Recipe for a Complete Process Hazard Analysis – Especially Addressing the Key Demands from US CSB

Revonda Tew, Principal Engineer & Instructor
PROCESS IMPROVEMENT INSTITUTE, INC. (PII)
1321 Waterside Lane, Knoxville, TN 37922
e-mail: rtew@piii.com

William G. Bridges, President
PROCESS IMPROVEMENT INSTITUTE, INC. (PII)
1321 Waterside Lane, Knoxville, TN 37922
Phone: (865) 675-3458
Fax: (865) 622-6800
e-mail: wbridges@piii.com

Prepared for Presentation at
13th Global Congress on Process Safety
San Antonio, TX
March 27-29, 2017

UNPUBLISHED

Recipe for a Complete Process Hazard Analysis – Especially Addressing the Key Demands from US CSB

Revonda Tew, Principal Engineer & Instructor
PROCESS IMPROVEMENT INSTITUTE, INC. (PII)

William G. Bridges, President
PROCESS IMPROVEMENT INSTITUTE, INC. (PII)

Keywords: PHAs, Damage Mechanisms, Risk control, Non-routine modes of operations, SOPs, process safety management, PSM

Abstract

Process Hazard Analysis (PHA) is not a new topic. Surprising, more that 80% of PHAs performed today do not comply with the current interpretations by US OSHA, much less the industry best practices. Most PHAs address less than 10% of the hazards during startup, shutdown, and online maintenance[1] and less than about 30% address damage mechanisms such as corrosion, erosion, external impacts, external stresses, vibration, etc. How to address these hazards has been part of the CCPS Guidelines for Hazard Evaluation Procedures since 1991 and the US CSB and US OSHA have noted how these weaknesses have led to many accidents. The citations and comments from US regulators and the CSB are detailed to provide some of the business case for performing more thorough PHAs on these key issues. This paper and presentation also illustrates step-by-step how to address all hazards of the process during ALL modes of operation, during a PHA. The presentation and paper will use examples of process hazards missed and found to illustrate the importance of this step-by-step approach. The results are based on thousands of unit-sized PHAs performed or managed by PII staff.

Background

Process Hazards is a broad term. The relationship between many components define process hazards. For a PHA team, Process Safety Information (information on the chemicals, technology and equipment) and operating procedures are necessary to identify specific components of and analyze a hazard scenario: process deviations (parametric and procedural), their causes, the process safety consequence and various safeguards for detecting deviations and causes, preventing causes, detecting and mitigating consequences and intervening safeguards. A thorough review of incident investigations offers an opportunity to further analyze process hazards.

Over the last twenty years the CSB has brought needed attention, through its investigations of industry incidences, to two significant gaps in many current PHAs; where the teams did not identify and analyze:

- Process hazards unique to non-routine modes of operations resulting in catastrophic consequences and
- Process hazards related to Damage Mechanisms.

Though the intent of the US OSHA PSM regulation has always been for PHA teams to analyze the hazards for all modes of operation, OSHA did not give specific requirements for addressing damage mechanisms and only recently have they increased their enforcement attention on PHA of non-routine modes of operation.

Industry has responded by modifying the *Guidelines for Hazard Evaluation Procedures*, 3rd Edition, 2008,[1] CCPS/AIChE to improve the coverage of these two main issues. API in turn issues guidance on addressing damage mechanisms. Industry best practices now exist for addressing both of these weaknesses. Now, with proper approaches, a team with process safety competencies and process knowledge can thoroughly address the issues during a PHA.

Another less significant gap noted by regulators and by the US CSB has been an incomplete consideration, within the PHA, of previous incidents.

This paper lays out the case from the US CSB and US OSHA on these PHA gaps:

1. Poor or no coverage of hazards during non-routine modes of operations
2. Poor or no coverage of damage mechanisms
3. Poor coverage of prior incidents

This paper also provides proven-in-use best practices for how to close these gaps, while also comparing these best practices to other approaches that have not performed as well.

Although regulatory pressure can be a driver for improvement, data from prior papers on the subject has shown there is near a 1000 to 1 economic return on investment for simply doing a reasonable PHA of non-routine modes of operation (primarily due to the catastrophes avoided).[22]

This paper will **not** cover the other critical aspects of a complete PHA/HAZOP, which can certainly still be problems in PHAs and which PII still finds issues with around the world. The other critical aspects of a fully compliant (excellent) PHA include:

- Excellent team leadership and PHA scribe that are fully competent in all aspects of a Best Practice PHA, including how to efficiently lead and document the PHA
- The most experienced and knowledgeable team members available from operators, operations engineers, and others as needed
- Up-to-date process safety information and access to underlying details, as needed
- Up-to-date, clear, and accurate operating procedures
- Thorough understanding and coverage of facility siting issues and human factors

Increasing Regulatory Pressure Related to PHA/HAZOP of Procedures to Analyzing Process Hazards During All Modes of Operation

Industry initiatives:

Industry has taken some initiatives to help standardize PHA analysis of non-routine modes of operation. One initiative was to improve the focus on PHA of non-routine procedures in *Guidelines for Hazard Evaluation Procedures,* 3rd Ed, 2008, AIChE/CCPS[1]. 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 explained 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 (based on PII data from hundreds of clients) But, the vast majority of 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, the US regulators are beginning to bring more pressure for the regulated companies to do a PHA of all modes of operation.

US OSHA Regulation and Enforcement:

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 there was a PSM regulation from US OSHA**, the Agency published CPL 2-2.45 (Systems Safety Evaluation of Operations with Catastrophic Potential).[2] 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.*[3]

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.[4] **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[5] 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 are presented as a Case Study later in this paper for sake of clarity.

- **Paragraph (e) of the US OSHA regulation on PSM, 29 CFR 1910.119,[6] and similar requirements in US EPA's rule for risk management programs (RMP), 40 CFR 68.24,[7]** 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 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).**[8] 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 incorrectly.

- **US OSHA published an internal document on Program Quality Verification of Process Hazard Analysis in 1993 (by Henry Woodcock, of OSHA).**[3] 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)**[9] – 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 concentration of fuel gas was allowed to enter the heater before the pilot light was ignited. The resulting explosion killed one employee. The operators bypassed safety shutdown features and did not do a visual check of the emergency shutdown system to ensure that the features were closed. 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.

- **Recent US OSHA PSM National Emphasis Programs** for Chemical Processes[10] and also for Refineries[11] 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 has added as Chapter 9.1 in the 3rd edition of *Guidelines for Hazard Evaluation (2008*[1]) 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 to 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*.[1] 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.**

Pressure from the 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 statement was in the report **2008-08-I-WV-R1[12] for the Bayer CropScience accident in Institute, WV, 2008.** In that report, CSB asks Bayer to:

- Revise the corporate PHA policies and procedures to require:
  a. 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
  b. **Addressing all phases of operation and special topics including those cited in chapter 9 of "Guidelines for Hazard Evaluation Procedures" (CCPS, 2008),**
  c. Training all PHA facilitators on the revised policies and procedures prior to assigning the facilitator to a PHA team, and

d. Ensure all PHAs are updated to conform to the revised procedures.

Another strong emphasis on PHA of procedures was in their report: ***Tesoro Anacortes Refinery April 2, 2010 Incident CSB Report, "Catastrophic Rupture of Heat Exchanger," Report 2010-08-I-WA, January, 2014.***[13] This accident resulted in 7 fatalities. In that report, CSB states:

- The startup of the NHT heat exchangers was hazardous non-routine work. Leaks routinely developed that presented hazards to workers conducting the startup activities. Process Hazard Analyses (PHAs) at the refinery repeatedly failed to ensure that these hazards were controlled and that the number of workers exposed to these hazards was minimized.
- None of the Anacortes refinery PHAs effectively evaluated and controlled hazards associated with the non-routine work necessary to periodically clean the NHT heat exchangers. The Washington PSM regulations address the need for non-routine operations to be evaluated and require that at least one member of the PHA team has expertise in non-routine tasks.[14] The CCPS describes the importance of PHA evaluations, as well as the hazardous potential and frequent problems of PHAs that lack sufficient analysis of nonroutine work as follows:[1, 15]
- It is not uncommon for initial PHAs of continuous processes to focus only on normal operations, failing to address non-routine, critical operating modes such as startup, shutdown, preparation for maintenance, emergency operations, emergency shutdown, and other activities whose characteristics may differ considerably from normal operations. Experience indicates that many accidents do not occur during "normal" operation but, rather, during such non-routine modes of operation. Consequently, it is important that a PHA evaluate the hazards of a process during non-routine as well as normal (routine) operating modes. The 1996 Shell Oil PHA for the NHT unit did not evaluate or identify any issues related to non-routine hazardous work associated with the frequent NHT heat exchanger cleaning operations. The 2006 Tesoro NHT unit PHA revalidation identified startup as a non-routine operation but noted that existing procedures were adequately addressing non-routine work.

