TEES | MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

20th Annual International Symposium
October 24-26, 2017 • College Station, Texas

Improving Barrier Effectiveness using Human Factors Methods

Dave Grattan PE, CFSE
aeSolutions
10375 Richmond Ave. Suite 800
Houston, TX 77042
dave.grattan@aesolns.com

Abstract

The Process Industry has an established practice of identifying barriers to credit as IPLs (Independent protection layers) through the use of methods such as PHA (Process Hazard Analysis) and LOPA (Layer of Protection Analysis) type studies. However, the validation of IPLs and barriers to ensure their effectiveness especially related to human and organization factors is lagging.

The concept of barriers as discrete onion layers comprised of administrative controls, alarms, instruments, mechanical devices, and post-release mitigation is highly idealized. Even worse it is misleading because it blinds us to the reality that all barriers are human. Further, this human base is often made up of small groups of people, comprised of operations, maintenance, and technical staff, with a management layer. The groups of people that maintain and manage all barriers is the most critical factor to ensuring good performance of those barriers in the threat path of a hazard scenario. The methods of PHA and LOPA as currently practiced are not addressing this issue. There is not even awareness of this issue, because the mantra to "ensure independence between protection layers" creates the illusion that barriers can be made independent.

The two related issues this paper will address are, (1) the human and organization impact on effectiveness of a single barrier, and (2) the human and organization impact on all barriers in the same threat path. The first issue can be addressed with established human factors and human reliability tools such as Task Analysis, coupled with a public domain human reliability model. The second issue is more complex and requires analyzing the groups of people that cross barrier types and can negatively influence multiple barriers.

The methods and concepts will be explained by considering the following barrier types, in a common threat path. The approach described in this paper has been in use for the past two years applied to actual barriers.

- Critical Alarm with Operator Response
- Safety Instrumented System
- Mechanical Pressure Relief Device

Demonstrating barrier effectiveness involves both qualitative and quantitative considerations. Demonstrating qualitative effectiveness is done by performing a Task Analysis to identify the degradation factors (human and organization) and degradation factor controls related to the barrier. Demonstrating quantitative effectiveness of the same requires use of a Human Reliability method. Neither of these approaches has been widely adopted in the Process Industry and so there exists a competency gap related to their use. However the need for these tools is evident by the incidents arising in industry due to human and organization factors.

Finally, documenting the results on a Bow-tie diagram (the left-hand side) will be demonstrated. Identifying leading process safety indicators embedded in the Bow-tie will be discussed.

Key Words

Bow-tie, Barrier effectiveness, Task Analysis, Human Factors, Human Reliability

Disclaimer

The following paper is provided for educational purposes. While the author has attempted to describe the material contained herein as accurately as possible, it must be understood that variables in any given application or specification can and will affect the choice of the engineering solution for that scenario. All necessary factors must be taken into consideration when designing hazard mitigation for any application. aeSolutions and the author of this paper make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of this document.

1 Introduction

This paper discusses system error and system failure related to barriers of the kind shown in the following three examples (all are taken from actual events).

1. A project is upgrading a legacy PLC to a modern safety PLC. The project is not creating a set of installation drawings to show the contractor how to wire the existing field devices to the new I/O points. Instead, the work will be directly supervised by the site electrical engineer. The potential for future problems is large. You could classify this as an organizational failure.

2. A console operator receives a high level alarm and interprets the alarm as false. The operator enters a notification to have the instrument checked. The tank overflows. You might be tempted

to call this “human error.” However, a more correct way to think about this is to understand the human factors that were behind the decision to interpret the alarm as false.

3. Operations systematically applies a bypass to a high level interlock during start-up to avoid tripping. Following one start-up, the operator forgets to remove the bypass. Later, a high level condition occurs and places a demand on a downstream safeguard (independent automatic pump-out), which operations always run in manual mode due to a bad design (insufficient suction head), and is therefore unable to respond. An incident occurs. In this case, two independent barriers in the same threat path were defeated. Operations gets blamed. Later it was learned: The bypass was not identified during engineering design. The bypass step was added to a procedure to avoid the need for MOC when using it. In the rush to add the bypass step, the restoration step was omitted from the procedure. A log is kept, but the bypass is not audited. Operational bypassing is based on the “honor system.” The reality is this is an example of normal work practices producing a sneak path around multiple otherwise independent barriers. Latent conditions were allowed to persist because they were not identified and corrected by the Organization.

There are methods and tools available to identify, classify, and correct these types of system errors before something bad happens. That is the subject of this paper.

1.1 What is a Barrier?

A barrier is a safeguard or IPL (independent protection layer) used to stop an accident sequence. Barriers are typically identified in process hazard studies such as PHA (Process Hazard Analysis) and LOPA (Layer of Protection Analysis), as well as other methods that may be used by front-line workers to identify and control hazards. Some examples of barriers include,

- Piping and piping components (valves, blinds, etc.)
- Process (purges, etc.)
- Alarms
- Interlocks
- Safety Instrumented Systems
- Procedures/ Administrative controls (SOP, tags, locks, etc.)

Barriers are fundamentally human (i.e., they rely on people). For practical analysis a barrier can be thought of as composed of both hardware and human/ organization (see **Figure 1**). PHA-LOPA are suited for identifying barriers and their associated hardware. However, PHA-LOPA and its derivatives, are not human factors methods (and were not intended to be). For example, a PHA only evaluates states and conditions (e.g., is the alarm configured as priority, or, what-if this step in the procedure is omitted?) as opposed to behavior (e.g., how will the console operator interpret the alarm, or, how likely is the operator to skip that step and why?). And LOPA is primarily a hardware reliability calculation, which averages out human and organizational factors. In other words, LOPA may consider human error, however it treats human error as random, which can sometimes lead to nasty surprises, especially when the expectation is a LOPA target of 1e-4 or lower.

Human factors and reliability methods are well established, see for example [17]. But the Process Industries has yet to embrace them. For high hazards with low tolerable risk targets, now is the time.

Section 2 looks more closely at some of these issues and discusses the tools of human factors and human reliability. **Section 3** discusses human factors specifically in the context of barriers.

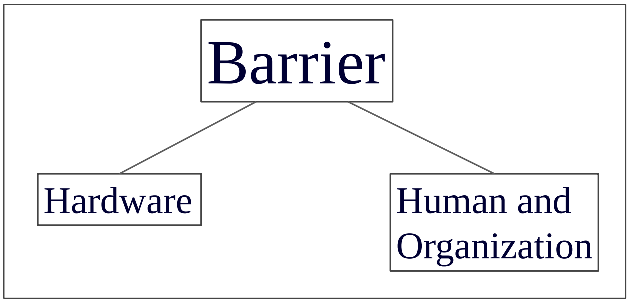

Figure 1. A Barrier is Composed of Hardware and Humans.

2 Top 10 Meta-Human Factors

Everybody has their favorite Top 10 human factors list (e.g., fatigue, task complexity, time constraints, quality of procedures, fitness for service, communication, etc.). This section will take a step back, and look at the Top 10 human factors of human factors (Meta-human factors).

2.1 Defining Human and Organizational Factors

To many leading practitioners, it is not obvious how to even define what human factors is, including what makes it unique from other disciplines [1]. This represents a significant hurdle to having organizations take up human factors type work.

The following definitions will be used from this point onward.

2.1.1 Human Factors v. human factors

Human Factors (upper case) is a science as defined in **Table 1**. When written in lower case, human factors is used more colloquially to mean all the things that could affect human performance (e.g., what one ate for breakfast) [2].

Table 1. Human Factors is a Science, adapted from [2]

Alarm Management	QRA
Automation	Risk Perception
Crew Resource Management (non-technical Team work)	Safety Culture
Design & Installation	Situation Awareness
Fatigue, effects of	Stress, effects of
Human-machine interaction	Codes and Standards
Operating and maintenance Procedures	

2.1.2 Ergonomics

The terms ergonomics and human factors are often used interchangeably.

However, for those wanting a little more depth in the definition, ergonomics can mean anthropometry, the study of the measurements of the human body to design an optimal work environment (console height, valve height, chair dimensions, etc.). Anthropometrics uses statistical averages of human height, weight, etc. (adjusted for the culture of interest) to inform the design process.

2.1.3 Human Reliability

The practice of Human Reliability refers to quantifying human error in the context of Human Factors. The quantitative unit of human error is the HEP (human error probability), defined as follows.

$$\boxed{\text{HEP} = \frac{\text{Number of errors occurred}}{\text{Number of opportunities for error}}}$$

The HEP is based on a task, or a sub-task. For example, step 23 of Procedure 2510.11 calls for the operator to open a valve (in this example opening this valve is a safety critical sub-task of the procedure). The procedure is executed weekly. If the operator successfully performs step 23 over the course of two years the HEP will approach 1e-2 (this is the average of the population of operators doing the sub-task).

Human Reliability Analysis (HRA) is an established field of practice that grew out of the Nuclear industry, where it is still practiced today. There are many HRA methods available for use [3]. One of the newer methods called “Petro-HRA” will be discussed below.

