Abnormal Modes of Operation – A risk-based focus

Stephen Bridges
Senior Process Engineer
Process Improvement Institute, Inc.
1321 Waterside Lane,
Knoxville, TN 37922 USA
sbridges@piii.com

William Bridges
President
Process Improvement Institute, Inc.
1321 Waterside Lane,
Knoxville, TN 37922 USA
wbridges@piii.com

Prepared for Presentation at
American Institute of Chemical Engineers
2020 Spring Meeting and 16th Global Congress on Process Safety
Houston, TX
March 29 – April 2, 2019

Abnormal Modes of Operation – A risk-based focus

Presenter:
Stephen Bridges
Senior Process Engineer
Process Improvement Institute, Inc.
1321 Waterside Lane,
Knoxville, TN 37922 USA
sbridges@piii.com

Keywords: Human Factors, Systematic Error, Human Error, Operating Procedures, Process Hazard Analysis, PHA, HAZOP, Risk Assessment, Hazard Identification

Abstract

Per PII, US OSHA, and CCPS, at least 70% of major process safety incidents have occurred during abnormal modes of operation. Abnormal modes of operation include startup, shutdown, temporary operations, emergency, and maintenance activities. Yet much of the focus in process safety is during steady-state operation. This paper summarizes the approaches that focus on the control of risk during abnormal modes of operation, including:

- Focusing PHAs on abnormal modes of operation by PHA of procedures using 2 guideword HAZOP and What-If, per Chapter 9 of *Guidelines for Hazard Evaluation Procedures*, 3rd Edition, 2008, CCPS. This paper will recap the approach and list examples of how these approaches were successfully applied. Usually, PHAs find that recommendations for reducing risk during abnormal operations account for 80% of the risk reduction from a PHA overall.
- Learning scenarios that are unique to abnormal modes of operation that help a company understand what can be found, and what PHA teams and investigation & audit teams should focus on.
- Unique remedies (many are IPLs) for scenarios specific to startup, shutdown, and online maintenance. Over the years, a list of typical remedies to accident scenarios unique to abnormal modes of operation have been developed. These have proven value in reducing risk. The paper will list 10 of the most common remedies.
- Optimizing human factors: Since most of the scenarios for abnormal modes of operation start with a human error initiating event, the paper provides a recap of how to optimize each human factor.

Note that the first 3 section of this paper are included for sake of clarity and completeness to those new to the topic of control of human error and the practical limitations of such controls and related remedies. *Readers who are well versed in the fundamentals of human error rates and human factors may wish to skip to Section 4 of the paper.*

1 Introduction to Human Error and Human Factors

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 any more 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 many decades of industry research and observation in the workplace on human error, industry has 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 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 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]

2 Human Error Probability for a Single Execution of a Rule-Based Task

To calculate the probability of human error (P_{HUMi}), the type of tasks must be defined and the baseline error rate for such a task needs to be established. Note that with excellent control of all of the human factors, a company can begin to approach the lower limits that have been observed for human error, but individual, specific human error probabilities may average about P_{HUMi} = 0.01 (which is a relatively large factor in SIL 2 and SIL 3

verification calculations). It is critical to provide detection and correction for specific human errors.

Excellent control of all human factors means a robust design and implementation of management systems for each human factor are achieved with a high level of operational discipline. The first well-researched publication detailing potential lower limits of human error probability was by Alan Swain and H Guttmann (NUREG-1278, 1983)[6] and by others. However, many times, the limits they referenced get used out of context. The lower limits in the NUREG-1278 assume excellent human factors, but such excellent control is rarely, if ever achieved. Additionally, some human errors listed by Swain and others were for a single error under highly controlled conditions, or on a "best day" instead of average error probability or rate over an average year of tasks. In general, Process Improvement Institute (PII) has found it best to use the average error probabilities as discussed in the following section.

2.1 Error Probability for Rule-Based Actions that are Not Time Dependent:

Actions that do not have to be accomplished in a specific time frame to be effective are not time dependent. It should be obvious then that these do not include response to alarms, or similar actions with time limits. Values listed below represent the lower limits for human error rates, assuming excellent control of human factors; these are expressed as the probability of making a mistake on any step:

- 1/100 - process industry; routine tasks performed 1/week to 1/day. This rate assumes excellent control of all human factors. Most places PII visits, the workers and managers and engineers believe this is achievable, but not yet achieved. {Actual data from the Savanah River Site indicated a Miscalibration error probability of 7.0E-3 and a Failure to Restore After Maintenance error probability of 5.1E-3 for an organization with excellent human factors control and data gathering (Table 1[7]). It is noted that these values could be rounded to 1/100. Organizations are cautioned to determine the actual data for human error rates in their own management systems before using human probabilities lower than 1/100.}
- 1/200 - pilots in the airline industry; routine tasks performed multiple times a day with excellent control of human factors. This average has been measured by a few clients in the airline industry, but for obvious reasons they do not like to report this statistic.
- 1/1000 - for a reflex (hard-wired) action, such as either proactive or minor corrective actions while driving a car, or very selective actions each day where your job depends on getting it right each time and where there are error recovery paths (such as clear visual cues) to correct the mistake. *This is about the rate of running a stop sign or stop light, given no one is in front of you at the intersection; the trouble is measuring this error rate, since you would have to recognize (after the fact) that you made the mistake.*

See Bridges and Collazo (GCPS, 2012)[8] for more details on this topic.

2.2 Adjusting the lower limit rates to estimate a baseline rate at a site

As mentioned earlier, the lower limit rates assume excellent control of human factors in the industry mentioned. Note that airline pilots have a lower error rate than what PII has measured in the process industry. This is due, in part, to the much tighter control by the airlines and regulators on factors such as fitness-for-duty (control of fatigue, control of substance abuse, etc.). Excellent control of human factors is not achieved in many organizations; therefore, the human error rates will be higher than the lower limit, perhaps much as much as 20 times higher. Table 1 provides adjustment factors for each human factor. These factors can be used to adjust the lower limit of error rate upward or downward as applicable, but the factors should not be applied independently. For instance, even in the worst situations, we have not seen an error rate for an initiating event or initial maintenance error higher than 1/5, although subsequent steps, given an initial error, can have an error rate approaching 1 due to coupling or dependency.

- 1/5 - highest error rates with poor control of human factors; this high rate is typically due to high fatigue or some other physiological or psychological stress (or combination). This is the upper limit of error rates observed with poor human factors and within the process industry. *The error rates in the Isomerization Unit the day of the accident at BP Texas City Refinery[9] were about this rate. The operators, maintenance staff and supervisors had been working about 30 days straight (no day off) on 12-hour shifts.*

For the examples provided later, this paper ***will use a baseline error rate of 0.02 (1/50) errors per step***, which is about average at the sites PII visited in the past 15 years. This value could be justified based on the fact that most chemical process sites do not control overtime during turnarounds and/or do not have a system for controlling verbal communication using radios and phones. In addition, for critical steps such as re-opening and car-sealing the block valves under a relief valve after the relief valve is returned from maintenance, the error probability is about 0.01 (1/100) to 0.04 (1/15)[10]; plus, the average probability of being in a "fail to function" state at time zero for a relief device is between 0.01 (1/100) and 0.02 (1/50)[11, 12, 13] (Bukowski, 2007-2009). Both of these tasks have multiple checks and have procedures (similar to what is done when servicing a SIF and when using bypasses for an SIF) and yet the observed human error probability remains between 0.01 and 0.02.

Table 1. SUMMARY TABLE of 10 HUMAN FACTOR CATEGORIES

Based in part on: Gertman, D.; et. al., *The SPAR-H Human Reliability Analysis Method*, NUREG/CR-6883, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington, DC, August 2005[14]. PII has modified the list slightly to account for general industry data and terminology and to incorporate PII internal data.

Human Factor Category	Human Factor Issue/Level	Multiplier for Cognitive & Diagnosis Errors
Available Time (includes staffing Issues) – ***for responses only***	Inadequate time Barely adequate time (≈2/3 x nominal) Nominal time (1x what is expected) Extra time (at least 2x nominal and >20 min) Expansive time (> 4 x nominal and > 20 min)	P(failure)=100% 10 1 0.1 0.01
Stress/Stressors	Extreme (threat stress)	5
(includes staffing issues)	High (time pressures such as during a maintenance outage; issues at home, etc.)	2
	Nominal	1
Complexity & Task Design	Highly complex	5
	Moderately complex (requires more than one staff)	2
	Nominal	1
	Obvious diagnosis	0.2
Experience/Training	Low	10
	Nominal	1
	High	0.5
Procedures	Not available in the field as a reference, but should be	20
	Incomplete; missing this task or these steps	8
	Available and >90% accurate, but does not follow format rules (normal value for process industry)	3
	Good, 95% accurate, follows >90% of format rules	1
	Diagnostic/symptom oriented	1
Human-Machine Interface (includes tools)	Missing/Misleading (violates populational stereotype; including round valve handle is facing away from worker)	20
	Poor or hard to find the right device; in the head calc	10
	Some unclear labels or displays	2
	Good	1
Fitness for Duty	Unfit (high fatigue level (>80 hr/wk or >20 hr/day, no day off in 7-day period; or illness, etc.)	20
	Highly degraded fitness (high fatigue such as >15 hr/day, illness, injury, etc.)	10
	Degraded Fitness (>12 hr day and >72 hr/wk)	5
	Slight fatigue (>8 hr per day; ***normal value for process*** industry)	2
	Nominal	1
Work Processes & Supervision	Poor	2
	Nominal	1
	Good	0.8
Work Environment	Extreme	5
	Good	1
Communication	No communication or system interference/damage	10
	No standard for verbal communication rules ***(normal*** value for process industry)	3
	Well implemented and practiced standard	1