But there was no PHA on the procedures to determine if there were sufficient protection against errors that could (and did) occur during non-routine operations. Simply stating there are procedures equates to No PHA of non-routine operations.

Another mention was in their report: ***DuPont La Porte, Texas Chemical Facility Toxic Chemical Release Interim Recommendations. Investigation: 2015-01-I-TX. Incident Date: November 15, 2014 Issue Date*: September 30, 2015.**[16] This accident resulted in 4 fatalities. In that report, CSB states:

- DuPont's process hazard analyses (PHAs) and relief system design scenarios do not effectively identify hazards from non-routine operations, such as opening valves to connect the liquid methyl mercaptan piping to the vapor waste gas vent header – the piping connection that provided the pathway for the methyl mercaptan release in this incident. Along the methyl mercaptan feed line there were three locations where it was

connected by valves to the waste gas vent header piping. At the time of the incident, one of these valves was fully open and a second valve was slightly open.

US EPA's RMP Regulation

In the Risk Management Program rule (40 CFR 68.24)[7] EPA also recognizes the importance of procedural analysis, by defining the purpose of a PHA to **"examine, in a systematic, step-by-step way, the equipment, systems, and *procedures* (emphasis added) for handling regulated substances."**

> *A well-done PHA should identify all failure scenarios that could lead to significant exposure of workers, the public, or the environment…….For toxics under PSM, however, you may plan to address a loss of containment by venting toxic vapors to the outside air. In each circumstance, a PHA should define how the loss of containment could occur. However, for EPA, the PHA team should reassess venting as an appropriate mitigation measure. (From EPA RMP Guidance, Chapter 7, pgs 7-6 & 7-7; General Risk Management Program Guidance.[26])*

Pressure from the Local Regulator – Contra Costa County (CCC) California

CCC implements the state's Accident Release Prevention (ARP) regulations locally and have supplemented the Cal-ARP with an Industrial Safety Ordinance (ISO)[17] for elements or features of process safety that they deemed were not handled appropriately (or were missing altogether) from the ARP and/or from Cal-OSHA regulations on PSM. One element they added was the requirement that PHA of Procedures, which requires a guideword analysis, step-by-step, through each critical non-routine task. **These requirements closely follow Chapter 9.1 of the Guidelines for Hazard Evaluation Procedures, 3rd Edition.** CCC Hazardous Materials Department enforces these requirements.

CCCHM contracted PII to perform a Safety Evaluation of the Chevron Richmond Refinery following the August 2012 accident in the Crude Unit. The audit was refinery-wide and included the review of safety culture and also reviewed refinery implementation of process safety versus industry best practices. One specific finding listed in the Draft Report[18] was:

- **Recommendation 5 from the Draft Report:** Continue and expand the current Procedural PHA program implementation so that all modes of operation are evaluated. Include a PHA of startup, shutdown, and online maintenance procedures, as described in Chapter 9 of the *Guidelines for Hazard Evaluation Procedure*s, 3rd edition, CCPS/AIChE, 2008.[1] This will entail using a 2-guideword HAZOP approach on each step for critical procedures and a What-if (no guideword) approach for less-critical procedures. No procedures should be excluded.[1, 22, 23, 24]

Increasing Regulatory Pressure Related to Addressing Damage Mechanism during PHA/HAZOP

Industry initiatives:

From the second edition of the *Guidelines for Hazard Evaluation Procedures* (1991) until 2007, there has been a good explanation and examples of how to cover damage mechanisms during PHA/HAZOP. However, most PHAs did not follow the examples in this textbook and instead provided no or minimal coverage of damage mechanisms such as corrosion, erosion, wrong materials of construction, external impacts, etc.

At the request of US CSB following the large explosion and losses at *Formosa Plastic*[19], the industry has taken some initiatives to improve the coverage of damage mechanism. In particular, additional text was included in the *Guidelines for Hazard Evaluation Procedures,* 3rd Ed, 2008, AIChE/CCPS[3] that emphasized the earlier examples of how to address damage mechanism during PHA team meetings and in the PHA report. In addition, ***API 571***[20] was issued that discussed various damage mechanisms and how these should be addressed by companies.

Many companies have taken the initiatives to do the same, including many of the largest chemical, petrochemical, and refining companies. But, the vast majority of companies do not provide thorough coverage of damage mechanisms during their PHA/HAZOP.

Pressure from the US Chemical Safety and Hazard Investigation Board (US CSB)

The CSB has made numerous references to the need for PHA/HAZOPs to address all damage mechanisms. Based on interviews of senior staff at CSB by PII staff, they recognize this as the second largest deficiency in current PHAs and have discussed this in presentations at the Global Congress on Process Safety (GCPS) over the past few years. In addition, they have provided in-depth analysis of a few accidents that stemmed from failure to address damage mechanisms, including the 2012 release and fire at Chevron's Richmond, Ca, Refinery and the catastrophic rupture of the heat exchanger at Tesoro Anacortes Refinery, 2010.

One of the first and strongest emphasis by US CSB on considering damage mechanisms during PHAs was in the ***Tesoro Anacortes Refinery April 2, 2010 Incident CSB Report, "Catastrophic Rupture of Heat Exchanger,"*** *Report 2010-08-I-WA, January, 2014.*[13] This accident resulted in 7 fatalities (note that the Anacortes Refinery was owned and operated by the Shell Oil Company prior to 1998). In that report, CSB states:

- The 1996 Shell Oil Naphtha Hydrotreating (NHT) unit PHA simply cited ineffective, nonspecific, judgment-based, qualitative safeguards to prevent equipment failure from high temperature hydrogen attack (HTHA). However, the effectiveness of these safeguards was neither evaluated nor documented; instead the PHA merely listed general safeguards. Had the adequacy of the safeguards been verified, improved safeguards intended to protect against HTHA failure could have been recommended.

- The 2001 and 2006 Tesoro PHA revalidations did not address or modify the analysis performed in the 1996 Shell Oil PHA. The Tesoro 2010 NHT unit PHA failed to identify HTHA as a hazard for the shell of the B and E heat exchangers. For the 15 years before the April 2010 incident, assumptions used by PHA teams at the Anacortes refinery contributed to ineffective safeguards, ineffective hazard identification, and ineffective control of hazards to prevent equipment failures from HTHA damage, such as the E heat exchanger in the NHT unit.
- Shell Oil completed a PHA in 1995 related to process modifications that could increase the hydrogen partial pressure in the NHT heat exchangers. However, when managing this change no consideration, evaluation, or recommendations were made to address the potential for HTHA damage to the NHT heat exchangers.
- Shell Oil and Tesoro periodically performed damage mechanism hazard reviews (DMHRs), called corrosion reviews. However, these reviews did not identify HTHA as a credible failure mechanism for the B and E heat exchangers. These reviews were weakened by primarily relying on design operating data for these heat exchangers rather than data from actual process operating conditions.

Note that the DMHRs were not done as part of a PHA or with a similar PHA team structure.

Another strong emphasis by US CSB on considering damage mechanisms during PHA was in the **U.S. Chemical Safety and Hazard Investigation Board (CSB),** ***Interim Investigation Report: Chevron Richmond Refinery Fire (August 6, 2012).***[21] In that report, CSB states that failure to do damage mechanism hazard reviews and follow-through on recommendations related to know damage mechanisms led in part to the accident.

Pressure from the Local Regulator – Contra Costa County (CCC) California

CCC implements the state's Accident Release Prevention (ARP) regulations locally and have supplemented the Cal-ARP with an Industrial Safety Ordinance (ISO)[17] for elements or features of process safety that they deemed were not handled appropriately (or were missing altogether) from the ARP and/or from Cal-OSHA regulations on PSM. One element they added was the requirement that DM reviews be completed for each unit and that DM be considered in each PHA. CCC Hazardous Materials Department enforces these requirements.