Attempting to put a number to human error via HRA forces one to look at the Human Factors associated with the task (by applying a Task Analysis). This qualitative aspect of HRA to identify and fix Human Factors issues is the primary benefit of the analysis. The estimated HEP is a secondary benefit that could, for example, be used to refine a LOPA calculation.

2.1.4 Organizational Factors and the Swiss Cheese Model

Human Factors arise at all levels of a system hierarchy, from the front-line worker to management, this includes the Organization, and is the basis of the term Human and Organizational Factors [4]. The HFACS taxonomy (The Human Factors Analysis and Classification System) provides a practical tool to identify, classify, and correct Organizational factors [5]. HFACS defines the holes in Reason's Swiss Cheese Model [6], making it useful to the practitioner. HFACS can be paired with Task Analysis as a predictive tool, or can be used in incident investigations to get beyond "human error."

LOPA (Layer of Protection Analysis) looks like the Swiss Cheese model. But LOPA is not the Swiss Cheese model (because LOPA treats "human error" as a cause, instead of a consequence). As mentioned above, LOPA is primarily a hardware reliability model that misleadingly averages out human and organizational error. The methods of PHA-LOPA are not enough. Human Factors methods are needed.

2.2 Nature of "Human Error"

Human Factors thinking recognizes "human error" as resulting from system (a.k.a., systemic or systematic) influences (e.g., poor Human Factors). "Human error" is a consequence not a cause. This is a significant shift in thinking from current practice of PHA-LOPA (see **Figure 2**). How many jokes have we heard about "Mal" the operator making a catastrophic error?

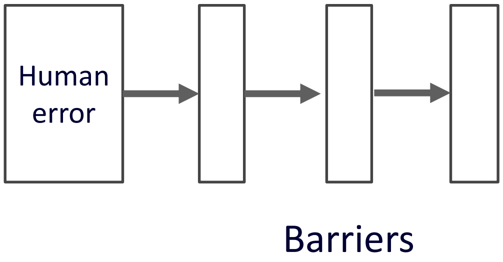

Figure 2. PHA-LOPA viewpoint of "Human Error" as a Cause

We shouldn't stop at the individual that committed the error, instead we should look for the system factors that could make the error more likely (see **Figure 3**). The tool for this is Task Analysis. Treating "human error" as a consequence allows a more accurate interpretation of the human as an important barrier to prevent the sequence of events. And it explains why the vast majority of time operations go as planned (i.e., people are the resilient component working in a less than perfect system).

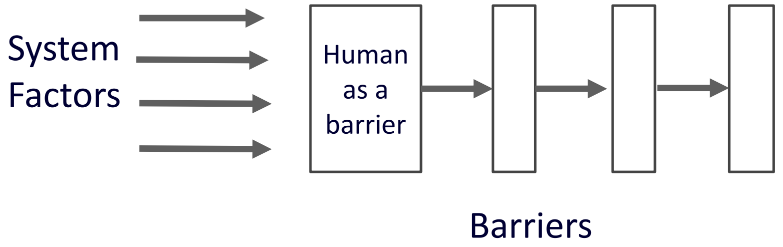

Figure 3. When “Human Error” is viewed as a consequence (not a cause), the human becomes an important Barrier in the sequence of events [4]. “Human error” is placed in quotes when we recognize this fact [21].

System factors not only act on front-line workers, they also act on barriers as shown in **Figure 4**. **Figure 11** shows for example the organizational links involved with barrier management that will impact barrier effectiveness. **Figure 4** is an adaptation of Johnson’s Three Level Model of Accidents [7] that shows system factors imposed on barriers in a common threat path. As previously mentioned, the HFACS method can be used to identify, classify, and correct these system factors. Note that **Figure 4** is an alternate representation of Reason’s Swiss Cheese Model [6] in which the arrows (system factors) go around the barriers instead of through holes in them.

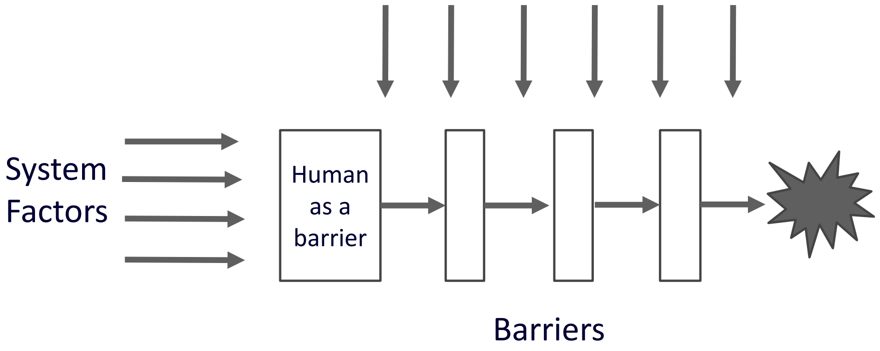

Figure 4. System factors can create sneak paths around barriers to the undesired outcome.

2.3 When do Human Factors and Reliability require a closer look?

Time and money constraints (e.g., “ETTO” – Efficiency-Thoroughness-Trade-Offs [16]) dictate a selective approach to using Human Factors and Reliability methods applied to barriers. Certainly the highest hazards with the lowest tolerable risk targets are good candidates for these methods. Claiming LOPA targets 1e-4 or lower without considering human and organizational factors leaves one blind to system effects. High hazard scenarios with significant human components either as the initiating event or barrier are also good candidates. Barriers in the same threat path that utilize a common technology (e.g., BPCS and SIS) are good candidates. LOPA scenarios with one barrier are good candidates for these methods.

An owner operator will often suspect weak spots may exist in barriers or in other safety critical tasks. For example, normal work practices involving work-arounds, or re-design that could unknowingly impact a barrier's performance. This would be another source for more detailed study from a human factors perspective.

2.4 The Law of Medium Numbers

Note: This subsection discusses the validity of attempting to quantify barrier performance recognizing that all barriers are fundamentally dependent on humans and their organizations.

It was noted above that "human error" which is a result of system effects does not average out in a standard hardware reliability calculation (e.g., LOPA, SIL calculations, etc.). It is tempting to lump systematic error with random hardware failure to produce a reliability number and believe all is well.

The issue is the Law of Medium Numbers [8] as shown in **Figure 5**. The term Law of Small Numbers has also been used to describe the same phenomena [9].

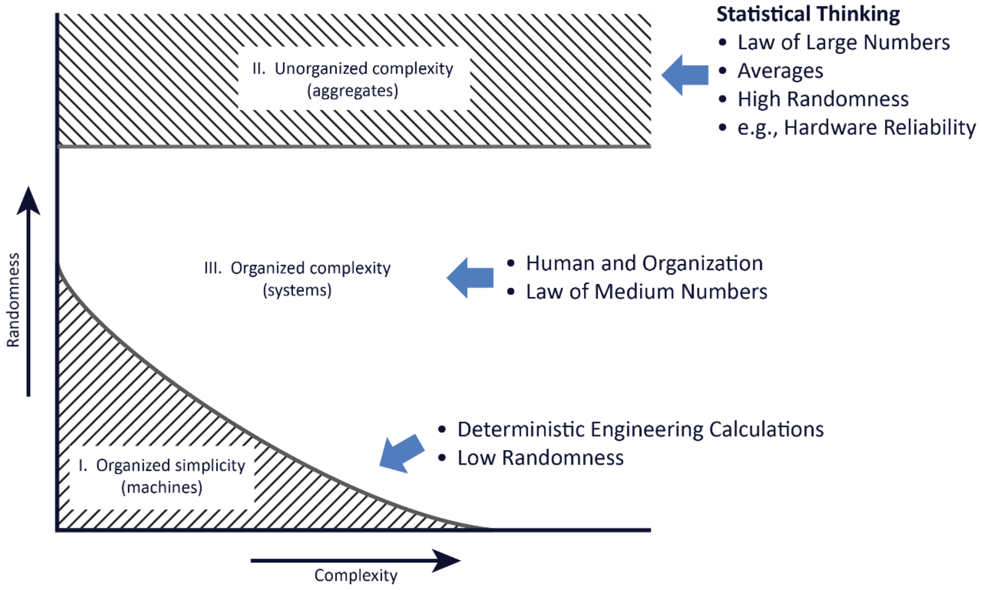
Statistical Thinking
• Law of Large Numbers
• Averages
• High Randomness
• e.g., Hardware Reliability
II. Unorganized complexity (aggregates)
III. Organized complexity (systems)
• Human and Organization
• Law of Medium Numbers
I. Organized simplicity (machines)
• Deterministic Engineering Calculations
• Low Randomness
Randomness
Complexity

Figure 5. The Law of Medium Numbers adapted from [8]

Humans and their Organizations belong to the large middle region labelled "organized complexity." Humans and their Organizations are too organized for statistics to apply (averages will be deranged [7]), yet too complex for determinism (LOPA is a deterministic equation). The organizational groups involved in barrier management for example, from **Figure 11**, make up small or medium numbered systems. Is the statistical mathematics used to quantify barrier reliability and availability a worthwhile effort given the large uncertainty?