3 Human Error Probability for Multiple Executions of a Rule-Based Task

Coupled (dependent) Error Rates: Coupling represents the probability of repeating an error (or repeating success) on a second identical task, given that an error was made on the first task. The increased probability of failure on subsequent tasks given that an error has already been made is known as dependence. The list below provides some starting point guidance on values to use:

- 1/20 to1/90 - if the same tasks are separated in time and if visual cues are not present to re-enforce the mistake path. This error rate assumes a baseline error rate of 1/100 with excellent human factors. If the baseline error is higher, then this rate will increase as well.
- 1/2 - if the same two tasks are performed back-to-back, and if a mistake is made on the first step of two. This error rate assumes a baseline error of 1/100 with excellent human factors. If the baseline error is higher, then this rate will increase as well.
- 8/10 to 10/10 - if the same three tasks are performed back-to-back and a strong visual cue is present (that is, the worker can clearly see the first devices he/she worked on), if a mistake is made on the first steps of the three.
- Two or more people become the same as one person (with respect to counting of errors from the group), if people are working together for more than three days; this effect is due to the trust that can rapidly build.

These factors are based on the relationships provided in NUREG-1278[6] and the related definitions of weak and strong coupling provided in the training course by Swain (1993)[15] on the same topic, as shown here in Table 2. The following relationship is for errors of omission, such as failing to reopen a root valve or failing to return an SIF to operation, after bypassing the SIF. The qualitative values in Table 2 are based jointly on Swain (1993) and Gertman[14] (SPAR-H, 2005 which is NUREG/CR-6883).

One can readily conclude that staggering of maintenance tasks for different channels of the same SIF or for related SIFs will greatly reduce the level of dependent errors. Unfortunately, most sites PII visits do not stagger the inspection, test, or calibration of redundant channels of the same SIF or of similar SIFs; the reason they cite is the cost of staggering the staff. While there is a perceived short-term higher cost, the answer may be different when lifecycle costs are analyzed.

Simple Rule: Staggering of maintenance can prevent a significant number of human errors in redundant channels. In fact, the US Federal Aviation Administration (FAA) requires staggering of maintenance for aircraft with multiple engines or multiple control systems (i.e., hydraulics) (FAA Advisory Circular 120-42B, as part of ETOPS approval[16]. (ETOPS is Extended-range Twin-engine Operational Performance Standards, a rule which permits twin engine aircraft to fly routes which, at some point, are more than 60 minutes flying time away from the nearest airport suitable for emergency landing.)

Table 2: Guideline for Assessing Dependence for a within-SIF Set of Identical Tasks (based partially on SPAR-H, 2005[14], and partially on field observations by PII)
Courtesy Process Improvement Institute, Inc., All Rights Reserved

Level of Dependence	Same Person	Actions Close in time	Same Visual Frame of Reference (can see end point of prior task)	Worker Required to Write Something for Each Component
Zero (ZD)	No; the similar tasks are performed by different person/group	Either yes or no	Either yes or no	Either yes or no
Zero (ZD)	Yes	No; separated by several days	Either yes or no	Either yes or no
Low (LD)	Yes	Low; the similar tasks are performed on sequential days	No	Yes
Moderate (MD)	Yes	Moderate; the similar tasks are performed more than 4 hours apart	No	No
High (HD)	Yes	Yes; the similar tasks are performed within 2 hours	No	No
Complete (CD)	Yes	Yes; the similar tasks are performed within 2 hours	Yes	Either yes or no

The level of dependency is determined from Table 2 by assessing whether the same person is doing the tasks, the proximity of the actions in time, the proximity of the actions in space (same visual frame of reference), and whether the work is required to make a record for each component:

1. Read down the "Same Person" column and find the applicable row(s), then
2. Read down the "Actions Close in Time" column and find the applicable row,
3. Then check the two columns on the right for that row.
4. The Level of Dependence is shown in the left-most column for the applicable row.