CCCHM contracted PII to perform a Safety Evaluation of the Chevron Richmond Refinery following the August 2012 accident in the Crude Unit. The audit was refinery-wide and included the review of safety culture and also review refinery implementation of process safety versus industry best practices. Recommendation 3 and the background observations from the Draft Report are listed below:

- …since specific/individual damage mechanisms from API 571 "Damage Mechanisms Affecting Fixed Equipment in the Refining Industry"[20] are not considered at each process section (node) within the process, it is likely that unique hazardous scenarios have been missed (best practice, as stated in *Guidelines for Hazard Evaluation Procedures*, 2008[1], is to consider damage mechanisms within each equipment node). It is also likely that some

necessary safeguards such as remote isolations, leak detection, etc., for pipe sections, pumps, vessels, and columns have been missed.

- [Refinery] management reports that the Design Engineering Group piloted a specification- break review in 2013 (specification "spec" breaks are where the materials of construction or pipe thickness change). Also, each PHA is intended to identify any potential spec break concerns within the unit (as is typical for PHAs that follow industry best practice). It is understood that a policy and procedures to codify spec-break reviews will be implemented. This approach to damage mechanisms related to materials specification is considered a best practice. Most competent PHA teams in the industry ensure a discussion of each spec break during a PHA.
- **Recommendation 3 from the draft report**: To avoid missing causes and necessary safeguards against loss of containment, be sure hazardous scenarios starting from pertinent damage mechanisms are reviewed during each unit's PHA (pertinent damage mechanisms include corrosion, erosion, seal failure, pump failure, external impact, external fire, material defect, improper maintenance, drains/vents left open, etc.). In particular, review external impact as a damage mechanism for each node. A review of such loss of containment scenarios in each node is recommended, as described in the *Guidelines for Hazard Evaluation Procedures*, 3rd Edition, 2008, CCPS/AIChE.[1] Adding a loss of containment deviation would double-check against missing standard damage mechanisms (such as corrosion and erosion) during unit-wide reviews. It would also improve the current PHAs by providing a review at each node for external impacts and control of drains/vents. Review and incorporate mechanical integrity data during this analysis.

Best Practice for PHA/HAZOP of Procedures to Analyze Process Hazards During All Modes of Operation

Overview of Methodology for Hazard Evaluation of Non-Routine Modes of Operation

The hazard evaluation of non-routine modes of operation involves reviewing procedures using a HAZOP, simplified HAZOP, or What-if analysis to uncover potential accident scenarios associated with non-routine operations, for continuous or batch operations. Human error is more likely and more critical during non-routine operations. By analyzing procedural steps where human error is more likely, and where human error or component failure could lead to a consequence of interest, risk can be reduced. The hazard evaluation team's objective is to evaluate the risk associated with skipping steps and performing steps wrong.

FMEA cannot be applied to procedure-based deviations, unless you create a "human" component, in which case you have simply merged HAZOP deviations for "steps" into FMEA. Pre-Hazard Analysis (P_rHA) and other hazard evaluation methods are not applicable for accomplishing a detailed hazard evaluation of non-routine modes of operations.

Checklist of human factors issues (see an earlier paper[22, 23, 24] and also in the *Guidelines for Hazard Evaluation Procedures*[1]**)** can be very useful after the detailed hazard evaluation of deviations of steps. Such analysis can indicate where generic weaknesses exist that can make errors during any mode of operation more likely, or that can make errors during maintenance more likely. Such human factors checklists are normally used at the end of the analysis, they can be done piecemeal during an analysis (on breaks from the meetings) by individuals on the team, and then the results of each individual review can be discussed as a team at the end.

Purpose of Hazard Evaluation of Procedures-Based Modes of Operation

Although incorporating human factors considerations into hazard evaluation studies of continuous operation is straightforward by asking why the human might make a mistake that leads to a parametric deviation, this approach only addresses a small fraction of the potential human errors that can affect process safety. Many analysts have tried to find accident scenarios in non-routine modes of operations by adding generic guide words such as "deviations during startup" and "deviations during maintenance/sampling" to the hazard evaluation of equipment nodes/sections. Unfortunately, this only catches a fraction of the accident scenarios that can occur in non-routine modes since a hazard evaluation team is focused on "continuous" mode of operation during HAZOP or What-if of equipment sections/nodes.

From an informal survey of more than 100 companies, most do not currently perform process hazard evaluations of procedures, although many do perform some type of job safety analysis (JSA). The JSA is an excellent starting point for an evaluation of procedures because a JSA identifies the tasks that workers perform and the equipment required to protect workers from typical industrial hazards (slips, falls, cuts, burns, fumes, etc.). Unfortunately, a typical JSA will not usually identify process safety issues or related human factors concerns. For example, from a JSA perspective, it may be perfectly safe for an operator to open a steam valve before opening a feed valve; however, from a process safety perspective, the operator may need to open the feed valve before the steam valve to avoid the potential for overheating the reactor and initiating an exothermic decomposition. The primary purpose of a JSA and other traditional methods for reviewing procedures has been to ensure that the procedures are accurate and complete (which is required of employers in 29 CFR 1910.119(f)(3)).[6]

By contrast, the purpose of a hazard evaluation is ***not*** to ensure the procedures are accurate and acceptable, but instead, to ***evaluate the accident scenarios if the procedures are not followed***. Even the best procedure may not be followed for any number of reasons, and these failures to follow the prescribed instructions can and do result in incidents. In fact, in the chemical industry and most other process industries the chance of an operator or other worker making a mistake in following a procedure is greater than 1/100, and in some cases much greater. When taking into account common human factor deficiencies that accompany non-routine operations, such as fatigue, lack of practice, the rush to restart and return to full production, etc., the probability of errors can climb to 1/10 chances per task (a task being about 1 to 10 detailed steps). [28, 29]

The purpose of a hazard evaluation of non-routine modes of operation (governed by written procedures) is to make sure an organization has enough safeguards for the inevitable instance when a step is either performed wrong or skipped (inadvertently or due to shortcutting or other reasons)

Industry has found that a HAZOP or what-if analysis, structured to address procedures, can be used effectively for finding the great majority of accident scenarios that can occur during non-routine modes of operation.[1, 22, 23, 24] Experience shows that reviews of non-routine procedures have revealed many more hazards than merely trying to address these modes of operation during the P&ID driven hazard evaluations.

To reinforce the need for and to explain the method for analysis of deviations of steps in a procedure, Section 9.1 was included in the 3rd Edition of *Guidelines for Hazard Evaluation Procedures,* 2008[1]; this was one of the major changes to the hazard evaluation procedures**.**

HAZOP Method for Analyzing Deviations of Procedural Steps

The Hazard and Operability (HAZOP) method has two major variations; one for the continuous mode of operations (where the team brainstorms what would happen if there were deviations of parameters) and procedure-based (where the team brainstorms what would happen when the steps of a procedure are not followed correctly). The procedure-based variation of HAZOP is the oldest form of HAZOP (from ICI in 1960s).[1, 25] It was an expansion of a Hazard Evaluation method based strictly on asking:

- **What happens if the step is skipped?**
- **What happens if the step is performed wrong?**

In turn, the "pre-HAZOP" method for brainstorming accident scenarios from not following procedures (including because the procedure is itself wrong) is based on the understanding that human errors occur by someone not doing a step (errors of omission) or by doing a step incorrectly (errors of commission). So, simply asking what would happen if the operator omitted a step or performed a step wrong is one way to structure a hazard evaluation of a step-by-step procedure. The usefulness of this simple approach to hazard evaluation of steps will be discussed later.

Seven (7) Guide Word Method

In an effort to be more thorough, the inventors of HAZOP (at ICI) broke these two types of errors into subparts and agreed on using the following 7 Guide Words:

Omission:	**Skip (or Step Missing)**
	Part Of
Commission:	**More**

Less
Out of Sequence
As Well As
Other Than
Reverse

In the early 1990s, the guide word Skip was augmented by adding the option of discussing "are there any steps **missing** from the procedure."[24]

Table 1: Definitions of 7-8 Guide Words for HAZOP of Procedure-Based (Non-Continuous Mode) Operation

Guide Word	Meaning When Applied to a Step
Missing (optional guide word)	A step or precaution is missing from the written procedure prior to this step (similar to "Out of Sequence", except the missing step is not written)
Skip (No, Not, Don't)	The specified intent of this step is not performed
Part-of	A portion of the full intent is not performed. Usually only applies to a task that involves two or more nearly simultaneous actions ("Open valves A, B, and C".)
More	Too much of the specified intent is done (does not apply to simple on/off; open/close functions); or it is performed too fast
Less	Too little of the intent is done, or it is performed too slowly
Out of sequence	This step is performed too early in the sequence
As well as	Something happens, or the user does another action, in addition to the specified step being done correctly (could be a short cut)
Other than (or Reverse)	The wrong device is operated, selected, read, etc., or operated in a way other than intended. Or the wrong material is selected or added. "Other than" errors always imply a "Skip" as well.