The result of the Law of Medium Numbers is derived from a frequentist interpretation of probability, which says probability is a property of the physical world (i.e., nature), and you can't do anything to change it. Averages are misleading and occasional extreme outcomes will occur. Bayesian probability is based on the uncertainty we have about an outcome (i.e., how much information we have about the situation), which allows us to bend the Law of Medium Numbers in our favor if we can evaluate and fix the systematic error associated with small/ medium numbered systems. In essence we are reducing the randomness associated with an outcome in our favor. And since the LOPA calculation is deterministic, it makes the calculation (more) valid.

Back to hardware. Hardware reliability calculations miss the point when it is claimed they are conservative by including system (i.e., systematic) error. System error is either present or not, and in a Bayesian sense the probability of failure is either close to 1 or 0, respectively. It does not average out. And if it is present, it will dominate the result of any reliability or availability calculation.

The point here is not to argue whether a certain failure is classified as random or systematic. That is a deep question of nature and philosophy. Rather the point is, that medium (or small) numbered systems will occasionally produce extreme results that can't be predicted with standard statistical methods.

The advantage that HRA (Human Reliability Analysis) has over hardware reliability statistics is the use of task analysis to identify and fix Human Factors, and to estimate the human error probability based on those Human Factors.

Human Reliability also gives us the ability to place an error rate on a LOPA calculation. It is the contribution from system error (human and organizational factors). This is discussed in the next section.

Some statements of the Law of Medium Numbers:

- Expect extreme outcomes on occasion (e.g., a failed barrier).
- Don't put too much trust in hardware reliability calculations.
- It would be better to find and fix your Human Factors than to refine a reliability calculation to the nth degree.
- Reliability calculations breed over-confidence in system safety.
- Confidence intervals used for reliability data are more accurately described as "over-confidence" intervals.

2.5 Human Performance Limiting Values

HEP (human error probability) was defined above. What kind of values should we expect for the HEP? How low can a HEP be? What is the uncertainty?

Robert Taylor recently published his database of empirical human error probabilities that show several orders of magnitude difference can exist between nominally identical error modes [10]. And that this difference is dependent on the Human Factors specific to the situation. This is why you should never just pull data from a human reliability data table (even generic ones used in LOPA), without looking at the Human Factors. You are gambling with the Law of Medium Numbers if you do.

Human performance sets the achievable level of safety provided by a barrier, or a set of barriers in a common threat path. This is because all barriers are fundamentally human, and exist within the small and medium numbered systems of a project or an operating facility.

So what are the human performance limits of a barrier?

Recognized and published human performance limiting values can be found in the literature, for example, in Kirwan [11] as follows,

- Single operator carrying out task(s) on plant .. 1e-4
- Operators carrying out task on plant.. 1e-4 to 1e-5
- Control room based team.. 1e-5

These are HEP (human error probabilities). These are performance limits. Often human error rates for a specific task are found to be much higher than this.

To put this in perspective, one would need data for three years performing a daily task error free to demonstrate a HEP of 1e-3. One would need 30 years of data performing a daily task error free to demonstrate a HEP of 1e-4. One can easily convince themselves of the difficulty of achieving such low numbers by thinking of tasks in their own personal lives and the reliability in which they perform them. For example, I can think of a half dozen tasks that I perform to 1e-3. I can think of very few tasks that I've performed that approach 1e-4, one of which is not driving off from a gas pump with the hose still attached (an accident that sometimes happens in the process industries). Another is not blindly driving through an established red light (a potential hazard in the rail industry). I have on occasion driven through stop signs and "run" red lights.

For this reason, as a human reliability practitioner, one would be hesitant claiming as low as 1e-4 for a task performed by one person even with good human factors. So what is the implication of this for the LOPA calculation? Or a barrier, which potentially depends on dozens of people during its lifecycle to be effective? It is this: It is very difficult to achieve 1e-4 performance (much more 1e-5 or 1e-6), and it is not reasonable to accept a LOPA calculation of 1e-4 or better without verifying the human factors for each of the barriers in the threat path.

2.6 Human Factors and Psychology

How humans think represents a significant component of determining human barrier effectiveness. The human mind can unknowingly produce systematic biases related to judgment and decision making.

The concepts presented here are most relevant to human barriers such as critical alarm and SOP (standard operating procedures), but also apply anytime decisions or choices are made (i.e., normal work). Specifics will be discussed later. An introduction is provided here.

Several decades of research and thinking on how humans think is presented in the seminal work by Daniel Kahneman [9]. Ron McLeod in his book [12] first discussed the many implications of thinking fast and slow for the process industry.

Fast thinking, also called System 1, is our auto-pilot in which we spend the vast majority of time. Most of our decisions are made using System 1 thinking, which our conscious self is not even aware of. Most of the time our decisions turn out well. The problem is, System 1 thinking uses short-cuts and heuristics that can (sometimes) produce systematic error in our decisions. For example, substituting an easier question to answer for a harder one is a common heuristic humans utilize, without being aware it is happening. System 1 thinking happens from the board room to the PHA room to front-line operations.

Slow thinking, also called System 2, is our conscious aware self. System 2 is lazy. It is content to let System 1 do all the work. It only becomes engaged when made to (e.g., via cognitive strain such as surprises in the environment). System 2 is more logical and not as susceptible to systemic bias that System 1 is. But it takes effort to turn it on.

There are two design implications related to barrier effectiveness that involve System 1 and 2 thinking and impact Operation's awareness of barriers.

1. There is a principle associated with System 1 thinking called WYSIATI (What-you-see-is-all-there-is) [9]. Humans make decisions based not only on the information they have in front of them, but also on information we fabricate to fit the narrative in our minds to confirm what we already believe. Our System 1 will take sparse (and even false) information and create a flowing narrative to prove what we are trying to confirm. And System 2 is too lazy to stop it. Our designs must not only be compatible with System 1 thinking (because this is where we spend our day), they should also anticipate the short-cuts and heuristics that Operators will make. Translated this means:
    - Designs that require System 2 thinking run the risk of being ignored if there is an easier way to take. This is the principle of least effort that applies to physical effort (e.g., following procedures) as well as mental effort (e.g., reading). Examples include unnecessarily long or poorly written procedures, complex or cluttered graphics, or warning signs that will be read (cognitively) once and never read again. It takes effort (System 2 thinking) to read and comprehend. And System 2 is lazy. Our designs must work with System 1.
    - We must give Operations all the information they need to make good decisions (System 1 will fill in any missing pieces as a short-cut) in an easy to interpret presentation (e.g., 'at-a-glance' display). Operators should not have to work for information.

- Where we can, we should take away the need for the Operator to interpret information (i.e., remove the potential for short-cuts and biases). An example of this applied to critical alarm response is given in a later section.
- Under “threat-stress” System 1 goes into overdrive and makes the need for good design using these concepts even more critical.

2. The so far elusive goal of Human Factors Engineering is this:

   To jolt the operator out of Type 1 thinking into Type 2 thinking, just before he is about to make a catastrophic mistake.

   For example, say an operator is staring blankly at a sign that states ‘Reactor Valve A’ getting ready to open that valve, but that the operator intended to be on ‘Reactor Valve B’. As the operator reaches for the handle a small jolt of electricity or heat or something shocks him, and an audio output declares “You are on the wrong valve!”

   To achieve this takes some serious human factors engineering and technologies that probably do not exist yet, or not available to general consumer.

2.7 Task Analysis

Task analysis methods have many applications. For example, Hierarchical Task Analysis (HTA) can be used for task allocation, interface design, training design, procedure design, etc. [13]. The extension of HTA that is of interest for barrier effectiveness is “error assessment and prediction.”

At its heart, task analysis is about observing the way people work, i.e., observing their behavior. If the barrier of interest is an SOP (standard operating procedure), the task analysis would include watching the SOP be performed. If the barrier of interest is a hardware barrier (e.g., a rupture disc), the task analysis would include observing how work is done related to managing that barrier. This could involve interviewing and visiting shop areas.

There is no magic checklist or guidance document for performing a good task analysis. To be good at doing task analysis, the facilitator has to know a lot of Human Factors. There are no short-cuts. Practice obviously helps. But the key is to knowing Human Factors and how they can impact the work being done.

Figure 6 shows a generic work process for barrier task analysis.

