system may provide the best option for protection, requiring a proper sequence of valves be opened and closed during the startup procedure.

SINOPEC-SABIC Tianjin Petrochemical Company (SSTPC) (Tianjin, China)

The process plants at SS-TPC currently are:

- Ethylene (ET)
- MTBE & Butadiene (BD/MTBE)
- Phenol/Acetone (PHAC)
- High Density Polyethylene (HDPE)
- Linear Low Density Polyethylene (LLDPE)
- Polypropylene (PP)

- Pyrolysis Gasoline (DPG)
- Ethylene Oxide & Ethylene Glycol (EO/EG)
- Tank farm and Storage
- Utilities

A PHA was performed for all modes of operation on these units. Besides a HAZOP or What-if of continuous modes of operation, the PHA team also used the Two Guideword or What-if approach to complete a PHA of startup, shutdown, and online maintenance modes of operation. The PHA of the non-routine modes of operation took about 20% of the total meeting time and was done at the end of the unit node-by-node analysis for continuous mode of operation.

Hundreds of scenarios were found during analysis of procedure-based modes of operation, resulting in many recommendations that had not been found during PHA of normal mode of operation. These resulted in implementation of new instrumentation and permissives and interlocks to reduce the accident scenario likelihoods. The cost savings from the PHA of procedures alone is roughly estimated at close to $1 billion USD.

Butamer Process (Jubail, Saudi Arabia)

In the summer of 2019, a PHA was performed on a Butamer process, in Saudi Arabia. The scope required analysis of both continuous (normal HAZOP) and non-continuous mode of operations, and PHA of procedures accounted for about 30% of total meeting time.

It is estimated that the **total savings achieved from implementing recommendations which originated from PHA of Procedures is about 65% of the risk reduction from the entire PHA.**

Resin/Latex process (Illinois, USA)

In the fall of 2022, the PHA was performed of a Resin plant in a small town near Chicago, Illinois (USA). It is a semi-batch process. Materials are added in batches to one of two stirred-tank reactors. Some of the materials added were prepared and added manually while others were pumped from other units. Everything is controlled by a sequence/reaction controller. Once the reaction is complete, the product is sent to one of several intermediate storage tanks and from there it flows continuously through the coagulation and drying sections until final storage/bagging.

Given the low complexity of the process, What-If methodology was used throughout the plant/process with the exceptions of the make-up of two highly hazardous monomers and the batch operation of the main reactors. After reviewing the whole process with the What-if/HAZOP, the team risk ranked the procedures for non-routine modes of operation (21% of the procedures were ranked High/Medium).

> **EXAMPLE:** The addition of iron into the reactor played a crucial role, though the iron solution itself is low hazard. The iron solution was prepared and controlled manually and its flow to the reactor was controlled by a totalizer (through the reaction sequence controller). Not adding (or not adding enough) iron could lead to unreacted monomer buildup in the reactor potentially leading to a runaway reaction, resulting in overpressure

and loss of containment, releasing flammable material at about 50 psig, causing a fire/explosion and possibly leading to fatalities. The existing safeguards are a relief valves and a large rupture disk (the disk is designed for the runaway reaction case) and a reaction kill injection (manually triggered).

The PHA Team recommended an additional IPL for the Low/No iron scenario; however, there are a few Independence (potential non-IPL) issues to be considered during resolution of the recommendations:

- If the scenario was caused by a totalizer failure, the DCS has already been counted and therefore, other readings at the reactor used to trigger the reaction kill systems are not completely independent.
- If the scenario was caused by a human error, the human has already been counted and therefore the action to trigger the reaction kill system is not completely independent.

Conclusions on Business Case for PHA of Procedures

As the data suggests, the relative risk reduction from recommendations related to PHA of startup, shutdown, and online maintenance procedures accounts for:

- **50 to 80% of the risk reduction from all recommendations from a PHA**
- Average risk reduction of **more than $100,000,000 USD per PHA meeting week for PHA of Procedures**
- Cost savings due to risk reduction was gained in about **1/3rd of the total PHA time investment.**
- For USA-based companies, there is the added benefit of achieving compliance with the US OSHA, US EPA, and local regulators to complete a PHA of all modes of operation.
- PHA of procedures is 10 times more effective than the next best approach; and PHA of procedure has been streamlined 30% in the past 30 years, with relatively no loss in findings.

The return on investment for PHA of procedures (the savings in risk avoidance by implementing the recommendations from the PHA of procedures) is more than 1000 times the cost of the PHA of procedures.

PHA of non-routine operating procedures is an extremely powerful tool for uncovering deficiencies that can lead to human errors and for uncovering accident scenarios during all modes of operation. Examples and estimates of recommendations from many PHAs listed in this paper show the additional savings (cost avoidance) that can be achieved from PHA of procedures, especially considering the marginal increase in cost of the overall PHA given scopes cover non-continuous modes with procedure analysis. The savings more often outweigh those possible from PHA of continuous modes. Identifying related scenarios and safeguarding against them could mean protecting companies from the worst-case disasters, those where entire plants and billions of dollars could be at stake. Strategic loss prevention

should therefore require every PHA, from design phase to revalidation, consider adding procedure analysis to overall scope of the PHA; and prudent managers at *every level* need to consider the benefits of finding every scenario possible to minimize the exposure of risks in their areas of responsibility.

