Best Practices for Addressing Human Factors during PHAs/HAZOPs
… Especially during PHA of Non-normal Modes of Operation (Startup, Shutdown, & Online Maintenance)

By: William Bridges
Process Improvement Institute, Inc. (PII)
1321 Waterside Lane, Knoxville, TN 37922 USA
wbridges@piii.com

By: Rashed Al-Zahrani
UNITED, a SABIC affiliate
ZahraniRA2@united.sabic.com

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

Best Practices for Addressing Human Factors during PHAs/HAZOPs … Especially during PHA of Non-normal Modes of Operation (Startup, Shutdown, & Online Maintenance)

By: William Bridges
Process Improvement Institute, Inc. (PII)

By: Rashed Al-Zahrani
UNITED, a SABIC affiliate

Keywords: PHA, Human Factors, Process, Hazard Evaluation, HAZOP, Safety, Factors, Human Error, Operations, Maintenance, Hazards, Process Safety, Review, HRA, PSM, Inspection, Programs, Reliability, Ammonia, Emergency, Recommendations, Checklist, FMEA, Instrumentation, Process Hazard Analysis, Risk Management, Initial, LOPA, Materials, Relief, P&ID, Risk Assessment, Investigatory, Layer of Protection Analysis, Risk-Based Process Safety, RBPS

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 70% 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.**

Chapter 9 of "Guidelines for Hazard Evaluation" (3rd Ed, CCPS)[1], requires hazard evaluations of all hazards of the process during all modes of operation and it describes the Best Practices for this analysis. 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. US CSB and other agencies have also recognized this weakness in PHAs.

Another key weakness is that most PHAs fail to truly evaluate human factors when brainstorming and analyzing potential accident scenarios. Most PHA leaders are not trained in human factors and most do not know the limits of control we all have on human errors.

This paper describes an approach for integrating human factors considerations into hazard evaluations of process designs, operating procedures, and management systems. In the description of our approach, we cite OSHA's and EPA's definitions for consideration of human factors during PHAs. Critical issues related to human factors can be identified and addressed in different phases of a hazard evaluation. Case studies illustrate the effectiveness of this strategy. This paper also explains the business case for doing PHAs of procedure steps for non-routine modes of operation, while also describing the growing regulatory pressure from US OSHA and others. The paper recaps the practical ways to efficiently and thoroughly analyze the step-by-step procedures that are used to control non-routine operating modes, as well as those for batch and between batch operations.

INTRODUCTION

Human error in research, design, construction, installation, operation, maintenance, manufacturing, inspection, management, etc., can be considered the cause of almost all industrial accidents. (Experts typically quote that about 85% of accidents are caused by human error, though some say that except for natural disasters this figure is 100 %.) However, simply attributing these incidents to "human error" without evaluating the root cause implies that the errors are inevitable, unforeseeable, and uncontrollable. Nothing could be further from the truth.

Human errors are sometimes mistakenly called procedural errors. This is not true anymore than saying all equipment errors are due to design errors. People make mistakes for many reasons, but PII estimates that only about 10% of accidents due to human errors in the workplace occur because of *personal* influences, such as emotional state, health, or carelessness; most human error is due to weaknesses in the control of human factors. Over the past five decades of industry research and observation in the workplace on human error, we have come to know that human error probability depends on many factors.

These factors (described in more detail in *Human Factors Missing from PSM* [2]), include those shown below (note that the percentages shown below were developed by PII after analysis of more than 15,000 process safety, safety, and operational incidents):

- Procedure accuracy and clarity (the number one, most cited root cause of accidents):
    - A procedure typically needs to be 95% or better accuracy to help reduce human error; humans tend to compensate for the remaining 5% inaccuracies in a written procedure.
    - A procedure must clearly convey the information (there are about 25 rules for structuring procedures to accomplish this) and the procedure should be convenient to use.
    - Checklist features – These should be used and enforced either in the procedure or in a supplemental document.

- Training, knowledge, and skills
    - Employees should be selected with the necessary skills before being hired or assigned to a department.
    - Initial Training – There must be effective training. The initial training should be demonstration-based training on each proactive task and each reactive (e.g., response to alarm) task.
    - Ongoing validation of human action is needed and usually should be repeated (in either actual performance or in drills/practice) at least once per year *(*as discussed later in this paper). For human IPLs or safeguards, the action should be demonstrated to be "fast enough" as well.
    - Documentation – the human performance should be documented and retained to demonstrate the error rates chosen are valid.

- Fitness for Duty – Includes control of many sub-factors such as fatigue (a factor in a great many accidents), stress, illness and medications, and substance abuse.

- Workload management – Too little workload and the employee becomes bored (reducing alertness, increasing distractions), while too much overwhelms the employee (increasing stress, decreasing time per task); both cases can increase human error.

- Communication – Miscommunication (of an instruction or set of instructions or of the status of a process) is the second or third most common cause of human error in the workplace. There are proven management systems for controlling communication errors (such as repeat back, use of common jargon).

- Work environment – Factors to optimize include lighting, noise, temperature, humidity, ventilation, and distractions.

- Human System Interface – Factors to control include layout of equipment, displays, controls and their integration to displays, alarm nature and control of alarm overload, labeling, color-coding, fool-proofing measures, etc.