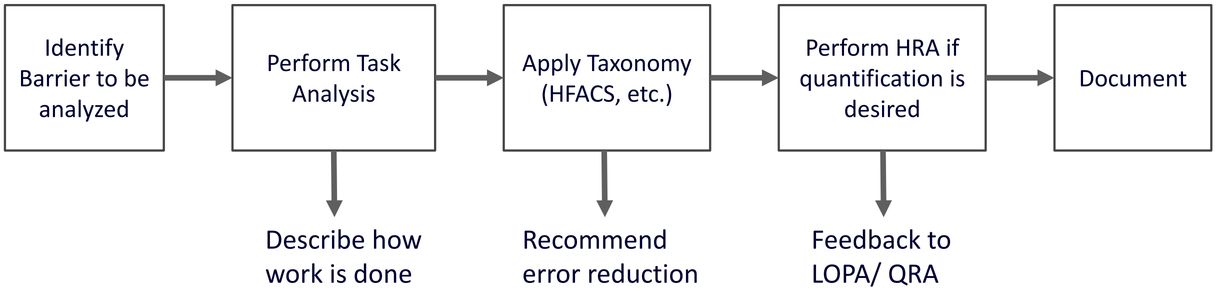
Identify Barrier to be analyzed
Perform Task Analysis
Apply Taxonomy (HFACS, etc.)
Perform HRA if quantification is desired
Document
Describe how work is done
Recommend error reduction
Feedback to LOPA/ QRA

Figure 6. A Generic Work Process for Barrier Task Analysis

2.8 Human Error Taxonomies and Accident Models

Task analysis should always be performed with a human error taxonomy to help guide the facilitator on the kind of errors that are possible, and so that recommendations can be made to reduce the likelihood of the identified error modes. SHERPA [14] and HFACS [5] are two good "human error" taxonomies.

The simplest human error taxonomy is:

- Error of omission – Not doing something.
- Error of commission – Doing something the wrong way.

The same "human error" taxonomy should be used for both predictive and investigative studies to leverage the full benefit. See **Figure 7**.

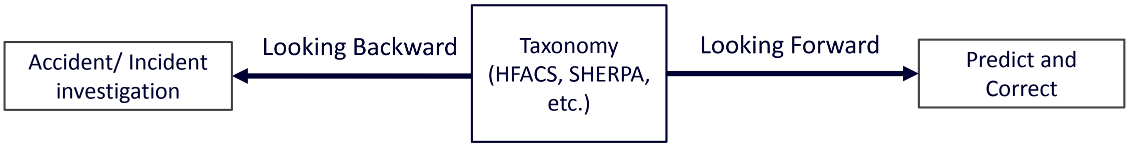
Accident/ Incident investigation
Looking Backward
Taxonomy (HFACS, SHERPA, etc.)
Looking Forward
Predict and Correct

Figure 7. The same Taxonomy should be used for both investigative and predictive studies.

Making good recommendations to reduce human error is a skill that comes with practice and a broad knowledge of Human Factors. Simply recommending better procedures or more training is not going to get us where we need to be, because all procedures could be improved, and everyone could use more training. Two references that I've found useful for helping to identify bad human factors are Don Norman's discussion of design induced error [15], and Robert Taylor's discussion of human error syndromes [10].

Reason’s Swiss Cheese Model [6] is the current gold standard of accident causation models used in the process industries. However, there are two relatively new accident models STAMP [7] and “Safety 2.0” [16] that can add to the discussion of barrier integrity management.

2.8.1 SHERPA (Systematic Human Error Reduction and Prediction Approach)

SHERPA was originally developed for the nuclear industry [17] but has widespread application in other domains. The SHERPA taxonomy applies to active errors (as opposed to latent conditions) committed by front-line workers (operations, maintenance, etc.). It is well suited for pairing with a human reliability technique such as Swain and Guttmann [18] for which a large part of the data set applies to front-line action errors.

Five types of errors are classified: Action errors, Checking errors, Retrieval errors, Communication errors, and Selection errors.

2.8.2 HFACS (Human Factors Analysis and Classification System)

HFACS was originally developed for aviation [5] but has extended its application into many industries including the process industry. HFACS was created to fit Reason’s Swiss Cheese accident model [5]. The ability of HFACS to describe both active (i.e., front-line) errors as well as latent conditions (systemic weaknesses in the organization that manifest themselves at the worst possible time) makes HFACS particularly appealing to use.

The four layers used in the HFACS taxonomy are (moving from front-line worker to organization): Unsafe acts, Precondition for unsafe acts, Unsafe supervision, Organizational influences.

2.8.3 STAMP (Systems-Theoretic Accident Model and Process)

STAMP is a systems theory model that uses the concepts of emergence, hierarchy, and constraints [7]. Safety is an emergent property of the system (hierarchy), as opposed to a component property of a device (e.g., like reliability). Safety constraints must be placed on the barrier for it to remain effective, and feedback is needed to monitor if the safety constraints are being broken.

As a systems model STAMP gives us the basis for why feedback on barrier performance is needed. Without feedback, how do we know the barrier is effective? Even *one* incident related to barrier effectiveness is important because of the extremely low probabilities assumed by LOPA (i.e., 1e-5 or 1e-6) [7].

Figure 8 represents barrier effectiveness as a control problem.

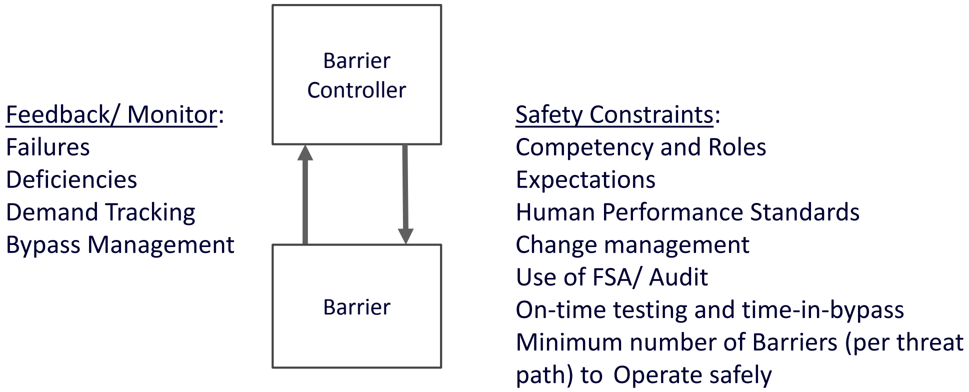

Figure 8. STAMP treats Barrier Effectiveness as a Control Problem [7]

2.8.4 SAFETY 2.0

Hollangel's Safety 2.0 [16] features the concept of Normal Accident Theory [19] as a means to explain catastrophic incidents in otherwise safe systems and processes. In systems utilizing the defense-in-depth concept (e.g., LOPA), single failures do not cause accidents [20]. What "causes" (there is no cause-and-effect in Safety 2.0, but something called Functional Resonance which sits between classical cause-and-effect and stochastic randomness) multiple protection layers to fail is normal work practices (i.e., the work-arounds, re-designs, ad hoc fixes, etc.) that sometimes combine in the worst way at the worst possible time to cause an accident. This is the basis of Hollnagel's Functional Resonance Accident Model (FRAM).

Normal work practices that degrade barriers are insidious because they are not viewed as a "change" (i.e., under change management). Human Factors methods such as Task Analysis should be used to discover normal work practices that can degrade barrier effectiveness.

2.9 Understanding the Limitations of LOPA

This section will summarize points made earlier about the limitations of LOPA. LOPA excels at defining the barriers an organization intends to rely upon to reduce process safety risk. LOPA is a semi-quantitative method. But it is misleading when trying to achieve such low risk targets (i.e., 1e-4 and lower). This reasoning is based on two arguments:

1. From a human reliability perspective it is *very* difficult to achieve 1e-4 performance or lower.
2. The Law of Medium Numbers deranges averages [7], such that we should expect extreme outcomes occasionally (i.e., incidents or accidents).

2.9.1 LOPA (and PHA) are Not Human Factors Methods

Procedural PHA, Human Factors checklists, and IPL validation checklists are not Human Factors methods. These tools look at states and conditions. Human Factors methods look at behavior. And looking at how people and organizations behave with respect to the barrier is the only way to ensure barriers are being managed effectively.

2.9.2 LOPA assigns "human error" as a cause (initiating event)

The limitation here is that by treating the front-line worker as the cause of potential accidents, we miss the opportunity to improve the system factors that affect the front-line worker's performance. For safety critical tasks (i.e., those that "go" to LOPA) performing a Task Analysis is the correct way to analyze those scenarios.

2.9.3 LOPA incorrectly averages out system error and failure (human and organizational factors)

Process safety people are in the prediction business. The LOPA calculation is a prediction of the likelihood of an undesirable outcome. In a Bayesian (statistical) sense, the more information we have about a system, the less uncertain we are about the prediction we make for the likelihood of an event. Evaluating the Human and Organizational Factors associated with a LOPA scenario is the primary way to increase the information we have about barrier performance related to the LOPA calculation, so as to reduce the uncertainty of said calculation.

2.9.4 LOPA is not the correct tool for achieving risk targets of 1e-4 or lower

LOPA is not an adequate tool for analyzing risk targets on the order of 1e-4 or lower. As discussed above, achieving human error probabilities approaching 1e-4 even for simple tasks is very difficult to do. Barrier effectiveness which depends on multiple groups of people is much more complex and to expect such low targets being met without putting in the Human Factors work is unrealistic.

