SPRING21
+17TH GCPS
A Joint AIChE and CCPS Meeting

Human Factors Elements Missing from Process Safety Management (PSM) Systems

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

William C. Rhodes II, P.E.
Process Improvement Institute, Inc. (PII)
82 Via Santa Maria
San Clemente, CA 92672
wrhodes@piii.com

PROCESS IMPROVEMENT INSTITUTE

Prepared for Presentation at
American Institute of Chemical Engineers
2021 Spring Meeting and 17th Global Congress on Process Safety
Virtual
April 18 - 22, 2021

Human Factors Elements Missing from Process Safety Management (PSM) Systems

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

William C. Rhodes II, P.E.
Process Improvement Institute, Inc. (PII)

Keywords: human factors, process safety, PSM, human error, risk-based process safety, RBPS, conduct of operations, operational discipline

Abstract

Process safety is about controlling risk of failures and errors; controlling risk is primarily about reducing the risk of human error. All elements of Risk-Based Process Safety (RBPS) and alternative standards for process safety (such as US OSHA's standard for Process Safety Management [PSM] or ACC's Process Safety Code™ [PSC]) have many elements, and each of these in turn helps to reduce the chance of human error or else helps to limit the impact of human error. But each process safety standard has some weakness in the control of human error.

This paper presents an overview of human factor fundamentals, discusses why many PSM systems are weak on human factors and outlines a comprehensive process safety element on Human Factors. It describes what belongs in each category within the Human Factors element and explains the intent, content, and the benefit of each category. The paper also presents examples of Human Factors' deficiencies and selected examples of industry practices for human factors control are provided. This paper builds on earlier papers, starting from 2010, on the same topic.

1 Introduction

All accidents (or nearly all, if you consider that there are some natural phenomena that we either cannot guard against or choose not to guard against) result from human error. This is because humans govern and accomplish all of the activities necessary to control the risk of accidents. Humans influence other humans in the process – not only do humans cause accidents (unintentionally) by making errors directly related to the process itself, but they also cause errors by creating deficiencies in the design and the implementation of management systems (i.e., we make errors in authorities, accountabilities, procedures, feedback, proof documents, continual improvement provisions). Ultimately these management systems govern the human error rate directly contacting or directly influencing the process. The process-related activities where errors have the most influence include:

- Designing of a process
- Engineering of a process
- Specifying the process components
- Receiving and installing equipment
- Commissioning
- Operating the process
- Predicting safeguards necessary to control the risk at an acceptable level and sustaining these safeguards for the life of the process
- Maintaining, inspecting and repairing the process
- Troubleshooting and shutting down the process
- Managing Process Changes

99% of accidental losses (except for natural disasters) begin with a human error ***(supported by data from more than 1500 investigations)***

Root causes of accidents are management system weaknesses
(Center for Chemical Process Safety, American Institute for Chemical Engineers, "Guidelines for Investigating Chemical Process Incidents", 2003) – OSHA agrees

Weak Management Systems ➔ Human Error ➔Accidents

Figure 1: Relationship between Accidents and Management Systems

Recent major accidents have highlighted the need for increased focus on Human Factors. The US Chemical Safety Board (CSB) cited human factor deficiencies as one of the main contributors of the catastrophic accident at the BP Texas City Refinery in March 2005. The human factor deficiencies included lack of control of worker fatigue, poor human-system-interface design, poor communication by radio/phone, out-of-date and inaccurate operating procedures, and poor (no) communication between workers at shift handover. The CSB cited similar issues from many other accidents, including the Chevron Richmond Refinery fire in 20212, and has urged industry and the US OSHA (the regulator) to pay much more attention to human factors. This led to the OSHA National Emphasis Program for Refineries to include human factors as one of the 12 core elements it reviewed in detail across many of the 148 oil refineries in the USA around 2010.

Implementing human factor engineering and policies to prevent accidents is not a new concept. Nearly all (or all, from a more complete perspective) of the causes and root causes of major accidents in the past 40 years have been the result of poor control of human factors. This has been cited in many root causes analysis reports and papers concerning these major accidents.

Process Safety Management (PSM) systems based on OSHA's PSM standard are likely lacking the fundamental human factor standards that if applied across the applicable PSM elements, would work together to reduce human error. The *Risk Based Process Safety (2007)* industry standard from the CCPS/AIChE does contain the human factor standards, but these are presented under at least six (6) of the PSM elements instead of under a stand-alone human factor element. This guideline does not provide a needed road map to help companies transition to RBPS from the minimum PSM systems defined in OSHA's PSM standard. A starting point for this transition should be implementing a human factor element comprised of the human factor categories missing from most PSM systems (especially from those based on the OSHA PSM standard).

Definitions for Use in This Paper

- This paper will use the term **Human Error** to mean the errors that are made during direct interface or direct influence of the process.
- **Human Factors** are those aspects of the process and related systems that make it more likely for the human to make a mistake that in turn causes or could cause a deviation in the process or could in some indirect way lead to the increased probability of an accidental loss.
- **Management systems are** the administrative controls an organization puts in place to manage the people and workflow related to the process under consideration, and so these inherently attempt to control human factors

2. Human Error Fundamentals

Types of Human Error

In simplest terms, there are only two types of human error: *Errors of Omission* (someone skips a required or necessary step) and *Errors of Commission* (someone performs the step wrong). But in addition, these errors occur either inadvertently (unintentional error) or they occur because the worker believes his or her way is a better way (intentional error, but not intentional harm). Intentional errors can usually be thought of as errors in judgment. Some believe a "lack of awareness of the risk" causes these errors, but in actual practice, the worker commits an intentional error may wellbe aware of the risk. They instead believe they know a better way to accomplish a task or they believe there are already too many layers of protection (so bypassing one layer will not cause any harm).

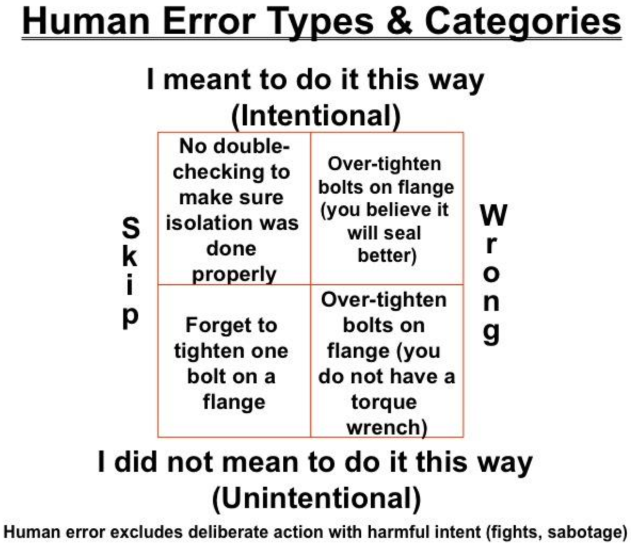


Figure 2: Types and Categories of Human Error

Regardless of type or category of human error, the organization can and should exert considerable control of the errors.