Table 2 has two rows for Zero Dependency (ZD) because ZD can be achieved two different ways:

- Tasks done by different persons or groups (staggered people), or
- Tasks done by same persons or groups, but tasks are done several days apart (staggered times).

Once the level of dependence is known, the probability of either repeat success or repeating errors on identical tasks can be estimated. For these probabilities, we use Table 3, which is a re-typing of Table 20-17 from NUREG-1278[6] (and the similar table in SPAR-H[14] [Gertman, 2005]).

Table 3. Equations for Conditional Probabilities of Human Success or Failure on Task N, given probability of Success (x) or Failure (X) on Task N-1, for Different Levels of Dependence

Level of Dependence	Repeating Success Equations (but shown as error probability)	Repeating Failure Equations
Zero (ZD)	$P_{Success@N} = x$	$P_{Failures@N} = X$
Low (LD)	$P_{Success@N} = (1+19x)/20$	$P_{Failures@N} = (1+19X)/20$
Moderate (MD)	$P_{Success@N} = (1+6x)/7$	$P_{Failures@N} = (1+6X)/7$
High (HD)	$P_{Success@N} = (1+x)/2$	$P_{Failures@N} = (1+X)/2$
Complete (CD)	$P_{Success@N} = 1.0$	$P_{Failures@N} = 1.0$

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

This section is a summary of an earlier paper.[17] 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 mode 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).[18] 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) [19]; 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.

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.[20] 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.

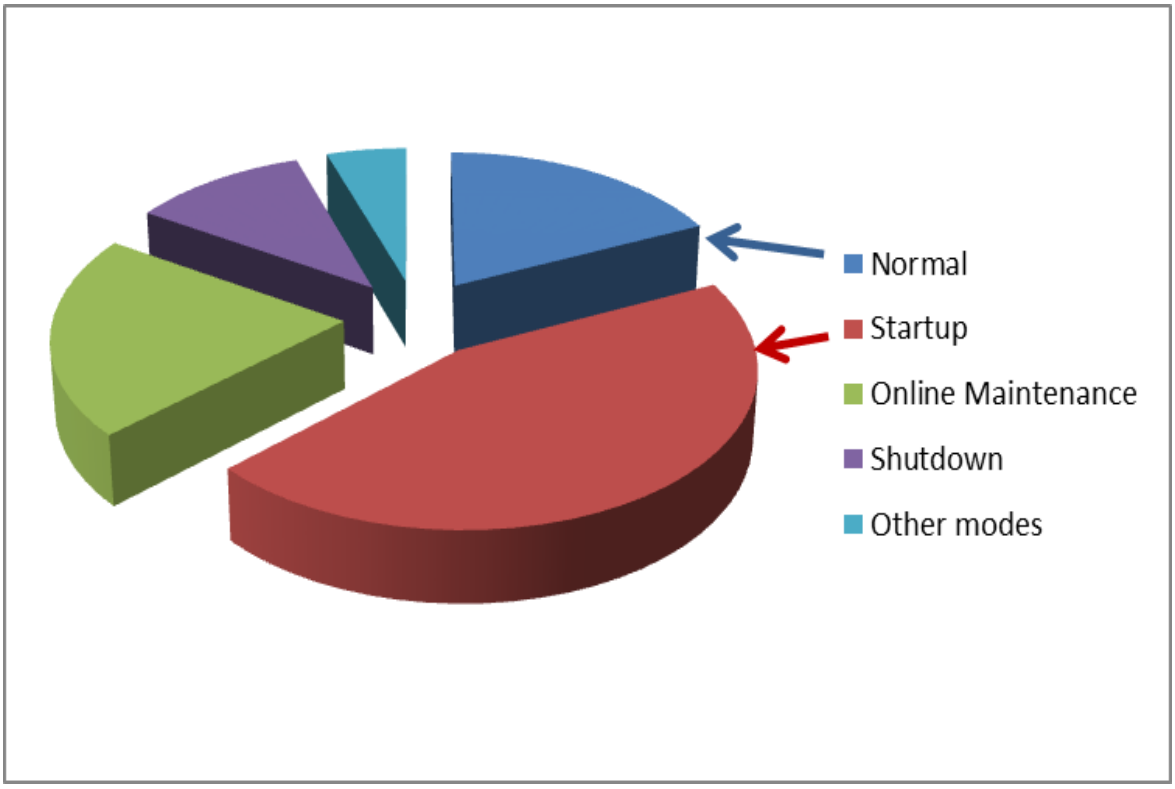


Figure 1: Distribution by Operating Mode of the 47 Largest Process Safety Accidents between 1987 and 2010[19]

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.