LOPA uses independent generic credits in series to achieve 1e-4 or lower. Won't this work? The Law of Medium Numbers says "no." In organized but complex systems such as those made up of humans that design and manage barriers, extreme outcomes (e.g., catastrophic failure) are to be expected. This is a mathematical certainty; therefore the 1e-4 or better numbers are misleading (as discussed above the Bayesian view of probability allows us to bend the Law of Medium Numbers in our favor).

Accident Theorists recognize 5e-7 as the mythical performance limit beyond which no socio-technical system (i.e., human and technology) can cross [21]. However, to even approach this limit one must invoke Normal Accident Theory [22], which states that accidents are caused by normal work that sometimes goes wrong. Normal Accident Theory is a key component of Hollnagel's Safety 2.0 [16] along with the concepts of Work-as-imagined v. Work-as-Done, ETTO (Efficiency-Thoroughness Trade-Offs), and Resilience, to explain why work mostly goes right, but sometimes can resonate out of control and produce catastrophic accidents. LOPA is an inadequate tool for addressing any of these factors.

2.9.5 The Illusion of Independence

Normal Accident Theory [19] reveals the illusion of independence. Multiple barriers in the same threat path are never independent. The process systems we work with are too complex and too physically coupled. Psychological dependence between barriers is another factor.

Psychological and human dependency have a far greater impact than what is typically estimated for hardware dependence (e.g., using the Beta factor method). Estimating a Beta factor is another example of only looking at states and conditions. This time related to the hardware design. But for LOPA targets of 1e-4 or lower, human dependencies affecting behavior become the controlling factor in estimating likelihood of an event.

Human Reliability methods incorporate human dependency models. Much of human dependency is psychological, based on System 1 thinking which as we have seen is prone to error in judgements. For example, two barriers in the same threat path become psychologically coupled in the mind of a person just by being aware of them.

Operations is the obvious group whose influence touches every barrier in a common threat path. Maintenance touches all barriers, but often separate crafts are involved. The same PHA-LOPA team will identify and specify all the barriers in a common threat path. Engineering design of the barriers is mostly done by different teams. Decisions to accept or reject barriers, and budgets for barrier implementation are often made by the same managers. All of the decisions and choices made regarding barriers by any person or group are subject to the bias of System 1 thinking.

2.9.6 LOPA does not accurately represent the Swiss Cheese Accident Model

By treating the Human (i.e., Operator) as the cause (i.e., initiating event) in a LOPA scenario, we are completely missing the precursors and latent conditions that negatively influence operator performance in making an error. We should keep the LOPA method, but recognize its limitation with respect to Human Factors.

2.9.7 LOPA creates Decoys that consume resources that could be better spent elsewhere

The classic LOPA decoy is an ASME rated relief device properly sized and specified, and in clean service, that cannot by itself close the LOPA gap. Any large facility will have at least one or two of these, especially when the LOPA target is 1e-4 or lower. If an ASME relief device was not enough to adequately protect a pressure vessel, the ASME Boiler and Pressure Vessel committee would be taking action. Instead, additional interlocks, alarms, and controls are added ad hoc to close the phantom risk gap, stealing resources, adding complexity, and making us less safe.

Other LOPA decoys include:

- Arguing whether to sum causes or not. It doesn’t matter. Considering human factors, the level of safety achieved by, for example, SIL 1 versus SIL 2 is practically negligible.

- Arguing one versus two BPCS credits. You would be safer performing a human factors FMEA and take two BPCS credits versus blindly claiming one BPCS credit.
- Arguing over any other generic IPL credits. For the same reason. You are gambling with the Law of Medium Numbers if you don't evaluate your human factors.

2.10 Human Reliability Methods

The Law of Small/ Medium numbered systems (e.g., humans and their organizations) tells us to expect extreme outcomes (e.g., incidents such as a failed barrier). There is no causality here, there is nothing to explain, that is just the way nature is. From this perspective, we could say quantitative estimation of likelihood (via SIL calculations, LOPA, HRA, QRA, or whatever method you want to insert) is wasted effort, because the occasional outliers derange the statistical averages. Enter Thomas Bayes, the 18th century English preacher and mathematician. Bayesian probability allows us to bend the Law of Small/ Medium numbers in our favor when we reduce the uncertainty in our estimate by accounting for (i.e., identifying and fixing) human and organizational factors. HRA (human reliability analysis) combines Human Factors review and quantitative estimation into a single methodology.

2.10.1 HRA Methods Discussion (General)

There are a myriad of HRA methodologies, some public, some proprietary, as evidenced by the veritable alphabet soup of acronyms associated with the methodologies.

The Health and Safety Executive (HSE) in the UK considered that it would be useful to be up to date with developments in the field of quantitative HRA methods and to have knowledge of the capability of the tools and an understanding of their strengths and weaknesses, to improve consistency, and determine acceptability of their use [3].

To sort this out, in 2009 the HSE published a review of 72 HRA methods that were "potentially relevant to HSE major hazard directorates." Of the 72 potential HRA tools, 17 were considered useful for major hazard directorates [3].

THERP (Technique for Human Error Rate Prediction) [18] and SPAR-H (Standardized Plant Analysis Risk-Human Reliability Analysis) are two of the 17 methods considered to be useful by the HSE.

2.10.2 HRA Methods Discussion (Detailed)

The basic idea of quantifying human error for a given task is shown in **Figure 9**.

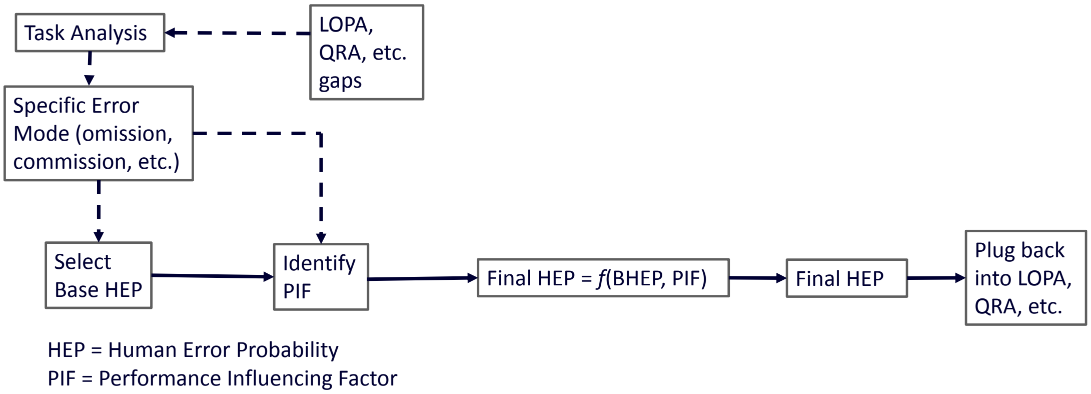
Task Analysis
LOPA, QRA, etc. gaps
Specific Error Mode (omission, commission, etc.)
Select Base HEP
Identify PIF
Final HEP = *f*(BHEP, PIF)
Final HEP
Plug back into LOPA, QRA, etc.
HEP = Human Error Probability
PIF = Performance Influencing Factor

Figure 9. Basic Work Flow of HRA

Some Human Factors have an obvious impact on the base HEP, for example, fatigue. But trying to quantify that impact can be difficult. Many of the HRA methods multiply a string of PIF together to get the final HEP. This often produces a HEP > 1.0 (for which correction factors must be applied). This weakens the confidence in the methods.

Another limitation is that the HRA methods have a fixed number of PIF that can be used in quantification (e.g., SPAR-H uses 8 PIF) so that the method tells the analyst what is important. Typical PIF that are used to calculate the final HEP number include fatigue, training, quality of procedure, task complexity, time pressure, experience level, etc. All of these are important, however, these are the most obvious human factors. For example, how does HRA account for inexperienced people? The answer is to expect more errors, but you probably already knew that. Fix what you already know. And then look for what you don’t know.

If only 8 PIF (for example) can be quantified into the final HEP, this means thousands of human factors are not. This also weakens the confidence in the estimate that HRA produces.

But don’t let this discourage you from using HRA. The clear value in performing HRA is Task Analysis, which does not limit the analyst to evaluating only 8 human factors (for example). Try to find what you don’t know and fix it.

2.10.3 <u>THERP</u>

The THERP method created by Swain and Guttmann [18] is a monumental achievement of human reliability science. It is the foundation of all future HRA methods that came after. It has never been updated because the method is so comprehensive, complete and thorough. It has weaknesses of course, but any serious practitioner of HRA will have read “The Handbook.” Some may consider it dated, a first generation method. But it is still widely used today, and its influence cannot be denied. The baseline HEP data for any HRA method even today comes from “The Handbook.”