- Task complexity – Complexity of a task or job is proportional to the (1) number of choices available for making a wrong selection of similar items (such as number of similar switches, number of similar valves, number of similar size and shaped cans), (2) number of parallel tasks that may distract the worker from the task at hand (leading to either an initiating event or failure of a protection layer), (3) number of individuals involved in the task, and (4) judgment or calculation/interpolation, if required. For most chemical process environments, task complexity is typically low (one action per step), but for response actions (human IPLs) there are almost always other tasks underway when the out-of-bounds reading occurs or the alarm is activated.

In addition to the human factors listed, other considerations for use of a human as an IPL include (1) time available to perform the action and (2) physical capability to perform the action safely.

Other papers provide much more detail on each human factor and the relative weighting of each.[2, 3, 4]

These human-error causes (human factors), which in turn result from other human errors, are all directly within management's control. When using human error data for controlling initiating events (IEs) and independent protection layers (IPLs), the site should ensure that the factors above are consistently controlled over the long-term and that they are controlled to the same degree during the mode of operation that the PHA, HAZOP, What-if, FMEA, or LOPA covers. For instance, if workers are fatigued following many extra hours of work in a two week period leading up to restart of a process, then the human error rates can increase by a factor of 10 times or 20 times during startup.[5]

Although this paper focuses on the requirements of a PHA (a redo or new hazard evaluation of an entire process), the approach is equally effective for other hazard evaluations such as preliminary and detailed design reviews (for new/revised processes) and large management of change hazard reviews.

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"[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. 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, US regulators are beginning to increase pressure on regulated companies to perform PHA's 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)[6]. 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.*[6]

  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.[7] **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[8] 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.

- **Paragraph (e) of the US OSHA regulation on PSM, 29 CFR 1910.119,[9] and similar requirements in US EPA's rule for risk management programs (RMP), 40 CFR 68.24,[10]** 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).[11]** 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.

- **US OSHA published an internal document on Program Quality Verification of Process Hazard Analysis in 1993 (by Henry Woodcock, of OSHA).**[12] 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)**[13] – 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.

- **Recent US OSHA PSM National Emphasis Programs** for Chemical Processes[14] and also for Refineries[15] 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*[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 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*.[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[16] on 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.

US EPA's RMP Regulation

In the Risk Management Program rule (40 CFR 68.24)[10] 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.[17])*

Example of Local Regulation: Contra Costa County Hazard Materials Program

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)[18] 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 CalOSHA's proposed rule for refineries). The 2008 update to the book *Guidelines for Hazard Evaluation Procedures*[1] 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.

Approach for Fully Addressing Human Factors in Hazard Evaluations - 4 Steps

To fully address human factors during PHA/HAZOP, a four-step approach is suggested.

- Step 1: Ensure education and experience of PHA/HAZOP Leaders in human factors and human error prevention. Also ensure the PHA/HAZOP Leaders are competent in PHA of procedures (which is very different than PHA of equipment nodes)
- Step 2: Ensure the brainstorming of scenarios includes consideration of human error and even multiple human error as causes; be specific as possible on the human error.
- Step 3: Have the PHA team perform a hazard review of procedure steps using a HAZOP or What-If analysis to uncover potential human errors associated with modes operations such as startup, shutdown, and online maintenance.
- Step 4: Supplement the PHA/HAZOP of the individual scenarios with a checklist analysis of general human factor issues, to ensure all major categories were addressed.

STEP 1 - Ensuring PHA/HAZOP Leaders are Competent in Human Factors and PHA of Procedures

The PHA Leader's understanding of human factors and human error prevention (HEP) will be the most significant indicator in whether the PHA will be successful in identifying the hazards

caused by human error (the team will not be equipped to do this on their own, especially for scenarios that have not yet occurred). This understanding required of the PHA Leader is not a given trait that all leaders share (though it should at least be covered partially as part of PHA Leadership Training), it is a unique skill set that must be developed deliberately by the Leader, specifically by completing focused courses in human factors/human error prevention, participating in coaching by mentor/senior PHA Leaders, and studying the relevant statistics regarding human factors and human errors in industry. This training, along with several years in operation or safety roles to provide experience, will give the leader the ability to quickly recognize potential human factors (human error modifiers such as high fatigue or miscommunication) in the modes of operation being analyzed, and will provide the necessary tools to systematically brainstorm with the team in a way that maximizes hazard identification and meeting effectiveness. A large portion of these human error related hazards can only be identified with analysis of procedure steps (PHA of procedures, as part of the non-normal/non-continuous modes of operation), so the leader must be adept in techniques required for such analysis, including methods such as What If or 2 or 7 Guideword brainstorming of procedure step deviations, and the rules for analyzing and documenting procedure deviations and safeguards listed, discussed below in *STEP 3*.

STEP 2 - Ensuring PHA/HAZOP Leaders Look for and Find Human Error Causes during Routine and Non-routine modes of Operation

The training discussed above in human factors and human error prevention is mostly wasted if it is not applied to non-routine modes of operation (normal modes of operation generally are less dependent on human error). Many companies have not learned the basic truth that accidents that can occur during startup, shutdown, and online maintenance have little to do with accidents that occur during continuous more of operation. In fact, safeguards that adequately protect against accidents in normal mode, are of little or use for some scenarios that are unique to these non-routine modes of operation. Finding the unique safeguards necessary for the each mode of operation is critical. In addition to standard brainstorming of step deviations, the leaders and scribes most look for multiple simultaneous causes of an accident scenario (double jeopardy). This may seem like a conflict with traditional HAZOP rules, but in fact, there has never been an official rule against consideration of double jeopardy, though there has been recognition that none of the qualitative PHA methods are thorough in finding ALL double-jeopardy scenarios. But during PHA of steps of procedures, it is fairly common for a double jeopardy to occur.