To apply HAZOP to procedural steps for startup, shutdown, online maintenance, and other modes of operation, the facilitator (or team) first divides the procedure into individual actions. This is already done if there is only one action per step. Then, the set of guide words or questions is systematically applied to each action of the procedure resulting in procedural deviations or what-if questions. The guide words (or procedural deviation phrases) shown in Table 1 above were derived from HAZOP guide words commonly used for analysis of batch processes. The definition of each guide word is carefully chosen to allow universal and thorough application to both routine batch and non-routine continuous and batch procedures. The actual review team structure and meeting progression are nearly identical to that of a process equipment HAZOP or what-if analysis, except that active participation of one or more operators is even more important and usually requires two operators for a thorough review; a senior operator and a junior operator. For each deviation from the intention of the process step (denoted by these guide words applied to the process step or action), the team needs to dig beyond the obvious

cause, "operator error," to identify root causes associated with human error such as "inadequate emphasis on this step during training," "responsible for performing two tasks simultaneously," "inadequate labeling of valves," or "instrument display confusing or not readable." The guide word *missing* elicits causes such as "no written procedural step or formal training to obtain a hot work permit before this step," or "no written procedural step or formal training to open the discharge valve before starting the pump."

Two (2) Guide Word Method for Analyzing Deviations of Procedural Steps

A more streamlined guide word approach has also proven very useful for (1) procedures related to less hazardous operations and tasks and/or (2) when the leader has extensive experience in the use of the guide words mentioned previously and can therefore compensate for the weaknesses of a more streamlined approach. The two guide words for this approach (as defined in Table 2 below) encompass the basic human error categories: errors of omission and commission. These guide words are used in an identical way to the guide words introduced earlier. Essentially "omit" includes the errors of omission related to the guide words "skip," "part of," and "missing" mentioned earlier. The guide word "incorrect" incorporates the errors of commission related to the guide words "more," "less," "out of sequence," "as well as," and "other than" mentioned earlier. Note that these two guide words (Table 2) fill the basic requirements for a human error analysis as outlined in OSHA's CPL 2-2.45.[2]

Table 2: 2 Guide Word (Guide Phrases) for Modified-HAZOP of Procedure-Based Operation

Guide Phrase	Meaning When Applied to a Step
Step not performed	The step is not done or part of the step is not done. Some possible reasons include the employee forgot to do the step, did not understand the importance of the step, or the procedures did not include this vital step
Step performed wrong	The employee's intent was to perform the step (not omit the step), however, the step is not performed as intended. Some possible reasons include the employee does too much or too little of stated task, the employee manipulates the wrong process component, or the employee reverses the order of the steps.

Table 3: Example of 2 Guide Word HAZOP of a Critical Step in a Procedure

Drawing or Procedure: SOP-03-002; ***Cooling Water Failure***	**Unit:** HF Alkylation	**Method:** 2 Guide Word Analysis	**Documentation Type:** Cause-by-Cause

Node: 23	**Description:** STEP 2: Block in olefin feed to each of the 2 reactors by blocking in feed at flow control valves				
Item	**Deviation**	**Causes**	**Consequences**	**Safeguards**	**Recommendation**
23.1	Step not performed	Operator failing to block in one of the reactors, such as due to miscommunication between control room operator and field operator; or control valve sticking open or leaking through	High pressure due to possible runaway reaction (because cooling is already lost), because of continued feeding of olefin (link to 11.7 - High Rxn Rate; HF Alky Reactor #1/#2) High pressure due to high level in the reactor, because of continued feeding olefin (link to 11.1 - High Level; HF Alky Reactor #1/#2)	High temperature alarm on reactor High pressure alarm on reactor Field operator may notice sound of fluid flow across valve Flow indication (in olefin charge line to reactor that is inadvertently NOT shutdown) Level indicator, high level alarm, and independent high-high level switch/alarm	
		Operator failing to make sure bypass valve is also closed, since this precaution is not listed in the written procedure; or the bypass valve leaks through	High pressure due to possible runaway reaction (because cooling is already lost), because of continued feeding of olefin (link to 11.7 - High Rxn Rate; HF Alky Reactor #1/#2) High pressure due to high level in the reactor, because of continued feeding olefin (link to 11.1 - High Level; HF Alky Reactor #1/#2)	High temperature alarm on reactor High pressure alarm on reactor Operator skill-training requires checking bypasses are closed, when blocking control valves Field operator may notice sound of fluid flow across valve Flow indication in olefin charge line (but likely not sensitive enough for small flows) Level indicator, high level alarm, and independent high-high level switch/alarm	
		Operator failing to close low control valve manually from the DCS because the phrase “block in” is used instead of the word “close”	Valve possibly opens full at restart, allowing too much flow to reactor at restart, resulting in poor quality at startup and/or possibly resulting in runaway reaction and high pressure	Control room skill training requires always manually commanding automatic valves closed before telling field operator to block in control valve	37. Implement best-practice rules for procedure writing, which includes using common terms.
23.2	Step performed wrong	Operator closing the olefin charge flow control valves before shutting down the charge pump, primarily because the steps are written out of the proper sequence	Deadheading of charge pump, leading to possible pump seal damage/failure and/or other leak, resulting in a fire hazard affecting a small area (link to 5.12 - Loss of Containment; Olefin Charge Line/Pump)	Step 3 of procedure that says to shutdown charge pump The step to shut down the charge pump (Step 3) is typically accomplished before Step 2 (in practice)	41. Move Step 3 ahead of Step 2.
		Field operator closing both upstream and downstream block valves	Possible trapping of liquid between block valve and control valve, leading to possible valve damage (due to thermal expansion)	Field operator skill training stresses that only one block valve should be closed	

What-if Method for Analyzing Deviations of Procedural Steps

The What-if method for analyzing procedure-based modes of operations is free brainstorming without the aid (or constraints) of guide words. This method is described in detail in the *Guideline for Hazard Evaluation Procedures (CCPS).*[1] The hazard evaluation team using this method would read the procedure and then answer the question: "What mistakes will lead to our consequences of interest?" The team would list these mistakes and then brainstorm the full consequences, causes, and existing safeguards – the same analysis approach described for the guide word approaches mentioned earlier in this section. What-if brainstorming **is not** applied to each step of the procedure, but rather covers the entire task (procedure) at one time.

Choosing the Right Method for Analysis of Non-Routine Modes of Operation

Obviously the What-if approach takes far less time than the 2-Guide Word method, and the 2 Guide Word method takes much less time than the 7-8 Guide Word method of HAZOP of procedures. Experience has shown that hazard evaluation facilitators, newly trained in the three techniques above, tend to overwork an analysis of non-routine procedures, so a tiered approach is best. In this tiered approach, the first step in choosing the right method of analysis in the hazard evaluation of procedures is to screen the procedures and select only those procedures with extreme hazards. These procedures should be subjected to a detailed HAZOP analysis (7-8 guide word set) presented above. The 2-Guide Word set is efficiently used for less complex tasks or where the consequences are lower. The What-if method is applicable to low hazard, low complexity, or very well understood tasks/hazards.

Experience of the leader or the team plays a major part in selecting the procedures to be analyzed, and then in deciding when to use each guide word set.

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 enough 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.