THERP is considered a deconstructive method, i.e., it allows an analyst to break down a task in great detail. The method itself grew out of estimating the reliability of *manually* assembling nuclear bombs in the 1950's and 1960's [23].

THERP can be used to model:

- Operator error as an initiating event
- Operator response to abnormal condition
- Failure to restore safety systems following ITPM (inspection, test, preventive maintenance)

"The Handbook" is free on the U.S. NRC website:
https://www.nrc.gov/docs/ML0712/ML071210299.html

2.10.4 Petro-HRA

At the other end of the age spectrum is Petro-HRA, a relatively new HRA method [14]. Petro-HRA is the result of a Norwegian research and development project. The starting point for developing the Petro-HRA method was SPAR-H (which was created to improve THERP), because SPAR-H was identified as the most promising method to apply to the oil and gas industry [24].

Petro-HRA represents the best current thinking applied to HRA in oil and gas. The methodology was created with task analysis as a core component [25]. The guidance document provides a lot of detail of how to conduct a task analysis [14], that alone makes the document worthy of study.

Petro-HRA was written to analyze operator response to abnormal condition [14].

2.10.5 Action Error Analysis (AEA)

The AEA method was formally published in 2016 by Robert Taylor [10] after decades of development. The AEA offers several benefits over traditional HRA methods (which are written for the nuclear industry with regulatory requirements to include Human Factors and Reliability and have a large overhead):

1. It avoids the problem of the HEP exceeding 1.0 by summing "special error causes and influences" in lieu of multiplying PIF. Because Boolean OR gate math is used, the intersections can be subtracted and the summation can never exceed 1.
2. It comes with its own human error data set and influencing factors. The method has been tested and validated on actual plant operations.
3. Most importantly the method is written for safety critical tasks performed in oil refineries, petrochemical, and chemical plants. The method is low overhead. It is designed to be fast and efficient, capable of producing high value on a small budget.

4. The qualitative treatment of human error causes and “syndromes” is a very practical and useful assessment.

3 Human Factors Methods for Barriers

It is advantageous to classify a barrier as either primarily Hardware or primarily Human (even though every barrier can be traced back to a human), because the models, methods, and tools used to identify and fix system related error fall into those classifications.

Traditionally, the effort applied to hardware engineering of barriers has far exceeded that given to the human and organizational factors associated with barriers (see **Figure 1**).

3.1 Hardware Barriers

Examples of hardware barriers include interlocks, safety instrumented systems, and pressure relief devices. Hardware barriers include a rigorous engineering design and specification effort that human barriers do not. Hardware barriers must be managed and maintained in operation to ensure their effectiveness.

3.1.1 Hardware Barrier Effectiveness – Model

Figure 10 shows a good hardware barrier integrity model to audit to. This is only a framework, however, detailed checklist type questions can be built around this model for an auditor to use on site. This model is a human factors model of a hardware barrier. A brief description of each leg of the model is provided.

- Organizational readiness: Provide competent people in defined roles to identify, implement and maintain barriers. Train Operations and Maintenance on their role in barrier integrity.
- Evergreen: Be able to identify when a barrier is affected by a change. Use feedback metrics to validate barrier design assumptions.
- Capital/ Grandfathering: Define and engineer barriers. Deliver required documentation for use by Evergreen, Operations and Maintenance.
- Test & Maintain: Periodically test and maintain barriers. Populate taxonomy related to barrier performance data.
- Operations Barrier Awareness: Provide tools and train operators to be able to identify when <u>normal work</u> (not a “change”) is degrading a barrier or multiple barriers in a threat path.

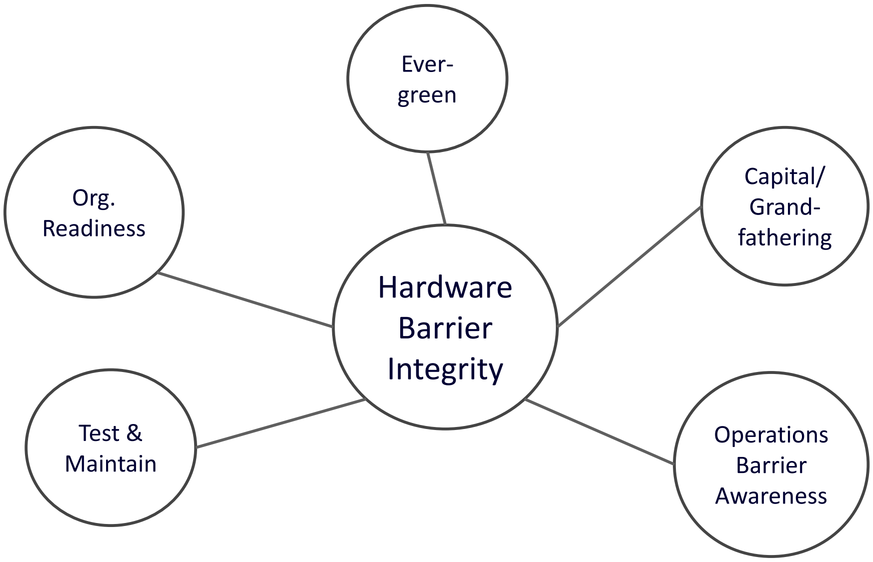

Figure 10. Hardware Barrier Effectiveness Model that incorporates human factors

3.1.2 Hardware Barrier Effectiveness – Tools and Methods

A useful way to structure a site assessment of a barrier is to investigate the gaps in communication between the different organizational groups as they perform their individual tasks related to the barrier. This concept is based on the EAST (Event Analysis of Systemic Teamwork) method of modeling distributed tasks, social systems, and information flow between them [26]. A communications diagram based on an actual site assessment of a barrier is shown in **Figure 11**. A variety of tools are available to assess hardware barriers relative to their human factors.

- Functional Assessments
- Audits
- Checklists
- Bow-Tie Analysis
- Other specialized methods (e.g., CHAZOP, FMEA, etc.) that provide an opportunity to investigate human factors.

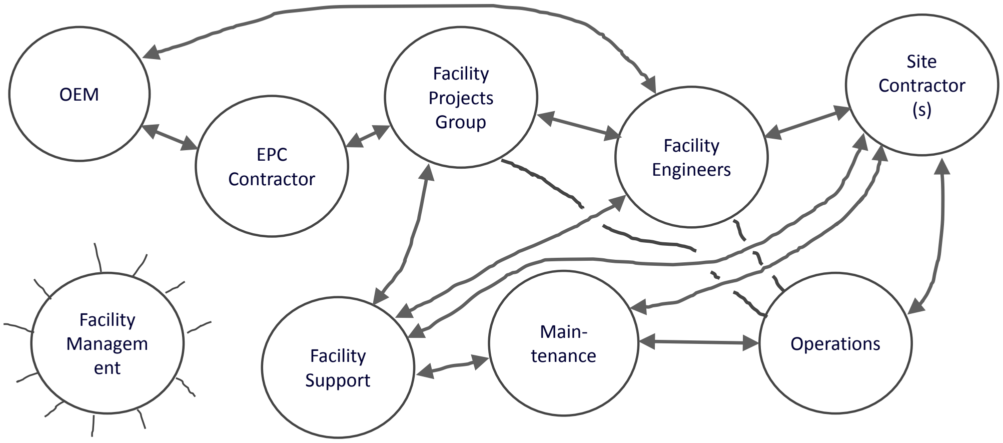

Figure 11. Gaps in Barrier Communication between Groups represent a Typical Latent Condition to identify and fix

3.1.3 Bow-Tie Analysis of a Barrier

Bow-tie diagrams can be used to represent barrier degradation in a cognitively easy manner [12]. The input to the Bow-tie can come from a Task Analysis or any of the methods listed in this sub-section. The objective is to identify what are called the degradation factors (those things that can degrade barrier effectiveness) and also degradation factors controls (safeguards to mitigate the degradation factors). The Left-hand side of the Bow-Tie is presented only. The top event is failure of the barrier. Quantification of the Bow-Tie can be made as well. **Figure 12** shows an example related to human factors degradation of a Spring Operated Relief Valve (SORV). Any time a human touches a barrier there is an opportunity to fail that barrier as shown in **Figure 13** for an SIS (Safety Instrumented System) component. A similar Bow-tie can be created for any of the 3 sub-systems that make up an SIS, using site specific work practices related to the barrier, discovered via Task Analysis.

As mentioned above, even *one* incident related to barrier effectiveness is important because of the extremely low probabilities assumed by LOPA (i.e., 1e-5 or 1e-6) [7]. If you can't fix a barrier weakness, at a minimum track it as a leading KPI (key performance indicator).