Checklist of human factors issues (see an earlier paper[20] 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.

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)).

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.

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 procedure

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).

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."

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.[22]

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.

Table 2: Two Guide Word Approach 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)	

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**
				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.

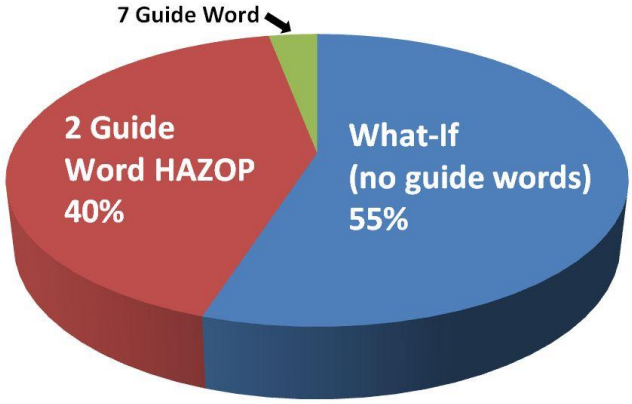


Figure 2. Relative Usage of Techniques for Analysis of Procedure-Based Modes of Operation

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 ALL Modes of Operation for a CONTINUOUS Process

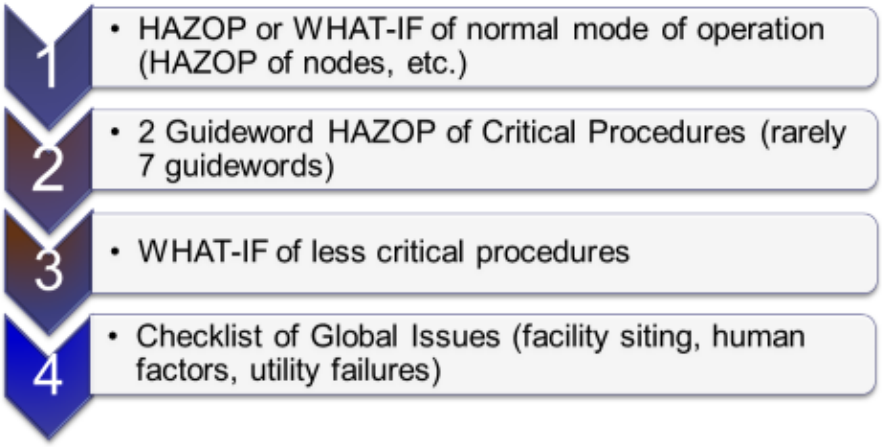
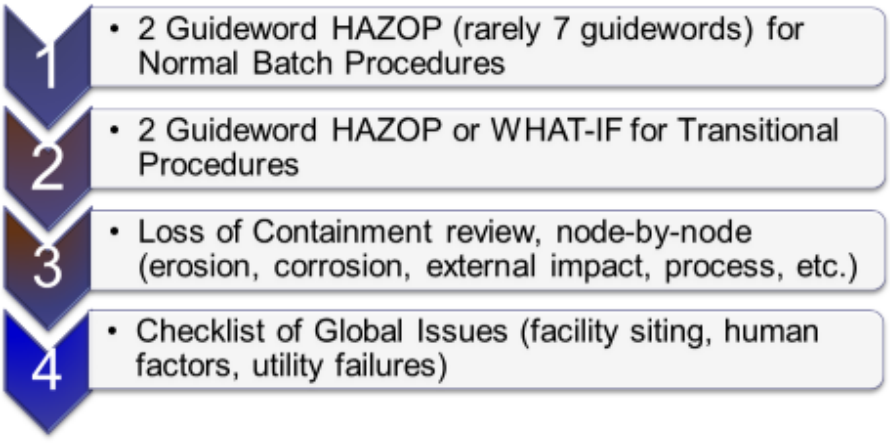


Figure 3B. PHA of ALL Modes of Operation for a BATCH Process



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

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)]. 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.