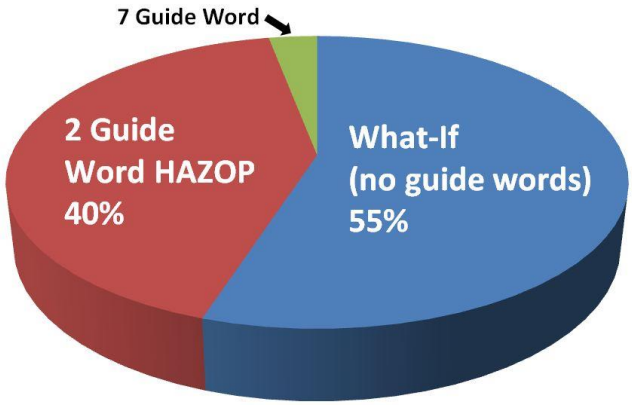


Figure 1. Relative Usage of Techniques for Analysis of Procedure-Based Modes of Operation [1, 22, 23, 24]

The experience of the leader or the team plays a major part in selecting the method to use for each task/procedures to be analyzed. However the first decision will always be "are these procedures ready to be risk reviewed?" 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 Figures 2A and 2B below:

Figure 2A: PHA of a ALL Modes of Operation for a CONTINUOUS Process

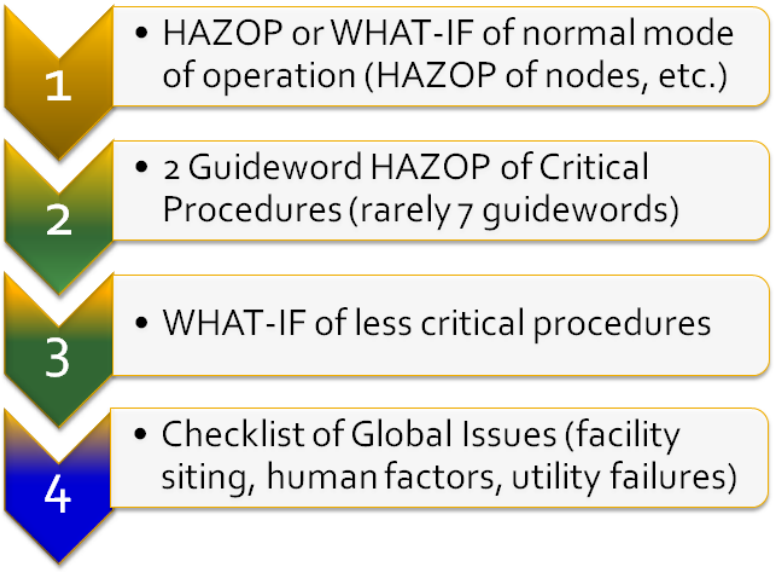
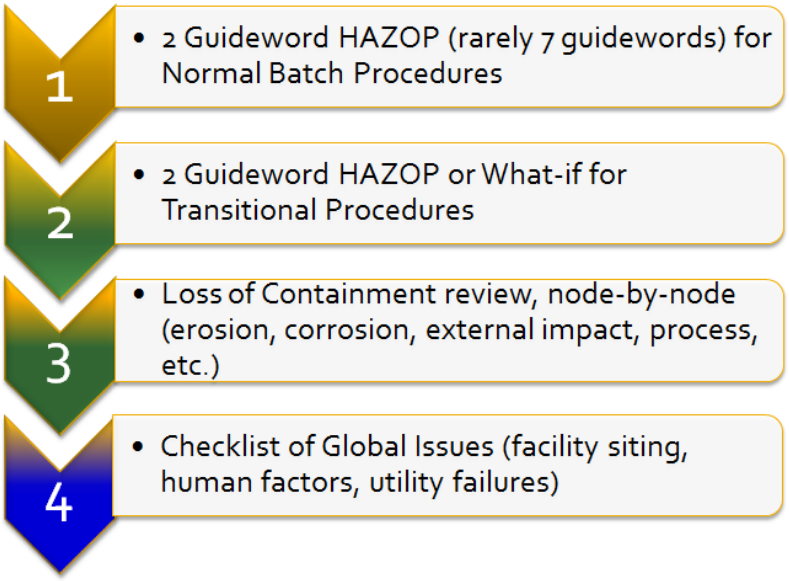


Figure 2B: PHA of a ALL Modes of Operation for a BATCH Process



If your procedures are not at least 90% accurate, 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.

Any procedure (even a computer program) can be analyzed using these techniques. Reviews of routine procedures are important, but reviews of non-routine procedures are even more important. As mentioned earlier, the nature of non-routine procedures means that operators have much less experience performing them, and many organizations do not regularly update these procedures [though this should change as companies comply with 29 CFR 1910.119(f)][6]. Also, during non-routine operations, many of the standard equipment safeguards or interlocks are off or bypassed.

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.[1, 22, 23, 24]

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, actually, 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[23]), 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 70-80% of catastrophic accidents occur during non-routine modes of operation.[22] Figure 4 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.[1, 22, 23, 24]

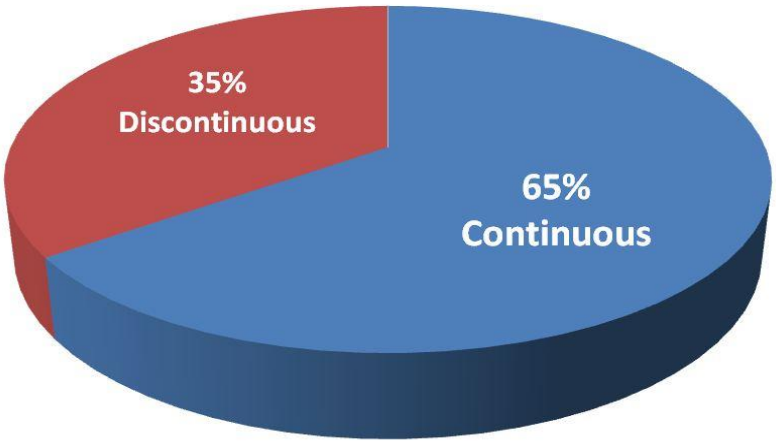


Figure 3. Relative Amount of Meeting Time Spent for Analysis of Routine and Non-routine Modes of Operation for a Continuous Process[1, 22, 23, 24]

General Guidelines for Analyzing Non-routine Modes of Operation or Batch (Step-by-step) Processes

- Define the assumptions about the system's initial status. "What is assumed to be the starting conditions when the user of the procedure begins with Step 1?"
- Define the complete design intention for each step. "Is the step actually 3 or 5 actions instead of one action? If so, what are the individual actions to accomplish this task?"
- Don't analyze safeguard steps that start with ensure, check, verify, inspect, etc., or where the consequence of skip is "loss of one level of safeguard/protection against ….." There is no reason to analyze these steps since they will show up as safeguards of deviations of other steps. This approach is similar to not analyzing a PSV during a HAZOP of continuous mode (parametric deviation analysis); instead the PSV is shown as a safeguard against loss of containment.
- Together with an operator before the meeting, identify the sections of the procedures that warrant use of:
    - 7-8 Guide Words (extremely large consequences can happen if deviations occur)
    - 2 Guide Words (the system is complex, mistakes are costly, or several consequences could occur)
    - On others, use What-If (no guide words or guide phrases; for use on simpler or lower hazard systems)
- Decompose each written step into a sequence of actions (verbs)
- Apply guide words directly to the intentions of each action

The Following Preparation Steps May Also Be Needed:

- Walk through procedure in the plant with one or more operators to see the work situation and verify the accuracy of the written procedure. This is optional and should have also been performed as part of validation of the procedure after it was originally drafted
- Determine if the procedure follows the best practices for "presentation" of the content; the best practices will limit the probability of human error
- Discuss generic issues related to operating procedures, such as:
    - staffing (normal and temporary)
    - human-machine interface
    - worker training, certification, etc.
    - management of change
    - policy enforcement
- Review other related procedures such as lock out/tag out and hot work.

IF the procedures are NOT >90% accurate, then redo procedures first!