Controlling Human Error through Management Systems

A process is a combination of the utilities, raw materials, and human actions (direct actions and those actions involving programming the process to accomplish automatic functions). If anything goes wrong with these Inputs, or if there are basic design flaws or basic fabrication flaws in the process, then the Outputs will not be desired. The desired output is acceptable (or high) production rates at acceptable or higher quality factors with no harm to the humans (long term or short term), no harm to the environment, and with acceptable (or higher) life of the process components. The negative outcomes resulting from humans failing to control the raw material quality, failing to control the utility levels consistently, making errors directly related to the operation of the process, or making errors in the care of the process (such as maintenance) will result in lower production, lower quality, higher number and severity of safety-related accidents, and more negative impact on the environment. The potential (probability) of the negative outcomes is collectively referred to as ***business risk*** – more precisely, the risk is a product of the likelihood of one or more of these negative outcomes and the severity of each outcome.

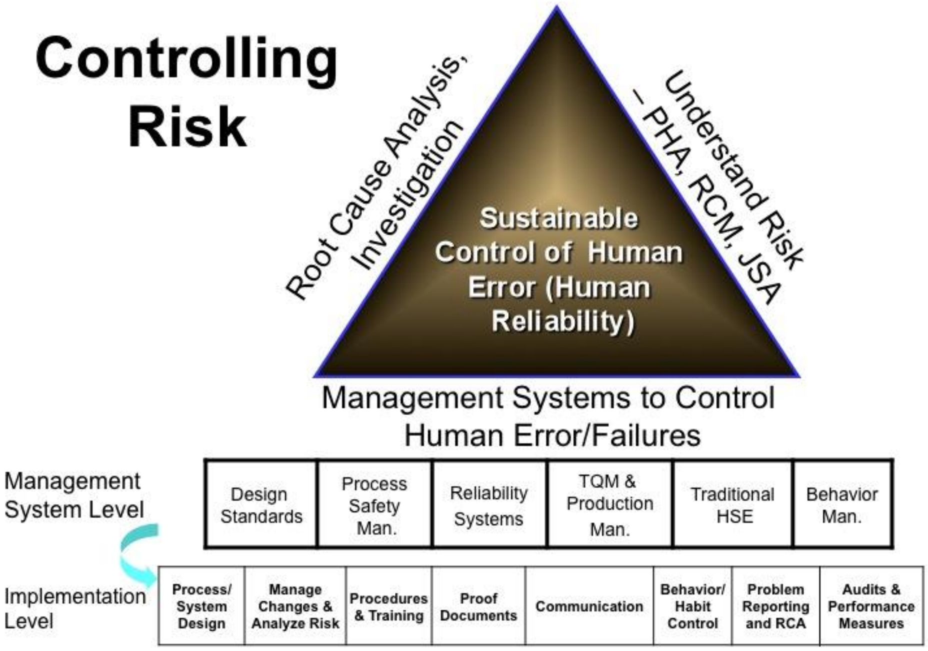
A critical concept is therefore:

If an organization does not directly control risk, the organization cannot directly control quality, safety, environmental impact, or production to acceptable levels. An organization must sustainably control human error to manage the risk of accidental losses that impact quality, safety, the environment, production, or assets.

In order to sustainably control the risk of a complex process (such as an oil/gas operation, refinery, chemical plant, steel plant, automobile manufacturing, aircraft manufacturing, etc.), the organization must design and implement management systems to:

- **Understand the Risk** – This involves predicting problems; which in turn includes predicting the risk of possible accident/loss scenarios, establishing the appropriate design and the right layers of protection to control risk to a tolerable level
- **Control Risk Factors Day-to-Day** – This involves controlling the original design by maintaining the established layers of protection and managing changes to the design using integrated management systems
- **Analyze Actual Problems and Determine Weaknesses in the System –** This involves identifying weaknesses in designs and management systems and weaknesses in risk understanding through root cause analysis of actual problems (losses and near-losses)

These three elements are illustrated in the following figure:



© Process Improvement Institute, Inc. (2004-2021)
Figure 3: Controlling Risk through Human Reliability

Management systems control the interaction of people with each other and with processes. They are the high level procedures we use to control major activities like conducting PHAs, management of change, writing operating procedures, training employees, evaluating fitness for duty, conducting incident investigations, etc. If management systems are weak, then layers of protection will fail and accidents will happen.

To reiterate, accidents are caused by human error. In general, Process Safety Management (PSM) is focused on maintaining these human errors at a tolerable level because:

- All accidents happen due to errors made by humans; including premature failure of equipment. There are a myriad of management systems to control these human errors and to limit their impact on safety, environment, and quality/production
- When these management systems have weaknesses, near misses occur
- When enough near misses occur, accidents/losses occur

3. Human Factor Categories and Typical Impact of Each

To minimize human error, process safety systems should address the **Human Factors Categories** (see various US NRC and US DOE standards from 1980s and 1990s)[1,2]. The table on the next page lists the key human factor categories along with multiplication factors that poor human factors can have on the base human error rates. If all of these human error rates are controlled very well, then the optimized human error rates listed in the next section are achievable.

TABLE 1: SUMMARY 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. 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	P(failure)=100%
	Barely adequate time (≈2/3 x nominal)	10
	Nominal time (1x what is expected)	1
	Extra time (at least 2x nominal and >20 min)	0.1
	Expansive time (> 4 x nominal and > 20 min)	0.01
Stress/Stressors (includes staffing issues)	Extreme (threat stress)	5
	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 hrs/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
	No communication or system interference/damage	10
Communcation	No standard for verbal communication rules ***(normal value for process industry)***	3
	Well implemented and practiced standard	1

If all of these human error factors are controlled very well, then the optimized human error rates listed in Section 5. of this document are achievable. Alternatively, if one or more of these factors are compromised, the human error rate will increase by the values shown in this table. As an example, an individual whose fitness for duty rating is unfit due to the excessive work hours shown in the table will make errors at a rate 20 times greater than an individual whose fitness for duty is normal.

With excellent control of each of the human factors listed above, a company can begin to approach the lower limits that have been observed for human error. These lower limits are about:

- **1 mistake in 100 steps for most procedures-based tasks** (such as starting up a process unit), a little less for a routine (daily) task that becomes almost a reflex

- **1 in 10 chance or a little better for diagnosis and response to a critical alarm**

Excellent control requires superior design and implementation of management systems, which is enabled through a thorough understanding of these factors, as outlined below.

4. Incorporating Human Factors into PSM Systems

The basis upon which most companies build their PSM system is their applicable PSM regulation (e.g., the OSHA PSM standard found at 29 CFR 1910.119 in the United States.) Unfortunately, this standard, which was promulgated in 1992 (and has been essentially unchanged since), is devoid of human factor controls with a few exceptions as outlined by Bridges and Tew[3]. The only direct reference to the term “human factors” is mentioned in paragraph (e), Process Hazard Analysis (PHA), which states that the PHA team must consider human factors (presumably in the review of the causes and the quality of the safeguards). The other mention that alludes to human factors, is in Operating Procedures (see paragraph (f)) which states procedures “must be written clearly and understandably.” Similar PSM regulations in other countries are likewise silent on human factors.