Therefore, the **company MUST require PHA of all modes of operation, and the analysis must be done the right way (as described in this paper).** This must be in a standard that is enforced by the company. At a minimum, the standard must:

1. Ensure the PHA Leaders are trained (Step 1) in the methods that best suit those modes of operation (like those in Steps 3 and 4), providing all procedures and related materials they will require (and ensuring that these materials are accurate and up to date), and that

the PHA team includes the necessary expertise (experienced operators, senior operators/trainers as needed, etc.).

2. Ensure that the right methods are in fact used for leading and documenting the PHA of non-routine modes:
    a. This includes auditing the PHA meeting, as it is in progress, to ensure PHA is complying with Steps 3 and 4.
    b. Auditing the PHA report to ensure completion of the analysis per Step 3 and 4. Was there a PHA of steps? Were the right methods used? Is there evidence of unique safeguards being found for unique scenarios for each mode of operation? Is the evidence of discussion of double-jeopardy scenarios?

STEP 3: PHA of Non-Continuous Modes of Operation

During the period 1970 to 1989, 60% to 75% of major accidents in continuous processes occurred during non-routine modes of operation (principally startup and online maintenance modes).[19] This trend has continued unabated for most of the process industry to the present day. A compilation of 47 major process safety accidents from 1987 to 2010 was provided in an earlier paper on this topic (Bridges, et al) [20]; of these, 69% occurred during non-routine operations. In addition, a poll of over 50 clients indicates that 70% of their moderate and major accidents occurred during non-routine modes of operation. This data is particularly disturbing when factoring in the time at risk, since most continuous processes are typically shut down 5% or less per year. Therefore, for many continuous processes the workers and other stakeholders are 30 to 50 times more likely to have a major accident during the time frame of startup, shutdown, or on-line maintenance modes of operation.

One reason for processes being at higher risk during these operating modes is many of the safeguards (independent protection layers; 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 four decades of 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.

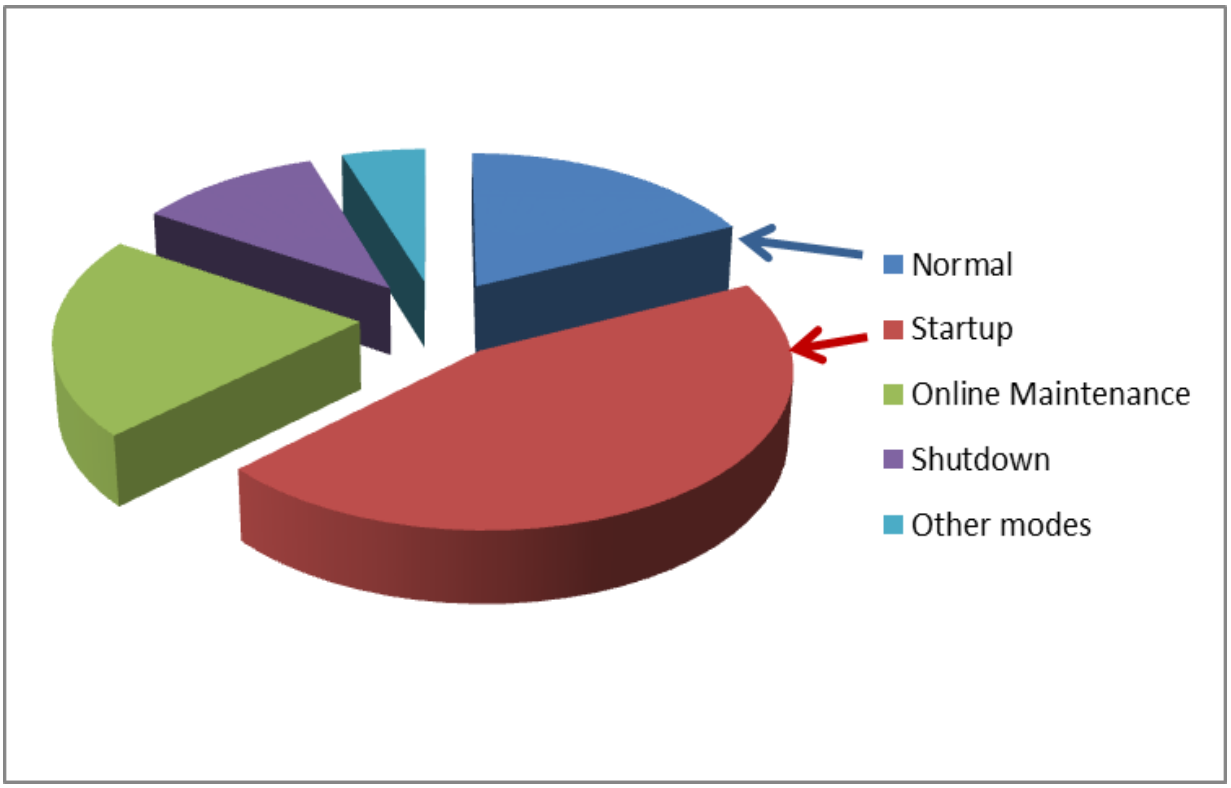


Figure 1: Distribution by Operating Mode of the 47 Largest Process Safety Accidents between 1987 and 2010[20]

How does someone responsible for coordinating or performing hazard evaluations (including PHAs) uncover potentially important accident scenarios during all modes of operation without consuming too many resources? To correctly answer this question, we must (1) understand the root causes of human error and (2) develop a strategy for systematically finding the scenarios that are caused by human error, during all modes of operation. The strategy must be thorough, yet provide for a practical allocation of resources. This paper provides a strategy that uses widely accepted hazard evaluation techniques (such as those referenced by OSHA and EPA for PHAs, which include what-if analysis and hazard and operability [HAZOP] analysis). This strategy has proven effective for hundreds of facilities over the past two decades since it was first published.[21] In addition to identifying accident scenarios during non-routine modes; this approach helps to more fully address human factors, which is a specific requirement of OSHA's PSM regulations and EPA's RMP rule.