Best Practice for Addressing Damage Mechanisms During PHAs

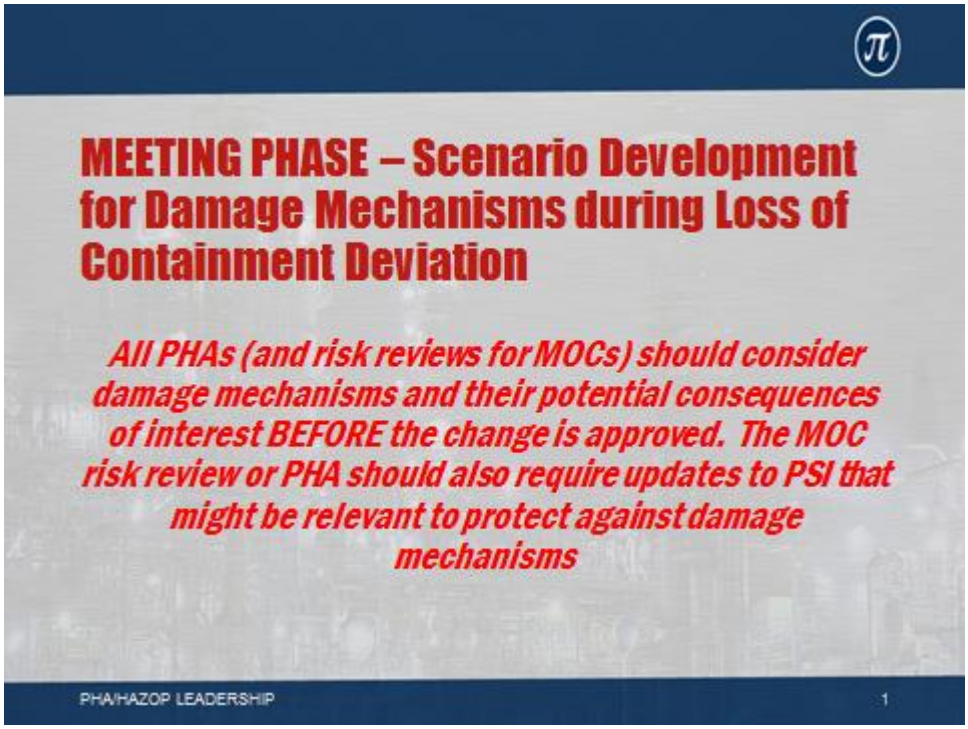


Figure 4. Meeting Phase – Review of Damage Mechanisms

Recently, US CSB and more and more regulators are making analysis of Damage Mechanisms (DMs) a PHA requirement. This requires that potential process damage mechanisms and their potential consequences of interest be identified. Damage mechanisms can be broken down into three main categories. These categories and examples of each are shown in the following table.

Table 4: Types of Damage Mechanisms

Mechanical	• Mechanical loading failure • Mechanical fatigue • Buckling • Cracking • Embrittlement • Ductile fracture • Brittle fracture

Chemical	• Corrosion
	  ○ Uniform
	  ○ Localized
	  ○ Pitting

Physical	• Thermal failures
	  ○ Creep
	  ○ Thermal fatigue
	  ○ Transformation

The team may use aids such as piping specs, established literature and standards, any applicable MOC documents, etc. to help identify DMs. The PHA leader has several options of how to address damage mechanisms:

- Discuss during HAZOP under "Loss of Containment" deviation
    - **This is PII's preferred approach and is one we recommend to all clients, so this is discussed in more detail below.**
- Note damage mechanisms revealed during discussions of other process deviations
    - Pressure
    - Temperature
    - Concentration

  The consequence of these deviations is ultimately loss of containment. Therefore causes of pressure, temperature and concentration deviations can be damage mechanisms and ultimately lead to loss of containment.
- Include Damage Mechanisms as a separate node (for HAZOP technique), *such as proposed by Risk Management Professionals.*[26]
- Perform a "mini" Mechanical Integrity checklist reviews under each process node
- Divide P&ID (or PFD) into separate services for purposes of DM hazard review (DMHR) discussion considering:
    - Process
    - Chemical
    - Spec changes
    - Flow through
    - Operating parameters

  This approach is used by some refineries to accomplish the requirements of a DMHR as recommended in API RP 571.[20] *From PII's experience, this approach has merit and finds some issues that the preferred PII does not always find, BUT overall the PII approach is superior in finding the key scenarios related to damage mechanisms and related safeguards because the review is specific to each Node of process equipment.*

Damage mechanisms can (and sometimes ***should***) be reviewed prior to the PHA. For example, all MOCs should consider damage mechanisms and their potential consequences of interest before the change is approved. The MOC should also require updates to process safety information which might be relevant to protect against DMs.

Coverage of Damage Mechanism for Each Major Section (HAZOP section or What-If node) – as recommended by PII

As mentioned above this is PII's preferred method for thoroughly covering all DM within a PHA/HAZOP of an entire unit. The benefits are that the team can more easily catch changes in DM from section to section and they can more easily identify when unique safeguards, such as Remote Isolation Valves, segregated containments (dike), and unique materials of construction are needed. To facilitate this, a list of generic causes of loss of containment and a generic list of safeguards against loss of containment are covered in the Loss of Containment (LOC) deviation of each section. Below are tables that summarize the typical causes of loss of containment and typical safeguards against loss of containment.

Table 5 Typical Causes of Loss of Containment (and Tube Leak/Rupture) to Discuss in Each Major Process Section (includes Damage Mechanisms)

- Corrosion – internal, including steady corrosion and also stress cracking
- Corrosion - external (including corrosion under insulation
- Erosion
- Fatigue failure (such as due to vibration)
- Improper material of construction (including wrong grade of welding rod/wire)
- Improper maintenance/repair
- Drain valve open
- Vent valve option
- Instrument line breaks
- External impact or external load (crane, load dropped, fork truck, backhoe, failure of structural supports, etc.)
- External fire (flame impingement and heating)
- Thermal expansion (while process is blocked-in)
- Lightning

➢ Any deviation that links into loss of containment as a cause, such as high process temperature or high process pressure

Table 6 Examples of IPLs Protecting Against or Mitigating Damage Mechanisms

RELIEF VALVES

- Relief valve designed for the limiting scenario which vents to a safe location or destruction system (can prevent loss of containment due to high pressure events cause by process upsets or external fire)
- Rupture disks (same criteria and functional protection as relief valve except cannot re-seat)
- Conservation vent (same criteria and functional protection as relief valve)
- Vacuum relief valve (same criteria and functional protection as relief valve, except protects against negative pressure)
- Thermal relief valve (online protects against thermal expansion in a closed system)

ISOLATION

- Remote isolation valves that either operate automatically or can be remotely closed manually and the loop qualifies as a Human IPL
- Locally operated manual valves that can be reached quickly and safely (typically not a valid IPL case)

- Remote shutdown of pumps, blowers, etc. to limit amount of material released

CONTAINMENT & MITIGATION

- Double-walled piping for lines that run under rivers and underground and that carry toxics
- Process contained in enclosed building
- Dikes are provided for secondary containment of spills from major vessels; drain valves on diked areas are kept closed/can be closed quickly
- Process areas are drained to sump
- Rainwater runoff containment
- Fire insulation that protects metal structures for 4 hours

SUPPRESSION AND EXTINGUISHING SYSTEMS

- Deluge system under or over tanks or storage vessels
- Manual pull station fire alarms
- Fire extinguishers in the Power Distribution Center
- Fire extinguishers in the control room rated for electrical fire

Table 7 Examples of Non-IPL Safeguards Protecting Against or Mitigating Damage Mechanisms

PIPING

- Applicable design codes are reflected in equipment design
- Welding done by qualified welders using qualified procedures
- Regular inspection (e.g., ultrasonic, X-ray) for wall thickness
- The wall thickness inspection frequency is increased in critical areas (e.g., areas where erosion or corrosion are likely)
- Systems are leak checked (pressurized with air and soap bubble applied at flanged joints) before starting up after systems are opened for maintenance
- A winterization list is used to check freeze-protection features before the onset of cold weather
- Piping and components that are fabricated on site and installed in the process are pressure tested before they are installed as necessary

PUMPS

- Written specifications in standard maintenance procedures (SMPs) for pumps to help ensure that pumps are maintained, repaired, and replaced in a way that meets original specifications

VALVES

- Fugitive emissions monitoring program that includes monitoring valves for packing leaks and

flange leaks
- Fail-safe settings for control valves upon loss of instrument air, nitrogen, or electric power

CORROSION DETECTION AND PREVENTION
- Periodic inspection of piping, equipment, and structures
- Application of exterior paint and protective coatings when needed on piping, equipment, and structures
- Positive material identification (PMI) of 100% of components and welds in the field/unit

EQUIPMENT MAINTENANCE
- Periodic walkthroughs by personnel inspecting for leaks or other abnormalities, and checking local instrumentation
- Preventive maintenance systems, including:
    - Lubrication schedule
    - Operators inspect pump seals for visible leaks
    - Records of equipment failures
- Periodic inspection of heat exchanger tube bundles

INSTRUMENTATION
- All controllers are indicating controllers
- Testing and calibration of critical process instrumentation

PERSONNEL PROTECTION
- Personal protective equipment (PPE), including:
    - Self-contained breathing apparatus
    - Respirators
    - Protective clothing
- Periodic inspection and testing of PPE and personal safety systems, including:
    - Self-contained breathing apparatus
    - Safety showers
- Availability of:
    - First aid kit
    - Specially trained Emergency Medical Technicians

EMERGENCY RESPONSE
- Remote emergency communication systems, including:
    - Handheld, two-way radios
    - Buddy system for critical or hazardous operations
    - Emergency communications procedures
    - Telephones
    - Emergency reporting stations strategically located in the plant
- Cooperative fire brigade
- Plant wide alarm system
- Facility and unit contingency plan

- Emergency procedures for special incidents
- Trained HAZMAT response teams with emergency equipment
- Spill containment and control guidelines; all operators receive hazardous waste operations and emergency response (HAZWOPER) training

The Leader and Scribe must consciously discuss the typical damage mechanisms listed in Table 5 and discuss at each LOC deviation (so, once in each section).