The next logical place to seek guidance for incorporating human factors into a company’s PSM system is industry-specific standards; therefore, some companies may use these to build upon the regulatory framework. In the chemical process industry, such a standard was published in 1985 by the Center for Chemical Process Safety (CCPS), which is a division of the American Institute of Chemical Engineers (AIChE). This standard included a strong emphasis on human factors since Human Factors was one of its original 12 elements. However, in 2007 the CCPS revised their standard as “Guidelines for Risk-Based Process Safety”[4] (RBPS). This revision abandoned the global element on human factors, and instead spread the direct control of human factors throughout 6 elements. The authors believe that this change not only diminishes the importance of human factors, but also reduces the ability of companies to effectively implement human factors throughout their PSM program.

The CCPS partially addressed this shortcoming by publishing a guideline entitled “Conduct of Operations and Operational Discipline”[5] (COO/OD) in 2011. As outlined in Section 8 of this paper, this newer guideline provides a great deal of practical and useful information for implementing *most* human factors; however, the information contained within it is still incomplete. Therefore, to fully integrate human factors into a PSM program, companies should consult the detailed review of each human factor outlined in Section 5 of this paper to develop the necessary tools to fully implement human factors into their PSM systems.

5. Details on Incorporating Human Factors Within Existing PSM Systems

A. AVAILABLE TIME and STRESS / STRESSORS

The **Available Time** for the task refers to the time the task is expected to be required for completion. In many cases the time determined for a process is determined using the theoretical times where the conditions are "ideal" and not necessarily realistic. When task and process duration are not realistic people tend to "find the best and easy way" to get it done, ultimately creating latent conditions for error occurrence. **Work Stress** refers to the emotional response that arises when work demands exceed the person's capacity and capability to cope. Some processes have been designed paying little attention to job design, work organization and management systems. Failing to fulfill this requirement eventually results in work stress.

Staffing levels directly impact both factors. Staffing is the process of assessing, maintaining and scheduling personnel resources to accomplish work. An adequately staffed organization ensures that personnel are available with the proper qualifications for both planned and foreseeable unplanned activities. Staffing is a dynamic process in which plant management monitors personnel performance to ensure that overall organizational performance goals are met or exceeded. The result of an effective staffing process is a balance between personnel costs and the achievement of broader organizational goals.

Three key issues must be considered when staffing decisions are made; the first of which is selecting the right staff for a job. Each organization requires the proper amount and type of expertise to safely and competently operate the plant under a variety of conditions. The term "expertise" includes the attributes of talent, effectiveness, knowledge, skills, abilities, and experience necessary to operate and maintain plant systems, structures and components.

The second key issue is avoiding staff overload. Surges in workload, such as during outages, typically require staff augmentation as well as longer work hours for permanent staff. The introduction of contractor personnel or company personnel from other sites may increase the likelihood of errors due to unfamiliarity with the plant, its procedures and hardware, for example. Longer work hours have the potential to increase fatigue, which also contributes to the likelihood of error.

The third key factor is rotating staff every 1 hour or less for tasks that require high vigilance. Humans are inherently unable to remain alert for signals that seldom, if ever, occur. Even a sailor whose life is at stake cannot maintain an effective watch (look-out) for hostile submarines for more than 30 minutes or so. The following figure illustrates the rapid decrease of vigilance with time.

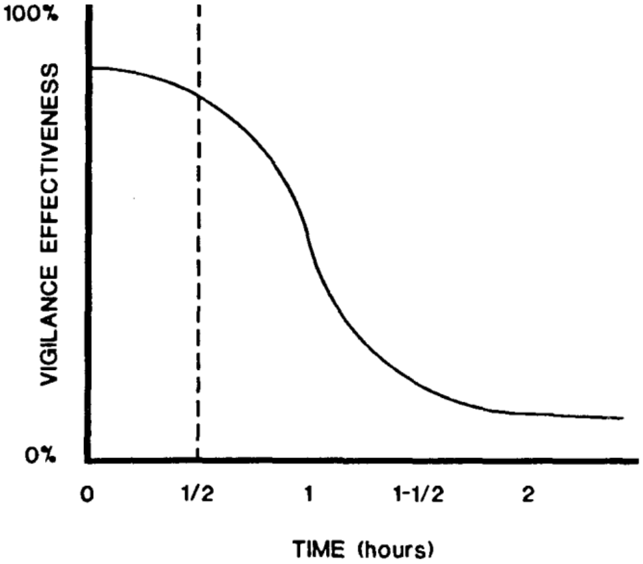


Figure 4: Vigilance as a Function of Time

Placing a worker in situations requiring extended, uneventful vigilance may lead to accidents. Therefore, it is important to design control systems in a manner that requires regular operator interaction so that the operator will remain attentive.

B. TASK DESIGN

A task that is designed with the human limits in mind is much more likely to work effectively than one that assumes humans can and will "always" do what is written. The task must consider that humans think and remember and factor in prior data and prior experiences. Factors to consider in assessing **task design** adequacy (i.e., minimizing the likelihood of human error during its completion) include:

- Complexity of the task
- Probability of repeat errors (coupled error) on redundant aspects of the design
- Error Detection and Error Recovery

Complexity of task (procedure-based or a call for action) – If the task is too complex, then humans can forget their place in the task, fail to understand the goal of each step or sub-step, or fail to notice when something isn't going right. Task complexity is a function of:

- 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)
- 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)
- number of staff involved (more staff = more complex)
- number of adjustments necessary to achieve the goal
- amount of mental math required (as a rule, NO math should be required in anyone's head when accomplishing a standardized task)

- how much judgment is required to know when you have accomplished each goal within the task

  For most chemical process environments, the complexity of the task is relatively low (one action per step), but for response actions (in which humans serve as the Independent Protection Layer (IPL)), there are almost always other tasks underway when the out-of-bounds reading or the alarm is activated. Complexity is difficult to predict (since it is not known when a human intervention will be needed), but higher complexity can increase error rates by 2 to 10 times.

Probability of repeat errors (Coupled errors) – For many maintenance tasks, making a repeat error or "common cause error" or "dependent error" can lead to failures of all backup systems. Such errors have led to MANY airplane crashes and major process safety accidents as well.

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 there 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 strong visual cue is present (if you can clearly see the first devices you worked on), if a mistake is made on the first step of the two or more
- 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 is due to the trust that can rapidly build.

These factors are based on the relationships provided in NUREG-1278[1] and the related definitions of weak and strong coupling provided in the training course by Swain (1993)[1] 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 a safety instrumented function (SIF) to operation, after bypassing the SIF. The qualitative values in Table 2 are based jointly on Swain[1] (1993) and Gertman (SPAR-H, 2005 which is NUREG/CR-6883)[2].