Human factor deficiencies can make operations during non-routine modes extremely hazardous – since operators generally have less operating experience for non-routine modes, and these types of operations rely heavily on operator decision-making and tasks. In addition, there are usually less layers of protection in effect during non-routine operations. Analyzing procedure steps can identify steps where the operator is most likely to make mistakes and suggest ways to reduce risk

of an accident scenario, ranging from adding hardware to improving management systems.

The approach outlined in this work applies equally to any hazard evaluation where the steps for a non-routine mode of operation are well defined (i.e., written), including PHAs of existing units, hazard evaluations during preliminary and detailed design phases of projects (for new/revised processes), and large or small management-of-change hazard reviews.

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. As mentioned earlier, 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 objective for the hazard evaluation team is to evaluate the risk associated with skipping steps and performing steps incorrectly.

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[21] and also 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.

As with scenarios uncovered during continuous modes of operation, the company may need to perform analysis (including semi-quantitative analysis such as LOPA or HRA) to more fully address any unresolved or complex issues raised in the hazard evaluation of non-routine modes of operation.

Case studies presented later in this paper illustrate the analysis approach and the usefulness of this strategy.

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; a PHA of procedural step deviations would likely find this deficiency, but a JSA will miss this process safety issue. 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)).[9]

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 considering 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).[5]

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, 21, 22, 23] 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.

> ***Example:*** *For the BP Texas City, Texas refinery, pre-2005, if the isomerization unit had a hazard analysis of the startup mode (using What-If and 2-Guide Word analysis [explained later in this work]), the team would have likely identified that the high-high level switch in the column was a critical safety device. They also may have recommended moving the switch to a location higher in the column and then interlocking the high-high level switch to shutdown feed to the column. However, the site performed a parametric deviation HAZOP of the equipment nodes which focusing on continuous mode of operation, and so the team decided that the high-high level switch was not critical since devices in upstream and downstream process units (during continuous operation) would indicate possible level problems in the column – and besides, the operator would certainly notice the high-level condition on the sight glass during the rounds twice per shift. Unfortunately, these are not necessarily safeguards during startup of the column (1) since the routine practice was to overfill the bottoms (raise the level above the upper tap of the level controllers transmitter and above the nozzle for the high-high level switch and (2) since swings in upstream and downstream units are expected (and so likely such swings would not have led to intervention by the operators of the other units).*

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)[24]. 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. (We will discuss the usefulness of this simple approach to hazard evaluation of steps 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."[21]

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 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."

Table 1: Definitions of 7-8 Guide Words for HAZOP of Procedure-Based Operations

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.

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.[6]

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 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 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.

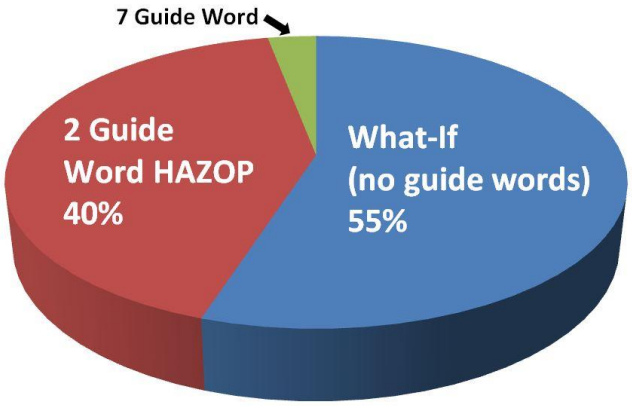


Figure 2. Relative Usage of Techniques for Analysis of Procedure-Based Modes of Operation

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 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 Figures 3A and 3 B below:

Figure 3A: PHA of a ALL Modes of Operation for a CONTINUOUS Process

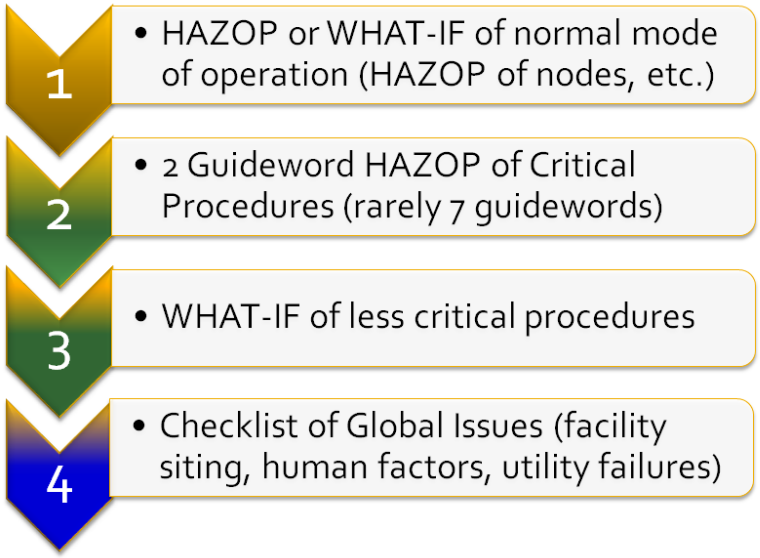
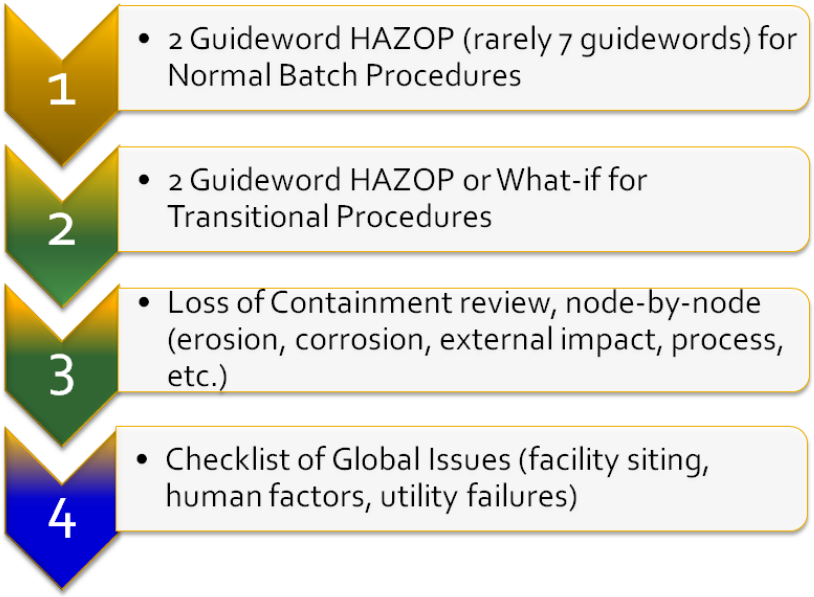


Figure 3B: PHA of a ALL Modes of Operation for a BATCH Process



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.

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)][9]. 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.

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[25]), 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 60-75% of catastrophic accidents occur during non-routine modes of operation. 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.

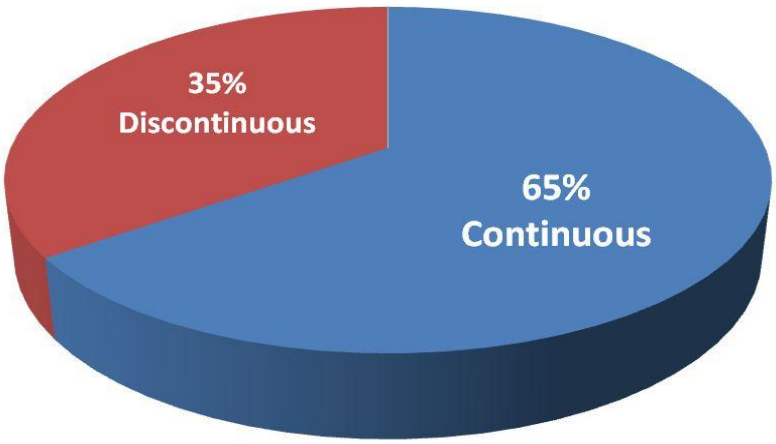


Figure 4. Relative Amount of Meeting Time Spent for Analysis of Routine and Non-routine Modes of Operation for a Continuous Process

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 re-write the procedures first!**

STEP 4 - Using Checklist analysis to Help Ensure Thorough Coverage of All Human Factors

A general, template based Human Factors checklist questionnaire should be included in the scope of any large, unit-sized PHA to help ensure generic human factors are thoroughly considered. These checklists are available in the default templates of some PHA documentation

software, such as LEADER ™ (from ABS Consulting). Even if not specifically called out in the PHA scope, it's worth going through template checklists during the last few hours of a meeting. If possible, the more efficient strategy is to send the checklists to team members a month or so before the meeting, so the team can go over the questionnaire, walk down the items on the checklists in the field (with an operator or other PHA team member, if possible), and then submit their responses to the PHA Leader prior to the meeting. Then, on the last day of the meetings, then Leader/Scribe reviews the consolidated list of issues found by the team members. This saves meeting time and allows for more in-depth consideration of the listed issues. (Note that generic checklists for Human Factors and Facility Siting are often completed together; and though the items listed on the siting checklist are not categorized directly as human factors, they include design considerations that may have been overlooked during the project/initial PHAs that can in turn lead to more human error.). Adding the Human Factors checklists to the analysis scope typically identifies more minor to moderate consequences (compared to those found in HAZOP of procedure steps or in HAZOP of normal mode of operation), and will generally yield far fewer recommendations (typically only 1-5% of the total recommendations come from use of the checklists). However, given the almost negligible additional costs to include the checklists in the analyses scope, the benefit from catching the last few hazards that might have slipped through the cracks otherwise will always justify such costs.