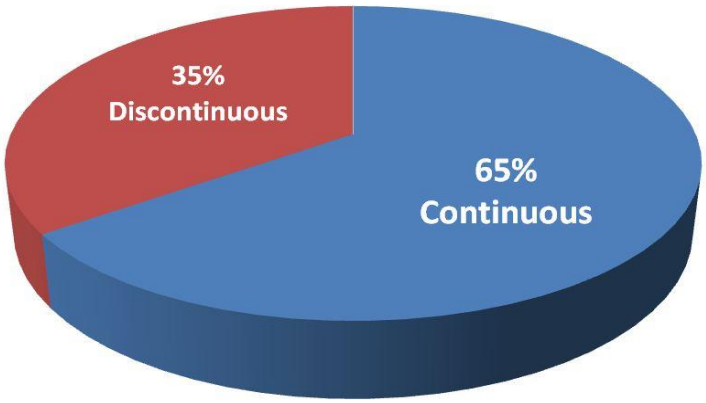


Figure 4. Relative Amount of Meeting Time Spent for Analysis of Routine and Non-routine Modes of Operation for a Continuous Process

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.

5 Best Remedies for Human Error

Once you have optimized human factors as much as possible, then to lower the residual risk further, you will need do something that is independent of the human error and that either helps prevents the error or compensates for the error. Again, **the additional remedies must be independent of the human error initiating event.**

Here are examples remedies that have been proven in use for related scenarios:

- Captive Key. Applied to the valve handle hub. PFD = 0.01. Requires placing one component, such as a valve or door, into an open or closed position before releasing the key needed to move another component into a potentially unsafe position. Can be used to make a sequence of steps for certain tasks difficult or impossible to skip or perform in the wrong order.

    - Examples: PHAs performed by PII recommended adding captive key systems to protect against misalignment during hydrocarbon furnace/reformer decoking, gas drier bed regeneration, to prevent blocking in heat exchangers while heating/cooling media left valved in, to prevent starting compressor with block valve closed downstream/not lined up correctly, to ensure critical pressure relief valves are valved in before starting unit or that manual vent/depressuring valves are closed before off gas line to scrubber can be opened.
    - Special consideration: only captive one person at the site should have access to the machine that produces keys; only this person should be authorized to replace a key; copying of keys should not be tolerated and strictly enforced.

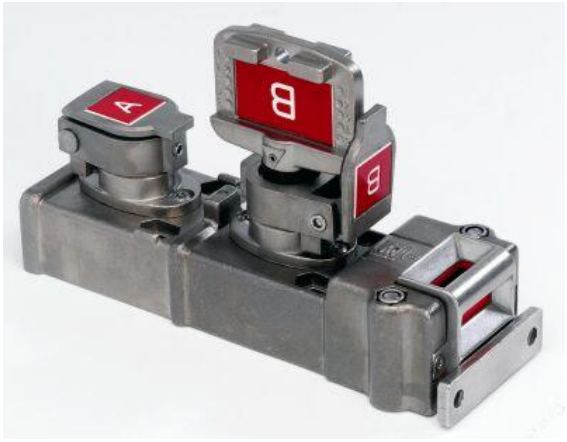


Fig 1. Rockwell captive key lock, prevents opening guard door

- Limit switches on valve position. Ensures that valves are in the correct position, potentially depending on mode or compared to another valve. The concept is similar to captive key, but the control is by limit switches instead. Switch would trigger shutdown or otherwise prevent misalignment. PFD = 0.1 to 0.01, with 0.01requiring strenuous maintenance practices for switches that is not typical in many plants.
    - Typical limit switches are used for many permissives and mode change interlocks. Maintenance practices and control strategies must be well established to bring the probability of jumpering, knifing, or otherwise defeating a limit switch to a very low probability.
    - Some manual valves can be modified to have feedback/indication (though these are harder to keep working); giving ability to verify if systems are isolated from DCS panel.
    - Not as robust as captive key systems.

- Mechanically coupled valves: 2 valves that are hydraulically or pneumatically or mechanically/physically linked. PFD = 0.1 to 0.01, with 0.01 requiring feedback/ indication on both valves.
    - Typically used to ensure that mode switch will be successful, such as when backwashing filters or entering regeneration mode for driers, i.e. preventing only one of two valves from operating.
    - Special consideration: Limit switches still needed to verify position, as these valves are difficult to maintain due to their more complex drive or pneumatic systems (can't operate on output alone)

- Instrumented Permissive. Such as an interlock/permissive to prove the pressure is in the right range before allowing an XV to open. Such as where pressurization with a gas is supposed to be done manually before opening a valve for a cryogenic liquid to enter the system, given that the materials of construction experience brittle fracture potential at the temperature (boiling point) of the flashing liquid. PFD = 0.1 to 0.01, depending on configuration as a SIL 1 or SIL 2 preventative SIF.