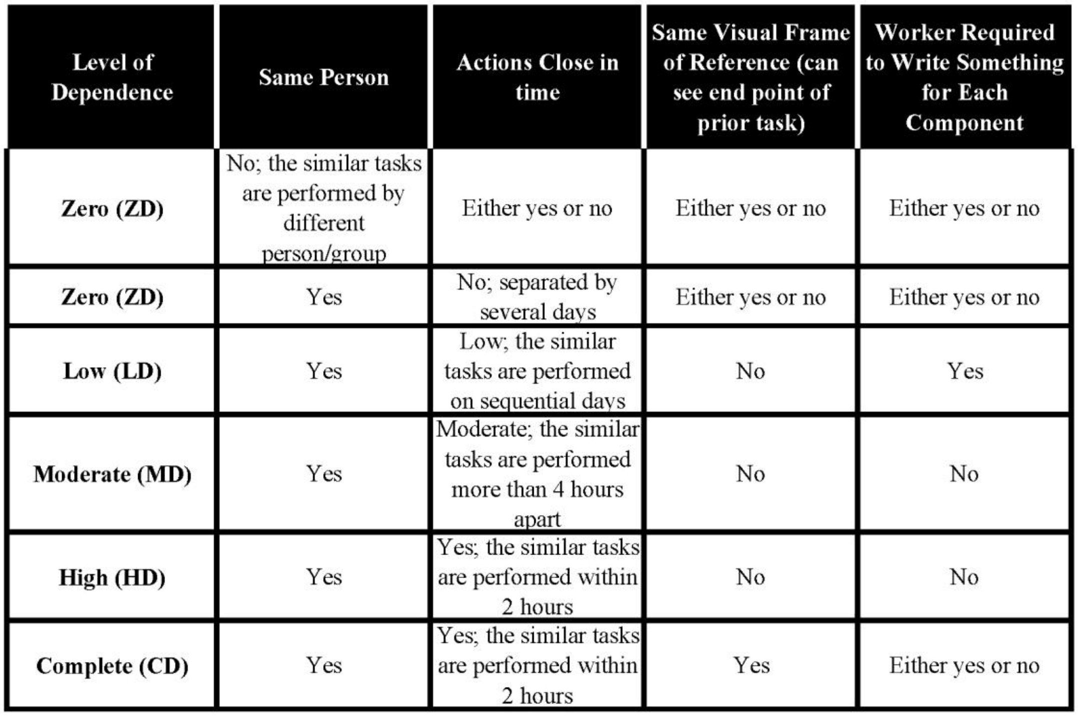
One can readily conclude that staggering of maintenance tasks for different channels of the same SIF or for related SIFs will greatly reduce the level of dependent errors. Unfortunately, most sites PII visits do not stagger the inspection, test, or calibration of redundant channels of the same SIF or 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 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 120-42A*, as part of Extended Operations (ETOPS) approval).[6]

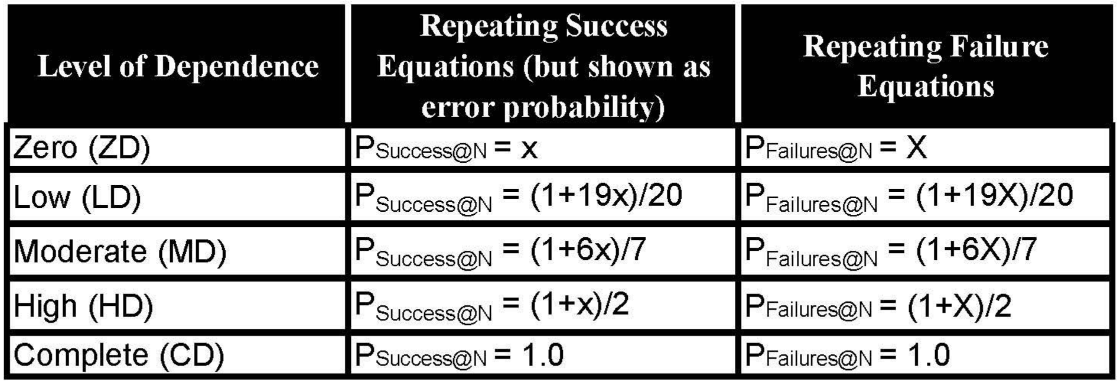
Table 2: Guideline for Assessing Dependence for a within-SIF Set of Identical Tasks (based partially on SPAR-H, 2005 [1,2], and partially on field observations by PII) Courtesy Process Improvement Institute, Inc., All Rights Reserved



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

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[1] (and the similar table in SPAR-H [Gertman, 2005][2]).

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 *Courtesy Process Improvement Institute, Inc., All Rights Reserved*



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)	$P_{Success@N} = 1.0$	$P_{Failures@N} = 1.0$

Error detection and error recovery – Is there enough feedback in the process to allow the worker to realize (in time) that they made a mistake? Have they been trained on how to reason through how to recover from mistakes they or others make? (Sometimes, doing a step too late is far worse than NOT doing the step at all.) Is there enough time available for the type of intervention necessary?

C. EXPERIENCE/TRAINING

Training is necessary for general functioning of management systems and for task-specific skills such as how to start up a compressor, repair a pump, lead a root cause analysis, perform a proper Lock-Out/Tag-Out, etc. Organizations normally do a good job of training, including hands-on training. Training systems can be weak (inadequate) however if the training system does not adequately:

- Address how to troubleshoot the process (i.e., handle process deviations or upsets).
- Provide workers with a mental model(s) of the process so they can perform the assigned tasks correctly, diagnose process upsets properly and quickly, and understand the consequences of their actions.
- Provide workers with enough practice of critical tasks

Ironically, training is many times listed as the "cause" or "root cause" of an accident, when in fact the training is adequate, and some other human factor is the major cause.

D. PROCEDURES

Many procedures do not follow best practices for controlling human error, and so the written procedure actually "contributes" to increased error rates. Further, many organizations are missing guides on how to troubleshoot (what to do when process deviations occur). The best practice rules for writing and validating procedures have been published for many years ***(see Bridges, 1997-2010)***[3, 7, 8]. Below is a checklist based on the current set of best practice rules for developing operating, maintenance, and other work-instructions (procedures):

TABLE 4: PROCEDURE QUALITY CHECKLIST (courtesy PII, 2008)

#	Issue	Response
	Procedure Content Checklist	
1	Is the procedure drafted by a future user of the written procedure? (Engineers should not author procedures to be used by operators or maintenance staff.)	
2	Is the procedure validated by a walk-down in the field by another future user of the procedures?	
3	Is the procedure reviewed and commented on by technical staff (engineers or vendors)?	
4	Is the procedure checked versus the Page and Step format rules below?	
5	Is a hazard review of step-by-step procedures performed to make sure there are sufficient safeguards (IPLs) against the errors that will occur eventually (when a step is skipped or performed wrong)?	