For an example, see the human factors checklist listed in ***Exhibit A.***

CASE STUDIES

PII and others have performed tens of thousands of PHAs, including many thousands of PHAs of all modes of operation. Everyone who applies the lessons above find hundreds to thousands of scenarios that are unique to startup, shutdown, and online maintenance. For example:

> *Results from thousands of PHAs of non-routine modes of operation indicates that about 3% to 6% of the relief valves across the industry have been discovered to be too small and so had to be resized to account for accident scenarios that were only found during analysis of non-routine modes of operation.*

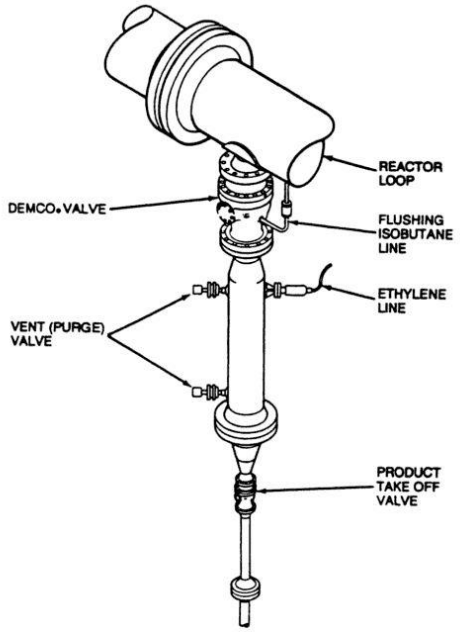
The following case studies illustrate the usefulness of the process outlined in this paper.

Case Study 1: Phillips Polyethylene Plant 6, Pasadena, TX

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. 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 team varied in size, but always included at least two operators. The team leader was a process engineer with 15 years of experience, who was also trained in human factors. The PHA first covered the continuous mode of operation for the approximately 200 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.

Figure 5: Typical Settling Leg Assembly for Phillips Polyethylene



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 3.5 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.

After the PHA was completed, the settlement agreement also required a quantified human reliability analysis (HRA) of the online maintenance task of clearing a plugged settling leg – mistakes during this task led to the accident in 1989. The HRA was performed similar to those performed for nuclear reactor risk assessments, using a human reliability event tree to model the error probability for the task. The HRA results indicated that if the three IPLs in the new design

are maintained, the probability of a similar event occurring when using this procedure was less than the risk of fatality when driving to work. This report was also approved by OSHA for settlement purposes.

The HRA shed light on new aspects of making errors and recovering from the errors during this task, but the HRA results did not result in changes to the process steps (at least not much), or the training program, or the human factors engineering, or the hardware/IPLs.

In this instance, the HRA validated the results of the 7 Guide Word HAZOP, but did not make new recommendations. The HAZOP of the procedures had already found the major accident scenarios and had already identified well enough the changes needed to reach tolerable risk.

Case Study 2: HUNTSMAN

Qualitative analyses 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. Huntsman recognizes that regulators have required similar approaches for decades and that the regulators continue to note lack of analysis of the risk of non-routine operations and lack of risk review of changes to procedures.

The Huntsman Geismar site implementation of PHA of non-routine modes of operation in conjunction with the traditional PHA creates a complete process hazard analysis of all modes of operation. Using PHA of non-routine modes of operation, Site teams have already identified hazardous scenarios that exist only during startup that were not identified by the traditional PHA approach. Teams have also identified existing safeguards and potential new layers of protection to prevent the newly identified hazardous scenarios from occurring. The site has already installed inherently safer designs identified using the new methodology that significantly reduce the risk.

The Geismar site believes our implementation of PHA of non-routine modes of operation is a world class initiative that is necessary to identify all potential hazardous scenarios at our facility.

Case Study 3: UNITED (a SABIC affiliate)

In January 2019, PII completed a ‘Re-do’ PHA of the UNITED Ethylene Plant (Jubail, Saudi Arabia; a SABIC affiliate), 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.[26]

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 hazard 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, but have some impact to communication or effective operation). 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.

> *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.

These hazards, many of which had NO safegaurds in place, would have been missed if the PHA scope failed to include procedure/non-normal modes of operation, which worth noting as statistically it is these types of errors/failures that lead to the majority of catastrophic consequences (non-normal modes of operation are when 80% of major accidents occur, as discussed previously). UNITED sees that the PHA of Procedures added extreme value to their current high value PHAs; and fully complies with corporate standards. As mentioned elsewhere, accurate procedures are needed to support a good PHA of procedures.

In summary, the PHA of procedures yeilded great benefit to UNITED by finding dozens of dangerous scenarios that were not found during PHA of normal mode of operation.

Another perhaps equally important aspect of human factors that was looked at carefully during the PHA was the fact that certain scenarios required more robust human intervention, esepcially when responding to some process alarms. These alarms are named "Critical Alarms" and directly trigger a Human Response IPL. These critical alarms required more attentive approach, where failure to respond adequately could results in severe consequences. Therefore, and in order to address the concerns of human errors that were specifically outlined in the work of Tew and Bridges (2010)[16], a common recommendation was made to UNITED to look at all alarms that are titled "critical" during the PHA study, and ensure that Training, Knowledge, and Skills are properly managed for these. For such Human Response IPLs, the pertinent operators must be provided a written trouble-shooting guide and each operator must be specifically trained for how to respond in time to each individual critical alarm. Moreover, response to these critical alarms must be tested and evaluated to ensure effectiveness of the Human Response IPL, and the time to respond (TTR) must be less than the safe span of time (within the Process Safety Time [PST]), based on simulated scenarios.

Another key human factor aspect covered in our PHA related to reducing specific human errors in the inspection and maintenance of Safety Instrumented Systems (SIS), which is a relatively new concept, largely introduced and proved by the work of Bridges and Thomas (2012)[28], and as it becomes increasingly important to maintain robust and effective high Safety Integrity Levels (high SILs). The PHA team closely looked at the concern of a possible increase in the likelihood of human error affecting the SIF's Probability of Failure on Demand (PFD). As a result, a recommendation was written for all of UNITED to consider maintenance staggering concept as a method to minimize the systematic probability of human error during proof testing and inspection. In essence, if a SIF has multiple channels (such as multiple sensors) that are voted 1oo2 or 1oo3, etc., then if the same person performs the calibration check of each channel, then the person should have 3 days separation between Channel 1 calibation and Channel 2, and similarly for Channel 3; otherwise the probability of repeating a failure on the 2nd and 3rd channel is about 90%. This is indeed an important consideration that needs to be always looked at when discussing human factors.