Example Recommendation from actual PHA report from step-by-step analysis of the procedure for initial pressurizing of a refrigeration system that is currently constructed from normal carbon steel:

Provide a permissive (RRF of 1000) in the ethylene liquid line to the Ethylene Refrigeration (C2R) system to ensure that the system is pressurized to 12 BarG with ethylene gas before charging the system with liquid ethylene to prevent loss of containment caused by low temperature embrittlement and thermal shock that could release ethylene, potentially leading to fire and possible injury/death. The permissive should be SIL 3 configuration which likely should include 3 pressure sensors (voted 2oo3D) with 2 XVs (voted 1oo2). Otherwise upgrade the metallurgy to stainless steel in order to reach insignificant risk. Upgrading the metallurgy in the entire system will provide a RRF greater than 1000, since the system design would then be inherently safe design. Also consider installing a ramp controller on the ethylene liquid flow control valve to limit thermal shock whenever adding liquid ethylene to the C2R system.

- Hand-held device with bar code reader. To verify the user has been to each device in the right sequence. PFD = 1 to 0.1 but could be stronger if tied back to the BPCS which would then have the computer, not computer operator, watching the activity to confirm a critical step is performed.

- RF tags and matching of a pair. Similar to Captive Key in concept, but for hose connections, and perhaps other situations. PFD = 0.01

- Unique connections. Unique size, coupling type, thread pattern, etc. to reduce the chance of a wrong connection. PFD = 0.01

- Spring closing lever valves. Manual valve that the human has to hold open by use of the lever handle (typically) that will automatically close when the lever is released. Also called a dead-man valve. PFD = 0.1 to 0.01 (but usually PFD = 0.1 maximum). Such arrangements are applicable to small valves to prevent leaving a valve unattended, such as during manual draining or loading. Can be defeated by tying the handle in the open position.

- Swing Elbow. The elbow and associated piping is designed to that the process can only be lined up in *One* direction at a time. PFD = 0.001. This arrange works well for switching to process modes, such as regeneration of desiccant driers or catalytic reactor beds with very hot air or steam, but when the normal flow alignment is to a hydrocarbon process.

- Unique SIF to compensate for, rather than prevent, a Human Error. PFD = 0.1 to 0.001. The example provided earlier was for an instrumented permissives. This remedy to compensate for a unique human error scenario includes installing SIFs to shut down a process or block or vent a line, such as to eliminate an overpressure scenario that is too

large for the current pressure relief system (the scenario is larger flow than any practical PSV or rupture disk system can handle).

- Increase PSV size for a scenario unique to startup or online maintenance. As needed; to achieve the full value of the PFD for the PSV configuration.

- Upgrade materials: Account for scenarios not considered in the original design by upgrading materials enough that the consequences from the human error are no longer possible, reduces likelihood by 2 to 4 orders of magnitude. See the "recommendation" in the Instrumented Permissive for one such example.

- Change design of at-risk components/system: Design out the need for components at risk, or change to a different strategy for certain unit processes. This is the inherently safer approach, and it can include some of the design considerations mentioned above.

Each organization will want to develop such a list with examples including (1) when to use each remedy, (2) what value is risk reduction is gained, (3) how to quickly estimate the cost of the remedy, and (4) an example or two of the remedy to help with clarification. Below is an example from a company standard for Additional Protection Layers against human error (once the baseline human factors have been optimized). This company's focus was primary on releases from open end pipes, but the remedies apply to many scenarios other than Open Ends (OE) and Misdirected Flow (MD).

EXAMPLE from one International Chemical Company: Types of Additional Protection Layers (APLs); some are Independent Protection Layers (IPLs)

Type	Specifics	Risk Reduction Factor	For …*	Cost, $K
Bar Code /Scanner	Bar Code – w/o procedure imbedded; combined with interlocks	3-10	OE/MD	0.1 per
Bar Code /Scanner	Bar Code – with procedure imbedded; combined with interlocks	3-10	All	0.3 per
Proof Switches	RFID (radio frequency identification; the reader is hardwired)	100	OE/MD	5 per
Proof Switches	Proximity Limit Switches (both ends are hardwired)	10-100	OE/MD	0.5 per
Hardware	Stand-alone valve (spring loaded dead-man valves; for quick draining/venting)	10-100	OE	0.2 to 1 per
Hardware	Dry disconnects (auto-closing valve on hose end designed to have no leaks on disconnection)	10-100	OE	TBD
Hardware	Automated/interlocked valve (typically to eliminate hose)	100	OE/MD	1 to 10 per valve
Hardware	Captive Key	100	OE/MD	0.5 to 1 per