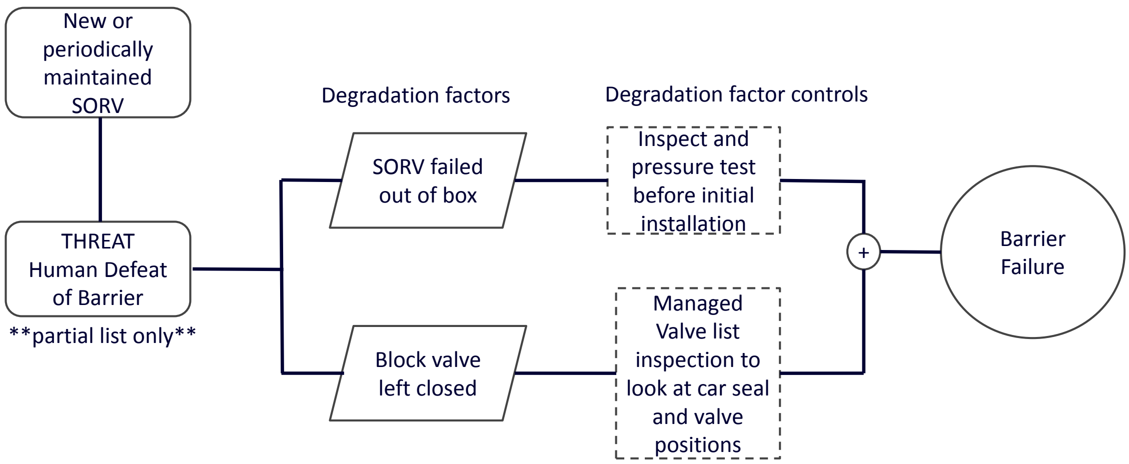
New or periodically maintained SORV
THREAT Human Defeat of Barrier
partial list only
Degradation factors
Degradation factor controls
SORV failed out of box
Block valve left closed
Inspect and pressure test before initial installation
Managed Valve list inspection to look at car seal and valve positions
+
Barrier Failure

Figure 12. The Left-hand side of a Bow-Tie can be used to represent the many ways a barrier can fail due to human factors. The example given represents what we already know. Perform a Task Analysis to discover what you don't already know that could fail your Barrier.

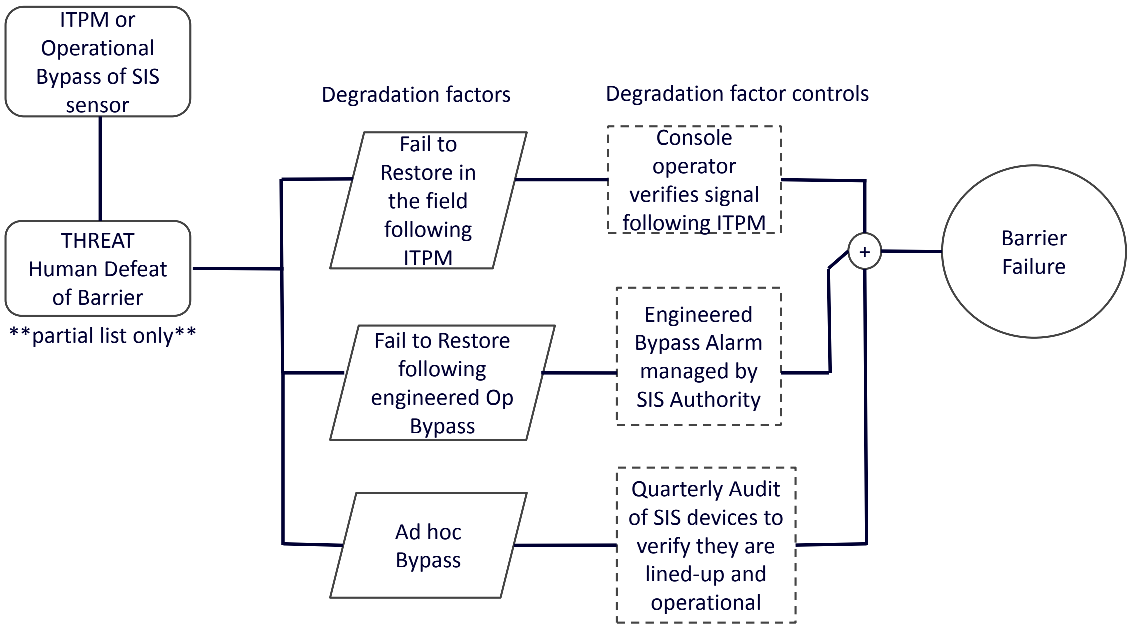
ITPM or Operational Bypass of SIS sensor
THREAT Human Defeat of Barrier
partial list only
Degradation factors
Degradation factor controls
Fail to Restore in the field following ITPM
Fail to Restore following engineered Op Bypass
Ad hoc Bypass
Console operator verifies signal following ITPM
Engineered Bypass Alarm managed by SIS Authority
Quarterly Audit of SIS devices to verify they are lined-up and operational
+
Barrier Failure

Figure 13. Any time a human touches a Safety Device, there is a chance to fail it. The Left-hand side of a Bow-tie can clearly communicate the risk.

3.1.4 Normal Work can Fail Multiple Barriers in the same Threat Path

Normal work processes can fail multiple barriers in the same threat path [19]. An example of this was given in the Introduction section. Another example presented here comes from what I'll call "Barrier Support" groups. This is based on learning from multiple Task Analyses.

It should be noted that attempting to predict the exact path of Normal Accidents a priori would be impossible [20]. Incident or accident analysis that claim to identify root cause(s) suffer the same problem. Could the root cause analysis have been used in advance to predict the accident? The answer is “no” it would be impossible. But we can still learn from incidents and accidents.

The best we may able to do is probe the health of our barriers by looking in places *where nothing bad appears to be happening*. Evidence suggests to look where there appear to be no problems [21, 22]. Barrier Support groups is one such area where nothing bad can appear to be happening related to a barrier. However, if expectations related to a barrier are not communicated to support staff (e.g., Contractors), such as their role in barrier integrity, expected behavior in the presence of breakdowns, and level of performance, etc., latent failure conditions can develop. See **Figure 14**.

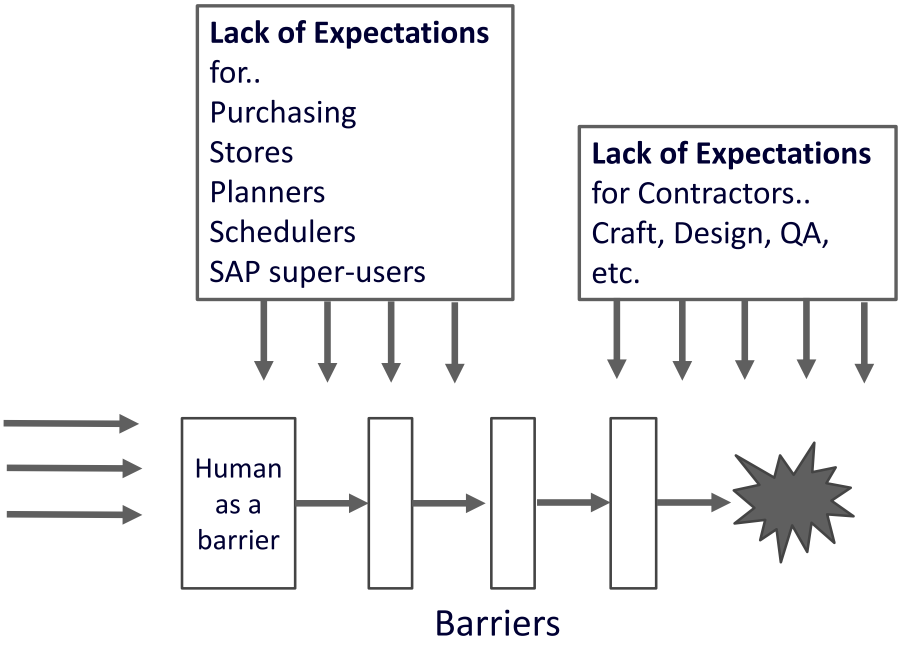

Figure 14. Barrier Support personnel are a common link in all barriers. Not communicating expectations to Barrier Support personnel will create Latent failure conditions that can fail multiple barriers.

3.2 Human Barriers

Examples of human barriers include operator response to alarm, and SOP (standard operating procedure). The front-line operator is a barrier when carrying out every-day normal work in the presence of equipment break-downs, late deliveries, off-spec product, staffing shortages, production pressure, etc. A human barrier has an added element of complexity relative to a hardware barrier because the human mind is a source of systematic bias (a result of System 1 thinking). Human behavior therefore is influenced from two sources:

1. Internal to the mind (psychology based).
2. External to the mind (in the environment or system).

Methods related to ensuring barrier effectiveness must include identifying and fixing external and internal (psychological) error mechanisms. See **Figure 15**.