Case Study 4: SINOPEC-SABIC Tianjin Petrochemical Company (SSTPC)

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

PII led the PHA of the units, for all modes of operation. 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.

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[87] 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."[27]*
>
> ***From CSB Report on August 2008 Bayer CropScience Explosion:[16]*** *"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."*

More regulatory pressure is sure to follow, since major accidents continue to occur during non-routine modes of operation.

Regardless of what hazard evaluation technique is employed, it is imperative for PHA teams to ask, "Why would someone make this mistake?" whenever a human error is identified as a cause of a potential accident. "To err is human" may be a true statement, but the frequency and consequences of such errors can be effectively reduced with a well-designed strategy for analyzing risk of non-routine operating modes.

Most critically, such analyses make it easier to provide a thorough consideration of human factors.

References

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

2. Tew, R. and Bridges, W., "Human Factors Missing from PSM," *Loss Prevention Symposium (part of the Global Congress on Process Safety [GCPS]),* AIChE, March, 2010.

3. "The SPAR-H Human Reliability Analysis Method," NUREG/CR-6883, U.S. Nuclear Regulatory Commission, prepared by Gertman, D.; Blackman, H.; Marble, J.; Byers, J. and Smith, C., of the Office of Nuclear Regulatory Research, Washington, DC, August 2005.

4. "Human Event Repository and Analysis (HERA)," NUREG/CR-6903, U.S. Nuclear Regulatory Commission, prepared by B. Hallbert, A. Whaley, R. Boring, P. McCabe, and Y. Chang, 2007.

5. Bridges, William G. and Collazo-Ramos, Dr. Ginette. "Human Factors and Their Optimization." *8th Global Congress for Process Safety Proceeding (GCPS).* American Institute of Chemical Engineers (AIChE), 2012.

6. 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.

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

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

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

10. "Risk Management Programs for Chemical Accidental Release Prevention," US EPA Final Rule, 40 CFR 68, 1994-2000.

11. OSHA Inspection Number 103490306, Issued November 2, 1992.

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

13. OSHA Inspection Number 123807828; Issued November 18, 1993.

14. 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.

15. 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.

16. "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.

17. *EPA RMP Guidance, Chapter 7, pgs 7-6 & 7-7; General Risk Management Program Guidance.*

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

19. Rasmussen, B. "Chemical Process Hazard Identification," *Reliability Engineering and System Safety*, Vol. 24, Elsevier Science Publishers Ltd., Great Britain, 1989.

20. Bridges, W. and Clark, T., *"*How to Efficiently Perform the Hazard Evaluation (PHA) Required for Non-Routine Modes of Operation (Startup, Shutdown, Online Maintenance)," *7th Global Congress on Process Safety [GCPS]),* AIChE, March, 2011.

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

22. Hammer, W., "Occupational Safety Management and Engineering, 3rd Ed.," Prentice Hall, 1985.

23. Kongso, H.E., "Application of a Guide to Analysis of Occupational Hazards in the Danish Iron and Chemical Industry," *International Conference on Hazard Identification and Risk Analysis, Human Factors and Human Reliability in Process Safety*, Center for Chemical Process Safety, AIChE, New York, 1992.

24. S. Mannan, ed., *Lees' Loss Prevention in the Process Industries, 4th Ed.*, Elsevier Butterworth-Heinemann, ISBN 978-0-12-397189-0, Oxford, UK, 2012.

25. 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.

26. *SHEM 02.01 Process Safety Risk Assessment, EHS-PRC-SM-002.01-07,* Rev 08, April, 2018, by SABIC

27. W. Bridges and H. Thomas, "Accounting for Human Error Probablity in SIL Verification Calculations" 8th *Global Congress on Process Safety*, AIChE, Houston, 2012

28. *Wall Street Journal*, January 29, 2011.

Exhibit A - The latest Human Factors Checklist

Company:	**Plant:**	**Site:**	**Unit:**	**System:**
Method: Checklist	**Type:** Human Factors Checklist	**Team Members:**		

Item	Topic	Questions/Issues	Responses	Recommendations
1.1	Housekeeping and General Work Environment	Are adequate signs posted near maintenance, cleanup, or staging areas to warn workers of special or unique hazards associated with the areas? Are adequate barriers erected to limit access to maintenance, cleanup, or staging areas? Are working areas generally clean? Are provisions in place to limit the time a worker spends in an extremely hot or cold area? Is noise maintained at a tolerable level? Are alarms audible above background noise both inside the control room and in the process area? Are normal and emergency lighting sufficient for all area operations? Is there adequate backup power for emergency lighting? Is the general environment conducive to safe job performance?		
1.2	Accessibility/ Availability of Controls and Equipment	Are adequate supplies of protective gear readily available for routine and emergency use? Are workers able to perform both routine and emergency tasks safely while wearing protective equipment? Is emergency equipment accessible without presenting further hazards to personnel? Is communications equipment adequate and easily accessible? Would others quickly know if a worker is incapacitated in a process area? Are the right tools (including special tools) available and used when needed? Is the workplace arranged so that workers can maintain a good working posture while performing necessary movements to conduct routine tasks? Is access to all controls adequate? Can operators/maintenance workers safely perform all required routine/emergency actions, considering the physical arrangement of equipment (e.g., access to equipment, or proximity of tasks to rotating equipment, hot surfaces, and hazardous discharge points)? Are valves that require urgent manual adjustments (e.g., emergency shutdown) easily identifiable and readily accessible?		
1.3	Labeling	Is all important equipment (vessels, pipes, valves, instruments, controls, etc.) legibly, accurately, and unambiguously labeled? Does the labeling program include components (e.g., small valves) that are mentioned in		