#	Issue	Response
6	Is the content measured using “newly trained operators” to judge the % of steps that are missing, steps that are confusing or wrong, and steps that are out-of-sequence? (A score of 95% accuracy of content is good.)	
	Page Format Checklist	
1	Is the title of the procedure the largest item on the page?	
2	Is the procedure title clear and consistent with other titles, and does it uniquely describes the topic?	
3	Are the document control features the smallest items on the page?	
4	Are temporary procedures clearly identified?	
5	Is white space used effectively? • Is there one blank line between each step? • Does indentation help the user keep their place? • Are the margins large enough to reduce page congestion?	
6	Is type size 12 point font or larger?	
7	Is serif type used (rather than sans-serif)?	
8	Is mixed case used for words of steps, with ALL CAPS used only for special cases (such as IF, THEN, AUTO, and WARNING)?	
9	Is the step number very simple (single level of number used)? Only an integer?	
10	Have sections or information not necessary to performing the steps been moved to the back or to another part of the manual or training guide?	
11	Are section titles bold or larger than the text font? Do sections have clear endings?	
12	Is the decision on electronic presentation versus hard copy correct? Are electronic linkages to procedures clear and accurate and easy to use? If paper is chosen, is the color of the paper appropriate?	
13	Is the overall page format (such as Outline format or T-Bar format) appropriate to the use of the procedure?	
14	Are play script features added for tasks that must be coordinated between two or more users? • Play script is normally used when there are two or more hand-offs of responsibility for steps.	
15	Are rules followed for formatting of Warnings, Cautions, and Notes? (See annotated rules, such as Warnings are for worker safety and Warnings must clearly standout from rest of page.)	
	Step Writing Checklist	
1	Is each step written as a command?	
2	Is the proper level of detail used throughout? This is judged based on: • *Who* will use the procedures • Same level of detail used in similar procedure steps	
3	On average, is there only one implied action per instruction? Best practice is to average 1.2.	
4	Does the procedure indicate when sequence is important? • If sequence matters, each step should be numbered (with an integer or letter) • If sequence does not matter, bullet lists should be used	
5	Are only common words used? Apply “education” level test (5 grade reading level is best)	
6	Do all acronyms, abbreviations, and jargon aid understanding? • Develop a list of such terms for use in procedures *and* communication. • Use terms that users use (within reason)	
7	Is each step specific enough? No room left to guess/interpret: • The meaning of a word or phrase (Check vs. Make sure) • The intent of a step or series of steps • A desired quantity or value • To what equipment the step applies	
8	Is the procedure free of steps that require in-your-head calculations? • Values expressed as ranges rather than targets with error bands • Conversion tables, worksheets, or graphs provided where needed	

#	Issue	Response
9	Are graphics to the user's advantage? • No explanatory paragraphs or lengthy instructions that could be replaced by a picture • No impressive graphics that provide no real advantage	
10	Are references to the user's advantage? • No lengthy explanations or instructions that could be replaced by branching to a reference • No references to a procedure that references still another • No gaps or overlaps between this procedure and a referenced document • If branching, must branch to a procedure, not to a specific step in a procedure	
11	Are rules followed for writing warnings, cautions, and conditional steps? • No more than 2 per page • No actions within a warning or caution (actions must always be numbered steps) • Warnings and Cautions contain descriptions of potential consequences	

For procedures to be effective in ensuring that tasks are performed correctly, they must be used. There are many reasons that workers may not use procedures. ***Deficient Procedures*** are the most prevalent problem in process industries since procedures have not traditionally been developed from the perspective of optimizing human factors; instead, procedures have been traditionally developed to meet a compliance requirement to have written procedures. Examples of procedure deficiencies (inaccuracies) include:

- Incorrect/incomplete/nonexistent. Most procedures we have audited have been only 70-85% accurate; the inaccuracies include missing critical steps, steps as written are not what needs to be done, or the steps are out of sequence
- No/misplaced warnings. For example, a warning should never **contain** the action to take; it should instead **emphasize** the action to take
- Poor format and presentation rules

Other reasons workers may not use procedures include:

- Procedures are out of date
- No procedure has been written for the task
- Users cannot find the procedure they want to use
- Users don't need a procedure because the task is simple
- Users need more information than the procedures contain
- Users see procedures as an affront to their skill
- Procedures are difficult to use in the work environment
- Procedures are difficult to understand

So, in addition to the rules for writing procedures that are shown in the table above, the organization must also address the reasons that cause the worker not to use the written procedure.

E. HUMAN-MACHINE INTERFACE (INCLUDING TOOLS)

The **Human-Machine Interface** (also known as the Human-System Interface, or HSI) is defined as the technology through which personnel interact with plant systems to perform their functions and tasks. The major types of HSIs include alarms, information systems, and control systems.

Each type of HSI is made up of hardware and software components that provide information displays, which are the means for user-system interaction, and controls for executing these interactions.

Personnel use of HSIs is influenced directly by (1) the organization of HSIs into workstations (e.g., consoles and panels); (2) the arrangement of workstations and supporting equipment into facilities, such as a main control room, remote shutdown station, local control station, technical support center, and emergency operations facility; and (3) the environmental conditions in which the HSIs are used, including temperature, humidity, ventilation, illumination, and noise.

There are three important goals to be achieved in the design and implementation of the HSI. These are:

- **Design for operability** refers to designing the HSI to be consistent with the abilities and limitations of the personnel who will be operating it. Weaknesses in the design processes can result in an HSI that is not well suited to the tasks that personnel must perform to ensure plant safety, resulting in increased workload, decreased performance by personnel, and an increased likelihood of errors.

  The wide-spread adoption of distributed control systems has provided many advances in process control. However, if implemented improperly, these systems can greatly reduce the operability of the facility. Although they were unable to provide as much information, old analog panels were typically laid out in a manner such that experienced operators were able to monitor the entire process and effectively identify conditions meriting attention. Due to space limitations, and their cost (e.g., hardware and installation), alarms were typically limited to those deemed to be associated with a significant process upset.

  The advent of distributed control systems has eliminated the space limitations associated with alarms, and greatly reduced their costs (in many cases, alarms can be added merely through programming). Without proper alarm configuration structure and discipline, this can lead to “alarm flooding” (an excessive number of simultaneous alarms) during abnormal operating conditions. The human error of failing to respond properly to an alarm increases by a factor of over 1,000 if ten alarms activate simultaneously compared to a single alarm activation.

  Therefore, it is critical that control and alarm system designers in facilities with distributed control systems properly prioritize information so that operators can respond appropriately to abnormal conditions. Further, trouble-shooting guides should be readily accessible via the distributed control system to reduce human error in alarm response.

  Beyond the topic of alarms, the proper design of the visual displays can also reduce human error. Certain color combinations, such as a light gray background with darker gray equipment and black lines coupled with a flashing red indication for those components in an alarm state effectively draw the operators’ attention to the relevant part of the process requiring attention. Further, an effective display should include:

    - Safety systems that are bypassed, impaired, or out of service
    - Process alarms that are disabled
    - Process conditions that are not within established limits
    - Backup systems that are unavailable
    - Special maintenance or testing activities that are currently in progress

- **Design for maintainability** refers to designing the HSI and associated plant equipment to ensure that personnel are able to perform necessary maintenance activities efficiently. Weaknesses in the design process can result in systems that impose excessive demands on personnel for maintenance and, therefore, are prone to maintenance errors or problems with reliability and availability.

- **Design for flexibility** refers to the way that changes, such as upgrades to the HSI, are planned and put into use. A new HSI component may require the user to perform functions and tasks in new ways. Skills that the user developed for managing workload when using the former design, such as ways for scanning information or executing control actions, may no longer be compatible with the new design. The new HSIs must also be compatible with the remaining HSIs so that operators can use them together with limited possibilities for human error. Also, HSI modifications may not be installed or put into service all at one time, causing the user to adapt to temporary configurations that are different from both the original and final configurations. Weaknesses in HSI implementation can increase operator workload and the likelihood of errors.