* OE = Open Ended; MD = Misdirected

Example of a specific application of the remedies at the same International Chemical Company:

- ***Bleed and Drain Valves*** *- Spills from small bleed and drain valves unknowingly being left open can be reduced by replacing these valves with spring-loaded dead man valves. This solution is the most attractive for small valves that are not opened for lengthy periods of time. It is estimated that annual disposal cost of material spilled from these events is roughly $300,000, along with a non-quantified product loss cost. The installed cost of these valves is about $200 each, and their use will reduce the probability of these spills by a factor of 10 to 100. Of course, there are ways to defeat this solution, but with selective application and audits by outsiders, the risk reduction factors stated should be achievable.*

6 Closing

Optimizing human factors is critical for reducing the risk of accidents that have human error as the initiating event. In many cases, lowering the human error rate of the initiating event will not achieve tolerable risk. In such cases, we need to first find (identify) the scenario and then understand the scenario well enough to realize the risk of such scenarios are real. 80% of major accident scenarios begin with a human error during startup, shutdown, or online maintenance, as stated in textbooks and many papers on hazard evaluations (PHA), the PHA of the procedure steps will find the 90% of such scenarios that are missed by PHA of normal / continuous mode of operation. Once the scenario is understood, the last step is the risk control is to identify and implement the best remedy to either (1) inhibit the capacity of the human to make the error or (2) compensate for the human error if it does occur. As described in this paper, these steps and remedies can and have been applied across many organizations and sites to control the risk of such human-centric accident scenarios.

7 References

References Cited

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. A. Swain and H. Guttmann, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Sandia National Laboratories*, 1983 [this document became NUREG/CR-1278– The Human Reliability Handbook, guidelines from the US NRC on Human Reliability Analysis].

7. STTD. WSRC-TR-93-581, H.C. Benhardt et al, "Savanah River Site, Human Error Data Base Development for Nonreactor Nuclear Facilities (U)", Westinghouse Savannah River Company, Aiken, SC, February 28, 1994.

8. W.G. Bridges and G.M. Collazo, "Human Factors and Their Optimization", 8th Global Congress on Process Safety, Houston, TX, April 1-4, 2012, American Institute of Chemical Engineers.

9. U.S. Chemical Safety and Hazard Investigation Board, *Investigation Report, Refinery Explosion and Fire*, Report No. Report No. 2005-04-I-TX, March 2007.

10. CCPS, *Guidelines for Independent Protection Layers and Initiating Events in Layer of Protection Analysis*, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, NY, 2012.

11. J.V. Bukowski, Results of Statistical Analysis of Pressure Relief Valve Proof Test Data Designed to Validate a Mechanical Parts Failure Database, Technical Report, exida, Sellersville, PA, 2007.

12. J.V. Bukowski and W.M. Goble, Villanova University, *Analysis of Pressure Relief Valve Proof Test Data: Findings and Implications*, 10th Plant Process Safety Symposium, American Institute of Chemical Engineers, 2008.

13. J.V. Bukowski and W.M. Goble, Villanova University, *Analysis of Pressure Relief Valve Proof Test Data*, Process Safety Progress, American Institute of Chemical Engineers, March 2009.

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

15. A. Swain, *Human Reliability Analysis*, Training Course, ABS Consulting (formerly JBF Associates), 1993.

16. US Federal Aviation Administration, “AC 120-42B - Extended Operations (ETOPS and Polar Operations)”, Washington, DC, June 13, 2008.

17. W. Bridges and R. Al-Zahrani, “Best Practices for Addressing Human Factors during PHAs/HAZOPs… Especially during PHA of Non-normal Modes of Operation (Startup, Shutdown, & Online Maintenance)” 15th Global Congress on Process Safety, New Orleans, march 31-April 3, 2019, American Institute of Chemical Engineers.

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

19. 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.

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

21. Hammer, W., “Occupational Safety Management and Engineering, 3rd Ed.,” Prentice Hall, 1985.

22. 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.

Additional References

1. A. Swain, Accident Sequence Evaluation Program (ASEP): Human Reliability Analysis Procedure, NUREG/CR-4772, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington, DC, February 1987.

2. Human Error Repository and Analysis (HERA) System, NUREG/CR-6903, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington, DC, 2006.