Documentation of Results of Damage Mechanism Discussions in PHA Meetings

For each node (each line, each vessel, each column, etc.), the PHA team should discuss and document each damage mechanism listed in Table 5 (as a cause of loss of containment), consequence of the failure if the damage mechanism occurs, and the safeguards in place to prevent the damage mechanism, detect the mechanism before failure, prevent the release, detect and response to the release, and mitigate or contain the release.

The documentation style varies between PHAs. Figure 5 show two different styles that have been acceptable in the past.

- One style (Example A) uses a reference to a summary table of typical causes (this summary table is not shown but is similar to Table 5 of this paper) instead of listing each individual damage mechanism. In Example A, the same approach is used for safeguards. This approach saves redundant text and some time, but it requires the leader and scribe to be diligent to cover everything in the Typical tables that were referenced in the Cause and Safeguard columns. A modified approach is to relegate some generic causes and safeguards to Typical tables for reference and then to carefully list the specific cause and/or safeguards of interest for LOC for each specific node.
- Example B does not use or reference a generic or Typical list of causes (damage mechanism) or Typical safeguards, but instead develops a specific listing for the LOC deviation of each node. This style has proven easier to justify to regulators and other outside reviewers but takes more documentation effort.

Regardless of method, the team leader and scribe must ensure the team rigorously discusses all of the damage mechanisms in Table 5 and adequately documents the results of the damage mechanism review in the PHA/HAZOP analysis tables.

Figure 5. Excerpts from Select PHA Reports Showing Various Acceptable Styles for Documenting Damage Mechanism Review Results Within the LOC Deviation

Example A – Referencing Generic Tables for Typical Causes and Typical Safeguards

Dev#	*Deviation*	*Causes*	*Consequences*	*Existing Safeguards*	*Recommendations*
9.10	Loss of containment	Accelerate corrosion External fire High pressure (linked from 9.7) Typical causes of loss of containment (see Table A.1)	Release to atmosphere leading to potential injury of workers and/or community	Pressure Relief Valve's 231A, B, C on Reactor and no valves in line to reactor Most lines / connections are welded construction; only a few flanges Drills conducted each year on evacuation, rescue and isolation Emergency Response personnel are trained at SABIC FTC Generic safeguards protecting against or mitigating process material releases (see Table A.2)	Safety 7. Consider changing the ITPM schedule for managing most PSVs whose inspections are too infrequent based on industry standards and best practice. For instance, the current inspection frequency for PSV-8220 on the Ammonia Receiver (I-2005G) is 9 years, whereas, consensus codes typically recommend testing/inspection every 1-4 years for PSVs in highly toxic services.

Example B – Specific Listing of Causes and Safeguards

1.9	Loss of containment	Corrosion/erosion External fire and/or flame impingement Gasket, packing, or seal failure Improper maintenance Material defect Operator failing to close or inadvertently opening a valve to the atmosphere (e.g., a valve at a hose connection) Railcar inadvertently derailed Valve leaking to the atmosphere High pressure (linked from 1.5) Acid corrosion caused by high concentration of water (linked from 1.8) High ambient temperature External impact (such as from a mini-engine or another railcar)	Catastrophic release of chlorine from a ruptured railcar Steady release of chlorine from a ruptured connection Steady release of chlorine from a leaky connection High pressure caused by thermal expansion of liquid chlorine if railcar is also over-full	Chlorine repair kit Derailer and warning flag to prevent impact by a mini-engine or another railcar Limited vehicular access to area Maintenance/operator response as required, including isolation if needed Operator periodically monitoring the railcar valves while unloading Personal protective equipment in the area Plugs installed in all chlorine valves to the atmosphere when the valves are not in use Relief valve on each railcar for mitigating releases caused by overpressure Supplier maintenance of railcars (per strictly enforced US DOT requirements) Video monitoring of the unloading area Concrete crossties on rail spur Dike preventing any combustibles spilled nearby from reaching the unloading rack area Concrete railroad ties in chlorine unloading area to prevent fires near railcar	10. Consider installing a chlorine detection system in the unloading and vaporizing area to help detect chlorine releases (especially at likely release points) 11. Verify that periodic maintenance and inspections are being performed in accordance with Chlorine Institute recommendations 12. Review the drainage system for the unloading are, and identify the areas that may be affected by a large chlorine release 13. Consider prohibiting the use of heavy equipment (e.g., cranes) in the unloading and vaporizing area unless special precautions to prevent equipment damage are enacted 33. Consider providing a high pressure alarm for each vaporizer 40. Consider providing a water deluge system in the unloading area to help mitigate chlorine releases from the railcar

Best Practices for Addressing Previous Incident

Information on process hazards is also found in incident investigation reports and are often discounted. PHAs predict what can go wrong. Incidents are actual sequences of human errors and equipment failures. Don't miss this opportunity to thoroughly review previous incidents. There is no industry or regulatory guidance regarding how to incorporate previous incidents into HEs. The intent is to review near misses and accidents to ensure that potentially catastrophic events are identified and analyzed.

Typically, this is done by listing and then discussing relevant incidents in the industry and in similar plants to:

- Help identify potential causes or consequences of interest
- Evaluate related safeguards in the process, and
- Make recommendations for additional layers of protection if needed to prevent similar incidents related to the system.

Know Your History

- What caused past incidents? *This includes near misses and accidents and also includes incidents in similar systems. If the company has a good system for getting near misses reported and any incident investigated to root causes, then the PHA team will have a deeper understanding of what can go wrong and why. Root cause analysis of incidents is just as important as PHA. The team should volunteer incidents that may not have been reported formally and these should be kept confidential so that more "unreported" incidents are reported within the PHA team setting.*
- What was done in response? *Were any changes made to the system? Did these improve the system (reduce the error or failure rates)? Has the incident reoccurred?*
- If the incident occurred in a system other than the one under review by the PHA team, should similar actions be applied to the system under evaluation?
- Did the previous countermeasures work? *Did these prevent similar incidents?*