Tools are a special category of HSI, which typically refers to hand tools or devices that are generally designed with the user in mind. A big part of human factor consideration is how to make the equipment and process operation mistake-proof (to prevent errors as much as possible). The following are some factors to consider when error proofing in designs:

- **Design for unambiguous assembly.** Design the product or device such that the assembly process is unambiguous (by designing components so that they can only be assembled one way); i.e., design matching parts that are easy to insert and align. For example, use notches, asymmetrical holes, and stops to mistake-proof the assembly process. Products that go together in only one way require less worker training, perform more reliably, and can be repaired more quickly.
- **Consult workers.** Operators, technicians, and maintenance personnel can pinpoint the most troublesome areas.
- **Avoid symmetry.** When a particular orientation is critical to the design, avoid symmetry. For example, use nonsymmetrical hole patterns.
- **Use labels sparingly.** Labels tend to come off equipment too easily and often are wordy.
- **Review the environment.** Environmental problems that encourage mistakes include poor lighting; high/low heat; excess humidity, dust, and noise — anything that distracts workers.

The following are some factors to consider when error proofing in process/operations:

- **Error-proof mechanisms.** Error-proof mechanisms are very powerful in improving system reliability when incorporated into the design. These mechanisms, by design, will not allow a user to perform an illegal operation. For example, if a user enters a value that is outside the accepted range of operation, the control logic will not accept the value.

- **Automatic alerts.** Automatic alerts immediately inform the user of an illegal operation to prompt corrective action. These alerts are particularly useful in critical operations that allow time for corrective action before some adverse consequence occurs. For example, a piping manifold may be designed such that a warning alarm sounds if valves are not opened/closed in the proper, critical sequence, or if a critical valve is left opened/closed.
- **Automatic system shutdown.** Automatic system shutdown should be incorporated into the design when an illegal action is performed during a critical operation and no time is available for corrective action. For example, if an operator uses the wrong sequence in charging a reactor, the reactor will shut down before other materials are charged that may lead to critical temperatures and pressures.

F. FITNESS FOR DUTY

Successful task performance requires that the capabilities that workers bring to the task fall within an expected range. **Fitness for Duty** issues include reduction in an individual's mental or physical capabilities due to substance abuse, fatigue, illness or stress, which increases the likelihood of errors. Types of possible impairments include:

- Physical attributes – strength, reach, eye-sight and color acuity, hearing,
- Mental attributes – drug and alcohol (abuse), mental stress (on and off the job);
- Fatigue – issues from on the job and off the job (especially control of hours per work-day and per work-week)

Safeguards to prevent fitness-for-duty-related errors include company programs for the detection and prevention of potential or actual impairment, as well as the individual responsibility of workers to decline assignments if they are impaired for any reason. The latter safeguard is a weak one, however, because humans are generally over-confident of their capabilities when under the influence of drugs or alcohol, or are stressed, fatigued or ill. Other factors that may discourage self-reporting include the fear of poor performance reports from supervision or not receiving pay for extra overtime.

Company programs that may be implicated in errors caused by personnel impairment include:

- **Fitness-for-Duty Program** – Company fitness-for-duty programs are primarily responsible for detecting and preventing impaired personnel from performing tasks that may affect public health and safety. Medical evaluations of personnel, behavioral observation programs, employee assistance programs and drug and alcohol testing are used to detect impairment. Impaired workers can be prevented from performing tasks by establishing protocols for instances in which a worker is believed to be unfit for duty, training for supervisors on detection of and response to fitness for duty issues, and employment guidelines for personnel who voluntarily enter drug or alcohol treatment programs. Weaknesses in a Fitness for Duty program may allow impaired personnel to have access to vital areas in a plant where they could commit errors. One excellent starting point for a Fitness for Duty sub-element is the guidance provided in ***US NRC's 10 CFR 26 (2005).***

- **Overtime Policies and Practices –** Most companies establish limits for work hours to reduce on-the-job fatigue. It has been shown that 17 hours of work without a break results in the same error rate as being legally drunk. And, at 10 days straight of 12 hours work-days, the error rates for non-routine tasks such as startup of a continuous unit can increase to 1 mistake in 5 to 10 steps (as opposed to the target of 1 mistake in 100 steps). Routine authorization for work hours in excess of those recommended may result in fatigued workers. Further, a practice of excluding training or meetings that occur outside of an individual's normal work schedule from work-hour limitations will also contribute to fatigue. In ***US NRC's 10 CFR 26*** (***2005)***, the guidance given for control of overtime hours is no more 72 hours of work per 6 day period, no more than 16 hours of work in one day within that period, and a minimum of 24 hours contiguous hours away from work within a 7 day period. The US DOT has even more stringent rules on limiting work hours and establishing required hours for recovery from fatigue.
- **Shift Scheduling –** Shift scheduling may also affect the likelihood that personnel will show performance decrements due to fatigue. A change in the assigned shift or a rotating shift schedule will disrupt circadian rhythms and may increase the likelihood of errors.
- **Safety Culture –** The effectiveness of self-reporting and behavioral observation programs depends greatly upon the safety culture at a site.

G. WORK PROCESSES AND SUPERVISION

Supervision is the process by which work is directed and overseen by first-line management. Successful supervision requires a combination of leadership skills and technical competence. Supervision differs from peer checking or quality control because a supervisor has line management responsibility for the worker(s) as well as responsibility for the work activity.

Supervision is more than the moment-to-moment direction of a work activity. Successful supervision requires the assessment and shaping of worker attitudes and motivation, communication and implementation of management expectations for performing work, the assignment of the best-qualified workers to various tasks, as well as the technical competence to identify incorrect actions and stop improper activities before an error is committed. Effective supervision involves directing the work, overseeing how it is performed, and leadership.

Organizations are typically structured to have sufficient supervision of the job, but many times the delineation between the trainer and the supervisor roles is blurred. Supervision can and normally does play a key role in selecting of the right worker for the job, scheduling of workers to match the required tasks for the day/week, and generally overseeing the task execution to ensure policies and procedures are followed. Supervisors are not always trained on all of their key roles in support of control of human factors, such as detecting issues in workers related to fitness for duty or fatigue.

H. WORK ENVIRONMENT

The **Work Environment** refers to the physical conditions in which work is performed. Environmental conditions that can affect performance include excessive vibration and noise, temperature extremes, and insufficient lighting, as summarized below:

- There are two types of **vibration** that may cause errors. The first is whole-body vibration, in which vibration is transferred to the worker from standing or sitting on a vibrating surface. The second is object vibration, in which a stationary worker interacts with a vibrating object in some fashion. The effects of vibration depend upon its frequency and acceleration. Frequency is the number of oscillations (cycles) that occur in one second. Acceleration is the force, or intensity, of the vibration.
- **Noise** is unwanted sound. Noise can cause errors in several ways. It may disrupt communications, affect the ability to perform tasks and annoy personnel. The effects of noise on communications are complex. Even relatively low levels of noise can mask speech, but only under some circumstances. For example, speakers naturally raise their voices when there is background noise and may be able to overcome some of its effects on communication. Being able to see the speaker's face or using standardized phrases also improves communication in a noisy environment. The type of background noise also affects communication. It is easier to communicate over noise that is steady and uniform than noise that includes sharp tonal peaks, such as background speech.
- **Heat exposure** is a common problem in many areas of a plant, such as the turbine building when the plant is operating. The extent to which workers will be affected by heat depends on many factors. These include physical characteristics, such as age, weight, acclimation to heat, physical fitness and dehydration. Other factors that determine the effects of heat on performance include airflow, humidity, clothing and level of physical activity.
- **Exposure to cold** affects the performance of manual tasks. Decreases in the ability to control hand movements begin at an air temperature of approximately 54° F. The fingers may become numb to pain at this temperature and touch sensitivity is reduced. Performance of gross manual tasks, such as those involving the arms and legs is also degraded at 54° F. The speed at which manual tasks can be performed is affected by the rate of cooling. Slow temperature drops have a greater negative impact on manual dexterity than rapid temperature decreases, during the initial exposure period.
- **Adequate lighting** is required for accurate performance of nearly every task in a unit operation.