3.2.1 Human Barrier Effectiveness – Model

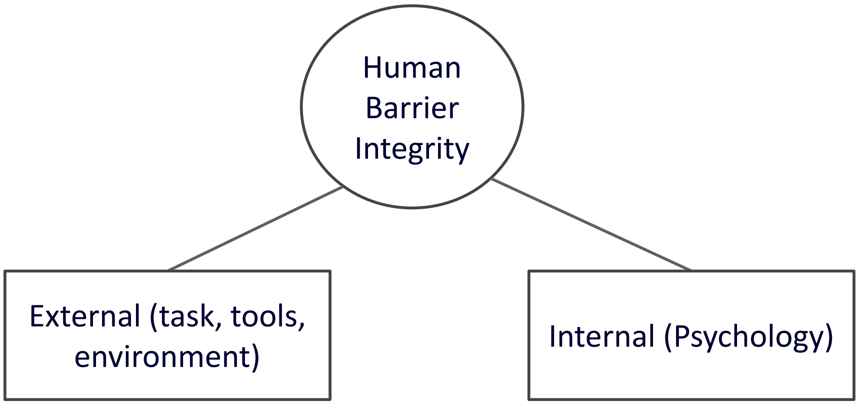

Figure 15. Human Barrier Effectiveness Model

3.2.2 Human Barriers Effectiveness – External Tools and Methods

- Task Analysis
- Taxonomy
- Human Reliability Analysis

3.2.3 Human Barriers Effectiveness – Psychology based Tools and Methods

This sub-section will be demonstrated with an example of what is possible with existing cognitive related tools.

- System 1 and System 2 Thinking
  It was discussed above the susceptibility of humans to make errors in judgement while under System 1 thinking (how most of our thinking is done).
- Cognitive Response Model
  Swain and Guttmann developed the Cognitive Response Model to an abnormal situation (e.g., response to a critical alarm) as part of the THERP methodology [18]. The Cognitive Response Model (Chapter 12) is adapted here to be composed of 4 sub-tasks:
  - Perceive – To detect or become aware, e.g., via an alarm ribbon on a DCS screen.

- Interpret – To decide if the signal (i.e., alarm) is real or spurious (i.e., a false alarm).
- Diagnose – If the signal is interpreted as real, diagnose the cause. This requires a nominal amount of cognition. If the response is more automatic or practiced (i.e., high level → do this) then diagnosis is minimal (in such a case the Annunciator Response Model in Chapter 11 of Swain and Guttmann is more applicable).
- Act – take action to mitigate.

Most alarm analysis ignore the 'perceive' and 'interpret' sub-tasks. For example, if you surprise a board operator with an index card that has an alarm tag written on it, with the intent to evaluate his response, you've bypassed perceive and interpret. What are the negative human factors that can influence each sub-task?

- Perceive – Narrow alarm ribbon displays. Hidden alarm displays. Speaker volume turned all the way down. Un-rationalized and un-prioritized alarms.
- Interpret – It takes just one spurious alarm for a console operator to experience for which System 1 thinking will grab onto the next time an alarm comes in. No matter how good your alarm metrics are statistically, one cause of a spurious alarm is what is remembered. Causes trump statistics [9].
- Diagnose – Probability of correct diagnosis is a direct function of the experience of the console operator. It may take 3-5 years for a board operator to become proficient.
- Act – Assuming the board operator successfully makes it to this sub-task, it is typically considered the least likely to go wrong.

Even experienced, well-trained board operators will make an incorrect interpretation of an alarm. How do we break into System 1 thinking in this case when, spurious alarms can never be completely eliminated?

The answer comes in two parts.

1. Provide a design that takes the need for interpretation away. With modern day DCS capabilities, an 'at-a-glance' graphic can be built incorporating signal trends and comparison to like measurements (a critical alarm will typically have one or more like signals on the same equipment). You need three signals to make the comparison valid. Mass balance can be used for tank levels, for example.
2. Train the console operators to dis-confirm their initial belief that an alarm is false. Confirmation bias is part of the System 1 thinking toolbox [9]. System 1 will supply the necessary confirmation independent of conscious thought, for example, "those instruments are always buggy, it spurious alarms anytime x happens, etc." The fallacy of confirmation is that no matter how much confirming evidence is found, it takes only one instance to dis-confirm a thought or belief. Train the console operators to dis-confirm the thought of a spurious alarm by accessing the engineered graphics page discussed above

that provides the interpretation. Don't allow System 1 to "give" the board operator the (wrong) answer.

The tools of psychology can be used together in novel ways to improve human barriers.

4 Getting Started in Human Factors and HRA

So what do you do if you think Human Factors related to barrier effectiveness needs to be better evaluated and the extent of your Human Factors knowledge comes from a PHA checklist, and no one else wants to get involved, and there is no money even if they did?

Let's first look at the Top 5 reasons why people do not want to evaluate Human Factors and Reliability related to barriers (in the Process Industries).

1. The standard (i.e., ISA S84/ IEC 61511) says you don't have to consider systematic failure (i.e., human error) in the calculations. True. But an astonishing claim nonetheless for the reasons discussed in this paper. Can we at least acknowledge that an error rate attached to the SIL calculation would be appropriate, and that this error rate is primarily a function of the Human Factors?
2. Human Reliability is used in the Nuclear Industry, it's not for the Process Industries. True. But there is evidence (publications, symposiums, etc.) that HRA methods and techniques are catching on in the Process Industries. Petro-HRA [14] and AEA [10] are two examples.
3. We already evaluate Human Factors in our procedural PHA, human factors checklists, and IPL validation program. As discussed previously, these tools look at states and conditions, not behavior. You have to look at how people behave for human factors to work.
4. The process industry isn't ready for it yet. See #2 above.
5. There is no money to do it. True. But it's a matter of establishing priorities based on what you think is important.

It will be a slow process but educating others on the importance and benefit of evaluating Human Factors (in general) and also specifically related to Barriers begins with gaining competence in the methods ourselves. Study the books and documents in the References section, and if you are a PHA-LOPA facilitator you can find creative ways to work these methods into your studies. CHAZOP (Computer Hazop) and FMEA (Failure Modes and Effects Analysis) are also opportunities to integrate Human Factors evaluation.

5 References

1. Laumann, K., Rasmussen, M., Boring, R., *A Literature Study to Explore Empirically: What is the Scientific Discipline of Human factors and What Makes it Distinct from Other Related Fields*. Presented at AHFE 2017 Los Angeles, CA.

2. Ocean Energy Safety Institute, *Human Factors and Ergonomics in Offshore Drilling and Production: The Implications for Drilling Safety*. December 2016.
3. Health and Safety Executive. *Review of Human Reliability Assessment Methods*, 2009.
4. Chartered Institute of Ergonomics & Human Factors., *White Paper: Human Factors in Barrier Management*, December 2016.
5. Wiegmann, D., Scott, S., *A Human Error Approach to Aviation Accident Analysis: The Human Factors Analysis and Classification System*, Ashgate, 2003.
6. Reason, J., *Human Error*, Cambridge Press, 1990.
7. Leveson, N., *Engineering a Safer World: Systems Thinking Applied to Safety*, MIT Press, 2012.
8. Weinberg, G., *An Introduction to General Systems Thinking*, Dorset House, 2001 Silver Edition.
9. Kahneman, Daniel. *Thinking Fast and Slow*, Farrar, Straus & Giroux, New York, 2011.
10. Taylor, R., *Human Error in Process Plant Design and Operations – A Practitioner's Guide*, CRC Press, Taylor & Francis Group, Boca Raton, 2016.
11. Kirwan, B., *A Guide to Practical Human Reliability Assessment*, CRC Press, Taylor & Francis Group, Boca Raton, 1994.
12. McLeod, R., *Designing for Human Reliability – Human Factors Engineering in the Oil, Gas, and Process Industries*, Gulf Professional Publishing, 2015.
13. Stanton, N., *A Practical Guide to Doing Task Analysis Tutorial*, Presented at AHFE 2017 Los Angeles, CA
14. Institute for Energy Technology, *The Petro-HRA Guideline*. Report IFE/HR/E-2017/001, 2017.
15. Norman, D., *The Design of Everyday Things, Revised and Expanded Edition*, Basic Books, New York, 2013.
16. Hollnagel, E., Safety – I and Safety II The Past and Future of Safety Management, Ashgate, 2014.
17. Stanton, N., et al., *Human Factors Methods – A Practical Guide for Engineering and Design*, Ashgate, 2013, 2nd Ed.
18. Swain and Guttmann. NUREG/ CR – 1278. *Handbook of Human Reliability Analysis*. 1983.
19. Perrow, C., *Normal Accidents*, Basic Books, 1984.
20. Reason, J., *Organizational Accidents Revisited*, CRC Press, 2016.
21. Woods, D.,et al., *Behind Human Error*, CRC Press, 2010 2nd Edition.
22. Dekker, S., *The Field Guide to Understanding 'Human Error*,' Ashgate, 2014 3rd Ed.
23. Spurgin, A., *Human Reliability Assessment*, CRC Press, 2010.
24. www.ife.no/petrohra
25. Taylor, C., *Task Analysis as a Cornerstone Technique for Human Reliability Analysis* Presented at AHFE 2017 Los Angeles, CA.
26. Stanton, N., *Keynote Address*, Presented at AHFE 2017 Los Angeles, CA.