REMINDER: The Goal of the PHA of Procedures is NOT to improve the procedures and not to identify new administrative controls. Instead the goal is to find the Independent Protection Layers (IPLs) such as increasing the size of a relief valve or adding an SIF or adding a check valve, to protect against the unique scenarios that occur during startup, shutdown, and online maintenance.

Acronyms

CCPS: Center for Chemical Process Safety
CSB: US Chemical Safety Board
COI: Consequence Of Interest
EPA: U.S. Environmental Protection Agency
HAZOP: Hazard and Operability study
KSA: Kingdom of Saudi Arabia
OSHA: US Occupational Safety and Health Administration
PHA: Process Hazard Analysis
PP: Polypropylene
PSM: Process Safety Management
PSV: Process Safety Valve
RBPS: Risk Based Process Safety
SOP: Standard Operating Procedure

References

[1] Bridges, W.G., et. al., "Addressing Human Error During Process Hazard Analyses," *Chemical Engineering Progress*, May 1994.

[2] "Guidelines for Hazard Evaluation Procedures, 3rd Edition, with Worked Examples," Center for Chemical Process Safety (CCPS), AIChE, New York, 2008.

[3] Bridges, W.G. (PII) and Marshall, M. (US OSHA), "Necessity of Performing Hazard Evaluations (PHAs) of Non-normal Modes of Operation (Startup, Shutdown, & Online Maintenance)", 12th Global Congress on Process Safety (GCPS), American Institute of Chemical Engineers (AIChE), 2016.

[4] Bridges, W.G., Al-Zahrani, R, "Best Practices for Addressing Human Factors during PHAs/HAZOPs", 15th Global Congress on Process Safety (GCPS), American Institute of Chemical Engineers (AIChE), 2019.

[5] Bridges, S.G., Bridges, W.G., **"Lessons Learned from Scenarios Found During PHA of Startup, Shutdown, and Online Maintenance"**, 16th Global Congress on Process Safety (GCPS), American Institute of Chemical Engineers (AIChE), 2020.

[6] Bridges, W.G., **"Further Lessons Learned on How to Efficiently Perform the Necessary PHA of Startup, Shutdown, and Online Maintenance"**, 17th Global Congress on Process Safety (GCPS), American Institute of Chemical Engineers (AIChE), 2021.

[7] Tew, R., et.al., "Optimizing Qualitative Hazard Evaluations (or How to Complete A Qualitative Hazard Evaluation Meeting in One-Third the Time Currently Required)," 5th *Global Congress on Process Safety,* AIChE, April 2009.

[8] U.S. Department of Labor: Systems Safety Evaluation of Operations with Catastrophic Potential. Occupational Safety and Health Administration Instruction CPL 2-2.45, Directorate of Compliance Programs, September 6, 1988.

[9] OSHA Inspection Number 106612443 - Phillips 66 Company, Houston Chemical Complex, Citations 1-1 through 1-566, Issued 4/19/1990.

[10] *Stipulation and Settlement Agreement,* Phillips 66 Company ("Phillips") and Lynn Martin, Secretary of Labor, United States Department of Labor, 8/22/1991.

[11] "Process Safety Management of Highly Hazardous Chemicals; Explosives and Blasting Agents," US OSHA Final Rule, 29 CFR 1910.119, February 24, 1992.

[12] "Part 68 – Chemical accident prevention provisions", US EPA Final Rule, 40 CFR 68, Revised as of July 1, 2021.

[13] OSHA Inspection Number 103490306, Issued November 2, 1992.

[14] Woodcock, Henry C., "Program Quality Verification of Process Hazard Analyses (for instructional purposes only)," US OSHA, 1993.

[15] OSHA Inspection Number 123807828; Issued November 18, 1993.

[16] U.S. Department of Labor: PSM Covered Chemical Facilities National Emphasis Program. Occupational Safety and Health Administration CPL 03-00-014, Directorate of Enforcement Programs, November 29, 2011.

[17] U.S. Department of Labor: Petroleum Refinery Process Safety Management National Emphasis Program. Occupational Safety and Health Administration CPL 03-00-010, Directorate of Enforcement Programs, August 18, 2009.

[18] "Investigation Report: Pesticide Chemical Runaway Reaction Pressure Vessel Explosion, at Bayer CropScience, LP, Institute, WV, on August 28, 2008", US Chemical Safety Board, Report No. 2008-08-I-WV, January 2011.

[19] "Investigation Report: FCC Unit Explosion and Asphalt Fire at Husky Superior Refinery. Superior, WI. Incident date: April 28, 2018", US Chemical Safety Board, Report No. 2018-02-I-WI, December 23, 2022.

[20] Contra Costa County Hazardous Materials Programs, *Contra Costa County Industrial Safety Ordinance (ISO)*, by CCHMP. June 15, 2011.

[21] SHEM 02.01 Process Safety Risk Assessment, EHS-PRC-SM-002.01-07, Rev 08, April, 2018, by SABIC

[22] "General guidance on Risk Management Programs for chemical accident prevention (40 CFR Part 68)", EPA 555-B-04-001, US EPA, March 2009