The organization must have engineering controls to help control each factor, but sometimes there is no other choice but to rely upon administrative controls.

I. <u>COMMUNICATION (most importantly, verbal communication)</u>

Communication is the exchange of information while preparing for or performing work. Verbal communication occurs face-to-face, by telephone, sound-powered phones or walkie-talkies, as well as over public address systems. Written communication occurs, for example, through policies, standards, work packages, training materials, and e-mail.

Communication involves two sets of behaviors: (1) creating and sending messages and (2) receiving and interpreting them. Communication always involves at least two individuals, the sender and the receiver, and occurs:

- Between individuals

- Within and among work groups
- In meetings
- In pre-job or pre-evolution briefings
- During shift turnover

Successful communication requires several steps. The sender first develops the intention to communicate **either** verbally or in writing. The sender then composes a message that presents the meaning as clearly as possible. The receiver must pay attention to the message and then interpret its meaning. If the communication is successful, the receiver interprets the message consistently with the sender's intended meaning. However, there are many potential errors in both sending and receiving the communication:

- **Sending Errors**

  - *Content wrong*
  - *Content inconsistent*
  - *Content inappropriate for the job*
  - *Content inappropriate for the receiver*
  - *Standard terminology not used*
  - *Familiar terminology not used*
  - *Message production inadequate or interfered with*
  - *Necessary information not sent*
  - *Wrong place or person*
  - *Wrong time*
  - *Sending verification failure*

- **Receiving Errors**

  - *Information not sought*
  - *Information not found*
  - *Information not used*
  - *Receiving verification failure*
  - *Message misunderstood*.

Communication errors may be reduced in the following ways:

- Structuring messages in a standard format, which alerts the receiver if important information has been skipped
- Providing written instructions or procedures for complicated tasks
- Establishing protocols to repeat key parts of verbal communications
- Preceding special or nonroutine activities with a pre-job briefing
- Using structured protocols, checklists and logs to supplement written instructions

One key opportunity for communication errors is when a new shift takes over responsibilities from the previous shift. An effective tool to reduce these errors is a properly designed shift handover process that includes appropriate checklists and logs of activities, and a structured and consistent method for verbally reviewing this information. Additionally, the logs and discussions need to include:

- Routine operations
- Transition operations (e.g., changes to produce a different product or switch to a different raw material source)
- Nonroutine operations (e.g., maintenance activities or temporary operating conditions)

6. Beyond Optimizing Human Factors: Best Remedies for Human Error

Once an organization optimizes human factors, they must recognize that human errors will still occur – albeit at a lower frequency and likely with a smaller adverse impact than before. Therefore, in cases in which the consequence of a human error is unacceptably high, the organization should implement solutions that will lower the residual risk further. These solutions can be designed to either help prevent the error or compensates for the error, but **they must be independent of the human error initiating event**.

Bridges and Bridges [25] have compiled the following list of the best remedies for human error for these situations:

- <u>Captive Key</u>. 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.
    - <u>Special consideration</u>: only 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.

- <u>Limit switches on valve position</u>. 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.

- <u>Mechanically coupled valves:</u> 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.

- 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.

- <u>Upgrade materials:</u> 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.

- <u>Change design of at-risk components/system:</u> 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.

7. Controlling Habits

The direct control of human factors as outlined above is the most effective means to control human error. However, about 15% of human error is due to acquired habits. Some call these Behaviors, but that normally carries negative connotations. Many companies have effective systems for combating bad habits; these systems normally involve peer-to-peer observations and feedback (coaching), and these are many times labeled behavior-based safety management (which is a trademark phrase belonging to BST), or behavior-based reliability, or simply job-observations. A peer-observing-peer system, such as these, can reduce habit-based errors by about 70%.

8. Applying Human Factors to Risk Reviews and Root Cause Analysis

It is important to note that while not directly controlling human factors, the PHA/HAZOP (hazard identification and risk assessment) and the Incident Investigation management systems help to identify where and how human factor practices are necessary to control certain risks and help to identify weaknesses in human factor practices and implementations.

Risk Reviews (PHA/HAZOP, HIRA, JSA, etc.) – Addressing Human Factors during risk reviews can help identify gaps in all human factor categories since human factor categories are types of safeguards. This is fundamental for predicting where and why humans might make mistakes and for determining (qualitatively, at first) if the protection layers are sufficient if such errors occur and if not, what else is needed. Unfortunately, many organizations do not fully analyze for errors during all modes of operation, and so many (in some cases, most) of the accidents that start with a human error are not predicted, as they should be ***(See Chapter 9.1 of CCPS/AIChE, Guidelines for Hazard Evaluation Procedures, 3rd Edition, 2008*[9]*; and paper by Bridges, LPS/AIChE, April 2009, Optimizing Hazard Evaluations*[10]*.)*** This practice ultimately strengthens SOPs, human system interface, and most importantly ensures there are sufficient IPLs for scenarios unique to non-routine modes of operation, such as startup, shutdown, and online maintenance.

Incident Investigation/Root Cause Analysis (II/RCA) – II/RCA is necessary to learn from mistakes. Although all companies have an II/RCA system, many companies are lacking in the awareness of where human factors fit into an accident sequence. This leads to the II/RCA missing the human factor weaknesses that led to the human error and so the II/RCA may stop at the cause (and even root cause) being "operator error." Many companies also do not get nearly enough near misses reported (the ratio should be about 20 to 100 near misses reported per actual loss/accident ***(See CCPS/AIChE, Guidelines for Investigating Chemical Process Incidents, 2nd Edition, 2003[12]; and paper by Bridges, 8th conference, ASSE-MEC, 2007, Gains in Getting Near Misses Reported[13].)***

9. Closing

An organization implementing PSM (or similar programs such as, SMS or OSHA's 18001 for occupational safety) must develop management systems for optimizing human factors to control human error rates. As noted above, three potential sources for guidance for the chemical process industry are regulatory standards, such as the OSHA PSM regulation, the CCPS RBPS reference, and the CCPS COO/OD guideline. As a matter of closing this analysis, it is helpful to compare how well each of these documents address human factor implementation. The following is a rating scale that the authors have developed to gauge how well human factors are incorporated in these sources.