Item	Topic	Questions/Issues	Responses	Recommendations
		the procedures even if they are not assigned an equipment number? Has responsibility for maintaining and updating labels been assigned? Are emergency exit and response signs (including wind socks) adequately visible and easily understood? Are signs that warn workers of hazardous materials or conditions adequately visible and easily understood?		
1.4	Feedback/ Displays	Is adequate information about normal and upset process conditions clearly displayed in the control room? Are the controls and displays arranged logically to match operators' expectations? Are the displays adequately visible from all relevant working positions? Do separate displays present similar information in a consistent manner? Are automatic safety features provided when a process upset requires rapid response? Are automatic safety features provided when a process upset may be difficult to diagnose due to complicated processing of various information? Are the alarms displayed by priority? Are critical safety alarms easily distinguishable from control alarms? Is an alarm summary permanently on display? Are nuisance alarms corrected and redundant alarms eliminated as soon as practical to help prevent complacency toward alarms? Have charts, tables, or graphs been provided (or programmed into the computer) to reduce the need for operators to perform calculations as part of the operation? If operators are required to perform calculations, are critical calculations independently checked? Does the computer check that values entered by operators are within a valid range? Do the displays provide an adequate view of the entire process as well as essential details of individual systems? Do the displays give adequate feedback for all operational actions? Are instruments, displays, and controls promptly repaired after a malfunction? Do administrative features exist that govern when instruments, displays, or controls are deliberately disabled or bypassed and that govern their return to normal service at the appropriate time? Does a formal mechanism exist for correcting human factors deficiencies identified by the operators (e.g., modifications to the displays, controls, or equipment to better meet operators' needs)?		
1.5	Controls	Is the layout of the consoles logical, consistent, and effective? Are the controls distinguishable, accessible, and easy to use? Do all controls meet standard expectations (color, direction of movement, etc.)?		

Item	Topic	Questions/Issues	Responses	Recommendations
		Do the control panel layouts reflect the functional aspects of the process or equipment? Does the control arrangement logically follow the normal sequence of operation? Can operators safely intervene in computer-controlled processes? Can process variables be adequately controlled with the existing equipment? Do operators believe that the control logic and interlocks are adequate? Does a dedicated emergency shutdown panel exist? If so, is it in an appropriate location?		
1.6	Workload and Stress Factors	Is the control room always occupied (i.e., assigned duties do not require the control room operator to be absent from the control room)? Are the number and frequency of manual adjustments required during normal and emergency operations limited so that operators can make the adjustments without a significant chance of mistakes as a result of overwork or stress? Is the number of manual adjustments during normal operations sufficient to avoid mistakes as a result of boredom? Have the effects of shift duration and rotation been considered in establishing workloads? Is the number of extra hours an operator must work if his or her relief fails to show up sufficiently limited so that worker safety is not adversely affected? Is the number of hours an operator or maintenance worker must work during startup or turnarounds sufficiently limited so that worker safety is not adversely affected? Can additional operators (e.g., from other areas or from off site) be called in quickly to help during an emergency? Is the staffing level appropriate for all modes of operation (normal, emergency, etc.)?		
1.7	Procedures	Do written procedures exist for all operating phases (i.e., normal operations, temporary operations, emergency shutdown, emergency operation, normal shutdown, and startup following a turnaround or after an emergency shutdown)? Are safe operating limits documented, providing consequences of deviating from limits and actions to take when deviations occur? Are procedures current (i.e., are they revised when changes occur)? Do operators believe that the procedure format and language are easy to follow and understand? Are the procedures accurate (i.e., do they reflect the way in which the work is actually performed)? Is responsibility assigned for updating the procedures, distributing revisions of the procedures, and ensuring that workers are using current revisions of the procedures? Are temporary notes or instructions incorporated into revisions of written operating procedures as soon as practical? Do procedures address the personal protective equipment required when performing routine and/or nonroutine tasks?		

Item	Topic	Questions/Issues	Responses	Recommendations
1.8	Training (Employees and Contractors)	Are new employees trained in the hazards of the processes? Do operators and maintenance workers receive adequate training in safely performing their assigned tasks before they are allowed to work without direct supervision? Does operator and maintenance worker training include training in appropriate emergency response? Do operators practice emergency response while wearing emergency protective equipment? Do operators practice emergency response during extreme environmental conditions (e.g., at night or when it is very cold)? Are periodic emergency drills conducted? Are emergency drills witnessed by observers and critiqued? Does a periodic refresher training program exist? Is special or refresher training provided in preparation for an infrequently performed operation? When changes are made, are workers trained in the new operation, including an explanation of why the change was made and how worker safety can be affected by the change? Are operators and maintenance workers trained to request assistance when they believe they need it to safely perform a task? Are operators and maintenance workers trained to report near misses as part of the incident investigation program? Are operators trained to shut down the process when in doubt about whether it can continue to operate safely?		