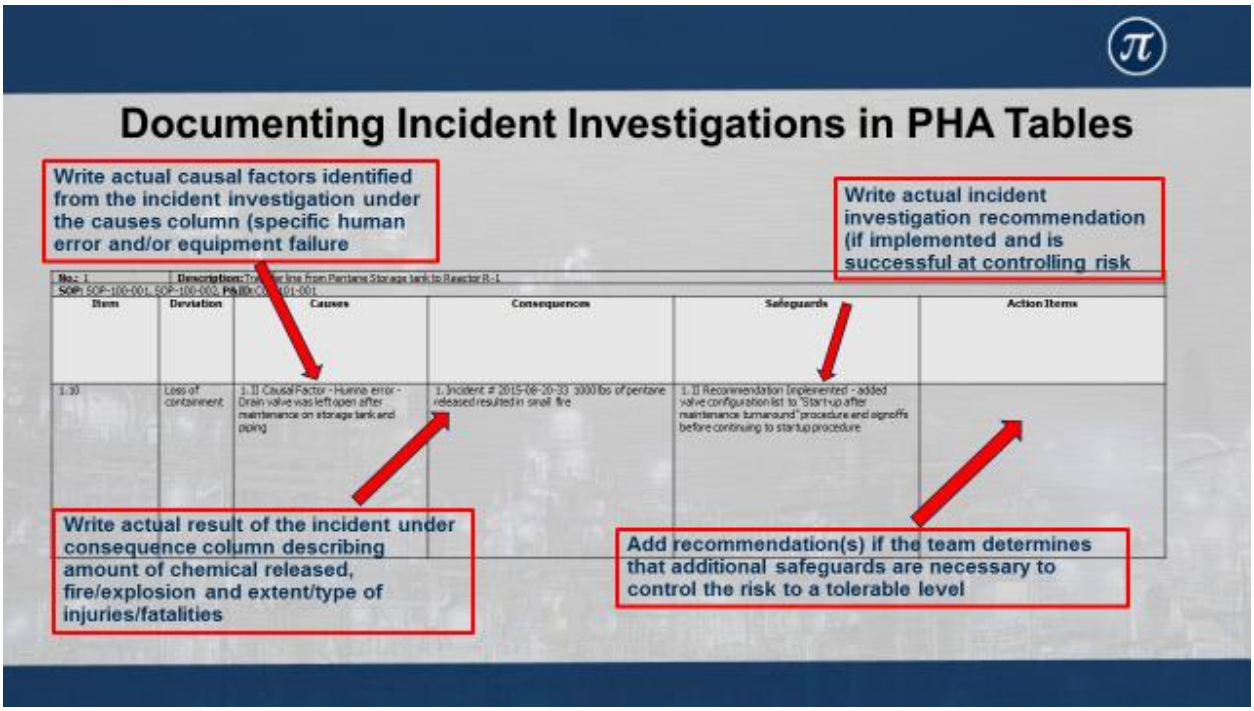


Figure 6. Documenting Incident Investigations in PHA Tables

Conclusions

Qualitative analysis 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. This approach of step-by-step HAZOP and/or What-If analysis is not new to industry, and regulators have required similar approaches for decades. And regulators continue to note lack of analysis of the risk of non-routine operations and lack of risk review of changes to procedures.

> ***From the Wall Street Journal[27] referencing the presidential commission investigating the Deepwater Horizon accident of April 2010:*** *BP had rules in place governing procedural changes, but its workers didn't consistently follow them, according to BP's September [2010] internal report on the disaster and the report released earlier this month [January 2011] by the presidential commission on the accident. "Such decisions appear to have been made by the BP Macondo team in ad hoc fashion without any formal risk analysis or internal expert review," the commission's report said. "This appears to have been a key causal factor of the blowout."*
>
> ***From CSB Report on August 2008 Bayer CropScience Explosion:[12]*** *"The accident occurred during the startup of the methomyl unit, following a lengthy period of maintenance ... CSB investigators also found the company failed to perform a thorough Process Hazard Analysis, or PHA, as required by regulation…In particular, for*

operational tasks that depend heavily on task performance and operator decisions, the team should analyze the procedures step-by-step to identify potential incident scenarios and their consequences, and to determine if the protections in place are sufficient."

Since about 80% of major accidents occur during non-routine modes of operation,[1] the PHA of the deviations from the steps of the procedures that govern these modes of operation is certainly critical. But, of the 20% of the major accidents that occur during normal operation, most of these arise from **damage mechanisms** such as corrosion, material defects, gasket failures, external impacts and the like (based on PII data). PHAs can effectively cover DM while discussing LOC.

So, the PHAs must cover both of these concepts (PHA of all modes of operation and addressing DM) thoroughly to fulfill the role of the PHA in controlling risk. **More regulatory pressure is sure to follow on these two issues**

But of course, the PHA must be strong in all aspects, including consideration of lessons learned from previous incidents.

Acronyms Used

AIChE– American Institute of Chemical Engineers
API – American Petroleum Institute
CCPS – Center for Chemical Process Safety (a division of AIChE)
CSB – US Chemical Safety and Hazard Investigation Board
DM – Damage mechanism
DMHR – Damage mechanism Hazard Review
HAZOP – Hazard and Operability Analysis
HAZWOPER – Hazardous and Waste Operater (US OSHA 29 CFR 1910.120)
HTHA – High Temperature Hydrogen Attack
IPL - Independent Protection Layer
LOC – Loss of Containment
LOPA – Layer of Protection Analysis
MOC – Management of Change
NHT – Naphtha Hydrotreater
OSHA – Occupational Safety and Health Administration, US Department of Labor
PHA – Process Hazard Analysis
PII – Process Improvement Institute, Inc.
P&ID – Piping & Instrumentation Diagram
PSI – Process Safety Information
PSM – Process Safety Management
SOP – Standard Operating Procedure

References

1. *Guidelines for Hazard Evaluation Procedures*, 3rd Edition, 2008, CCPS/AIChE.

2. 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.
3. Woodcock, Henry C., "Program Quality Verification of Process Hazard Analyses (for instructional purposes only)," US OSHA, 1993.
4. OSHA Inspection Number 106612443 - Phillips 66 Company, Houston Chemical Complex, Citations 1-1 through 1-566, Issued 4/19/1990.
5. *Stipulation and Settlement Agreement*, Phillips 66 Company ("Phillips") and Lynn Martin, Secretary of Labor, United States Department of Labor, 8/22/1991.
6. "Process Safety Management of Highly Hazardous Chemicals; Explosives and Blasting Agents," US OSHA Final Rule, 29 CFR 1910.119, February 24, 1992.
7. "Risk Management Programs for Chemical Accidental Release Prevention," US EPA Final Rule, 40 CFR 68, 1994-2000.
8. OSHA Inspection Number 103490306, Issued November 2, 1992.
9. OSHA Inspection Number 123807828; Issued November 18, 1993.
10. 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.
11. 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.
12. "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.
13. U.S. Chemical Safety and Hazard Investigation Board (CSB). *Investigation Report: Catastrophic Rupture of Heat Exchanger (Seven Fatalities), Tesoro Anacortes Refinery, Anacortes, WA, Report No. 2010-08-I-WA, Draft for Public Comment*, January 29, 2014.
14. Washington Administrative Code (WAC) 296-67-291 Appendix C--Compliance guidelines and recommendations for process safety management (nonmandatory) http://www.lni.wa.gov/WISHA/Rules/hazardouschemicals/default.htm#WAC296-67-021 (accessed December 3, 2013).
15. Center for Chemical Process Safety (CCPS). *Revalidating Process Hazard Analyses*. 2001; pp 31-32.
16. U.S. Chemical Safety and Hazard Investigation Board (CSB), *DuPont La Porte, Texas Chemical Facility Toxic Chemical Release Interim Recommendations Investigation: 2015-01-I-TX* Incident Date: November 15, 2014 Issue Date: September 30, 2015
17. Contra Costa County Hazardous Materials Programs, *Contra Costa County Industrial Safety Ordinance (ISO)*, by CCHMP. June 15, 2011.

18. Draft Initial Report "*Safety Evaluation of the Chevron Richmond Refinery*." November, 2015, by Process Improvement Institute, Inc., for Contra Costa County Hazard Materials Department.
19. U.S. Chemical Safety and Hazard Investigation Board (CSB). "CASE STUDY *Fire at Formosa Plastics Corporation: Evaluating Process Hazards,*" July 20, 2006.
20. API RP 571. "Damage Mechanisms Affecting Fixed Equipment in the Refining Industry." 2nd ed., April 2011.
21. U.S. Chemical Safety and Hazard Investigation Board (CSB), *Interim Investigation Report: Chevron Richmond Refinery Fire,* U.S. CSB, August 6, 2012.
22. "Necessity of Performing Hazard Evaluations (PHAs) of Non-normal Modes of Operation (Startup, Shutdown, & Online Maintenance)", W. Bridges and Mike Marshall (US OSHA), *18th Annual International Symposium, Mary Kay-O-Connor Process Safety Center, College Station, TX, October 2015 and 12th Global Congress on Process Safety, April, 2016.*
23. "How to Efficiently Perform the Hazard Evaluation (PHA) Required for Non-Routine Modes of Operation (Startup, Shutdown, Online Maintenance)," W. Bridges and T. Clark, *7th Global Congress on Process Safety*, Chicago, AIChE, March 2011.
24. Bridges, W.G., et. al., "Addressing Human Error During Process Hazard Analyses," *Chemical Engineering Progress*, May 1994
25. Rasmussen, B. "Chemical Process Hazard Identification," *Reliability Engineering and System Safety*, Vol. 24, Elsevier Science Publishers Ltd., Great Britain, 1989.
26. "Effectively Addressing New PSM/RMP Damage Mechanism Review Requirements with an Integrated PHA (iPHA)," Nour, Maher, Schutz, all from Risk Management Professionals, 11th GCPS, *April 2015.*
27. Wall Street Journal, January 29, 2011.
28. Gertman, D.; Blackman, H.; Marble, J.; Byers, J. and Smith, C., "The SPAR-H Human Reliability Analysis Method," NUREG/CR-6883, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington, DC, August 2005.
29. Swain, A. D., Guttmann, H. E., "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Final Report," NUREG/CR-1278, 1983, US Nuclear Regulatory Commission.