TABLE 5: DEFINITION OF HUMAN FACTOR RATING SYSTEM

Rating	Description
1	Human Factor is not specifically addressed
2	Human Factor is nominally addressed
3	Human Factor is partially addressed
4	Human Factor is mostly addressed
5	Human Factor is thoroughly addressed

The following table summarizes each document's (management system's) ratings for each human factor:

TABLE 6: HUMAN FACTOR RATINGS FOR PSM REFERENCE DOCUMENTS

Human Factor	OSHA PSM	RBPS Guideline	COO/OD (Component of RBPS)
Available Time	1	1	2
Stress/Stressors	1	1	2
Complexity & Task Design	1	1	2
Experience/Training	2	3	5
Procedures	2	3	2
Human-Machine Interface	1	1	4
Fitness for Duty	1	3	4
Work Processes & Supervision	2	4	4
Work Environment	1	1	1
Communication	1	3	4

As stated above, the OSHA PSM standard does not rate well for incorporation of human factors. It partially addresses them in the area of training, but only nominally at best in the other areas.

The RBPS guideline improves upon the coverage of human factors significantly compared to the US OSHA PSM regulation, particularly in the areas of:

- **Fitness for Duty (FFD)** – specifically by introducing the concept of sleep discipline and overtime limitations, but without specific guidance on limits and without recommended practices for controlling FFD
- **Work Processes & Supervision** – specifically by providing a great deal of emphasis in the areas of process safety culture and workforce involvement
- **Communication** – specifically by providing some (but not all) key communications rules to reduce human error, and by discussing the importance of shift turnover logs, but without enough detail on their content
- **Experience/Training** – specifically by providing a strong structure of the desired training program, albeit at a fairly high level
- **Procedures** – specifically by including most, but not all, of the best practices identified in this paper; the key items missing are the rules to have procedures written by future users of the procedures, and to conduct a hazard analysis of the consequences of human error in following the procedures

The COO/OD guideline further improves upon its parent book, RBPS, in most areas:

- **FFD** – specifically by addressing nearly all the key elements outlined in this paper. One main shortcoming is that it recommends API RP 755 as a guide for Fatigue Management, but this standard is terrible in that it fails to control fatigue that can occur during extended maintenance outages. Further, it does not cover all FFD issues, but rather focuses on fatigue. It would have been better to omit reference to the API RP 755 and instead reference the US NRC standard for FFD, 10 CFR 26. One major advantage of the NRC standard is that it includes the requirements for supervisors to be trained in and search for FFD deficiencies in staff coming onto the shift. A thorough management system for detection and the initial actions and follow-on actions is needed; 10 CFR 26 provides a lot of detail on what is needed.
- **Human-Machine Interface** – specifically by highlighting key DCS design features; however, much of the other factors described in this paper are not discussed.
- **Communication** – specifically by again including key (but not all) communication rules, and by providing specific details about the shift handover log.
- **Experience/Training** – specifically by providing a thorough, and properly detailed, overview of a strong training program.

Taken together, these two CCPS guidelines provide valuable advice on how to incorporate six (6) of the human factors into a PSM program, with notable exceptions in the areas of:

- *Available Time*
- *Stress/Stressors*

- *Task Design and Task Complexity*
- *Work Environment*
- *Procedures - poor/incomplete coverage of best practices*
- *Some gaps within the factors RBPS and COO/OD do cover*

This paper provides sufficient detail for implementing all 10 human factors so that companies following its guidance can be well on their way to building strong human factors elements within their PSM program.

9. References:

1. Swain, A. D., Guttmann, H. E., *The Human Reliability Handbook - with Emphasis on Nuclear Power Plant Applications*; NUREG/CR-1278, U.S. Nuclear Regulatory Commission, Division of Facility Operations, 1983.

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

3. Bridges, W., and Tew, R., *Human Factors Elements Missing from Process Safety Management (PSM),* 6th GCPS, AIChE, March 2010.

4. *Risk-Based Process Safety*, CCPS/AIChE, John Wiley & Sons, Inc.; Hoboken, NJ, 2007.

5. *Conduct of Operations and Operational Discipline*, CCPS/AIChE, John Wiley & Sons, Inc.; Hoboken, NJ, 2011.

6. *US FAA Advisory Circular* 120-42A (as part of ETOPS approval)

7. Bridges, W. G., Williams, T. R., “Effective Procedure Writing – A Two-Part Series (Part 1: Reducing Risk of Worker Errors; Part 2: Addressing Process Safety Management Requirements for Operating Procedures),” *Chemical Engineering Progress*, 1997.

8. Bridges, W., and Collazo-Ramos, G., *Human Factors and their Optimization,* 8th GCPS, AIChE, April 2012.

9. *Guidelines for Hazard Evaluation Procedures,* 3rd Edition, CCPS/AIChE, John Wiley & Sons, Inc.; Hoboken, NJ, 2008.

10. Bridges, W., *Optimizing Hazard Evaluations*, LPS/AIChE, April 2009.

11. Bridges, W., Lorenzo, D., and Kirkman, J., *Addressing Human Errors During Process Hazard Analyses*, CCPS Conference, AIChE, 1991 (also published in Chemical Engineering Progress May 1994).

12. *Guidelines for Investigating Chemical Process Incidents, 2nd Edition,* CCPS/AICHE, John Wiley & Sons, Inc.; Hoboken, NJ, 2003.

13. Bridges, W., *Gains in Getting Near Misses Reported*, 8th Conference, ASSE-MEC, Bahrain, 2008.

14. Della Rocco, P.S., et al., *The Effects of Napping on Night Shift Performance*, Federal Aviation Administration, U.S. Department of Transportation, 2000.

15. *Fitness for Duty Programs, Preamble, 10 CFR 26, U.S. Nuclear Regulatory Commission, Revised 2005.*

16. US Chemical Safety and Hazard Investigation Board (CSB), *Anatomy of a Disaster: Explosion at BP Texas City Refinery*, published 2006.

17. University of South Australia (UniSA), Adelaide Centre for Sleep Research, *SDA Fact Sheet - AT03*, 2006.

18. Hallbert, B.; Whaley, A.; Boring, R.; MCabe, P.; and Chang, Y.; *Human Event Repository and Analysis (HERA)*, NUREG/CR-6903, U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington, DC, 2007.

19. Bridges, W., and Clark, T., *LOPA and Human Reliability - Human Errors and Human IPLs*, 7th GCPS, AIChE, March 2011.

20. Bridges, W., and Thomas, H., *Accounting for Human Error Probability in SIL Verification Calculations,* 8th GCPS, AIChE, April 2012.

21. Bridges, W., *The Impact of Human Factors on LOPA*, 9th GCPS, AIChE, April 2013.

22. Bridges, W., and Tew, R., *Best Practices for Writing Operating Procedures and Trouble-shooting Guides,* 13th GCPS, AIChE, March 2017.

23. Bridges, W., *Proven Approaches to Ensuring Operators Can Respond to Critical Process Deviations in Time (Human Response IPL),* 13th GCPS, AIChE, March 2017.

24. Bridges, W. and Rhodes, W., *Everything you need to Know about Human Reliability and Process Safety,* 17th GCPS, AIChE, March 2019.

25. Bridges, S. and Bridges, W., *Abnormal Modes of Operation – A risk-based focus,* 16th GCPS, AIChE, March 2020