Accounting for Emergent Failure Paths in LOPA

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

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.

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

AIChE shall not be responsible for statements or opinions contained
in papers or printed in its publications

Accounting for Emergent Failure Paths in LOPA

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

Keywords: Systems thinking, Emergence, Meta-Uncertainty, Human Reliability, Human Factors

Abstract

One of the fundamental assumptions made when using standard LOPA (Layer of Protection Analysis) is that the barriers selected for a common threat path are independent. In most cases the analysis made by the LOPA team is adequate to judge the degree of independence between barriers. However, this may not always be the case, especially when the desired LOPA target is less than 1e-4 per year. In these cases, LOPA is more susceptible to unaccounted for system effects, than to independent random failures (what LOPA assumes). Another way to say this is that whenever a model (for example, LOPA) predicts that a failure will occur with a negligible chance, the probability that the model can fail becomes important.

Potential failure paths can emerge between barriers in a common threat path due to what is known as “system effects.” That is, to the interaction between otherwise independent barriers due to common support systems (for example, Maintenance), or other Operational or Management impacts. Emergence is a system effect that cannot be identified through other methods, such as IPL (Independent Protection Layer) validation. However, Human Factors methods exist that provide a framework for discovering emergent failures between barriers due to system effects.

This paper will discuss the application of one such system technique known as “NET-HARMS” (Networked Hazard Analysis and Risk Management System). The NET-HARMS technique is a combination of two well-established Human Factors methods, the first being HTA (Hierarchical Task Analysis) and secondly, a modified SHERPA (Systematic Human Error Reduction and Prediction Approach) as the taxonomy used to classify system failures. Both methods are easy to use and can be learned quickly with a little practice. The author has several years’ worth of experience applying these methods to difficult LOPA problems involving administrative controls, and will show how this analysis can be extended to include hardware barriers as well.

1 Introduction

The principles of Systems Theory (or "systems thinking") originated in the 1950's as a way to holistically analyze problems [16]. This is opposite to what is called Reductionism, which is when a system is broken down, and the parts analyzed individually. Reductionism is how most engineering activities occur. Systems thinking holds, that when the system is broken down for analysis, some properties that belong to the system will be lost. The properties that are lost, are called emergent properties, i.e., they are properties of the system, not the parts of the system. Emergence has been called the single most fundamental systems idea [16]. Mechanical systems provide the easiest way to visualize emergence. The parts of a car have different properties than the car as a whole (system). In this paper, we will utilize the Systems Theory concept of Emergence as applied to a Barrier System (see **Fig. 1**). Emergence involves the following concepts: (1) expand the barrier boundary to include people, (2) include focus on the interactions between people, and between people and hardware, (3) don't only focus on hardware reliability, and (4) determine how to define and measure Safety.

Many catastrophic accidents involve failure of multiple discrete barriers (safeguards and Independent Protection layers). It is unlikely (from a probabilistic standpoint) that multiple barriers would all be failed randomly (by chance) as is assumed in typical hardware centric probabilistic calculations. Instead, systemic (human based) conditions creating dependencies are more likely the cause. It makes sense then to study why and how multiple and otherwise independent barriers can fail by systems issues. Of course, the frustrating aspect of these incidents is, if just one barrier had worked, the accident would have been prevented. Therefore, understanding human behavior related to a specific barrier will be discussed as well.

Why do we focus on Barriers, in lieu of say, causes or enabling conditions? It is because the pathway to a potential hazard must go through a set of Barriers, no matter how the scenario starts or is enabled (this assumes we have properly identified the hazard and its Barriers). **Figure 2** shows the People in a Barrier system shown generically in **Fig. 1**.

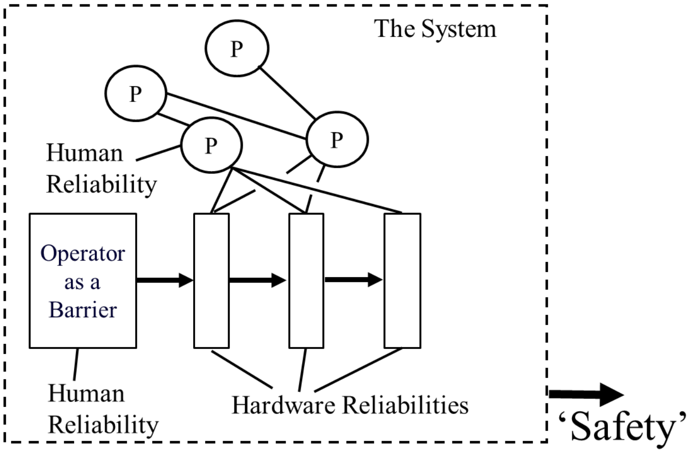

Figure 1. A Barrier System. 'Safety' is a system property that emerges from the interactions between the parts of the system. Component properties (for example, Hardware) are different than system properties. 'P' are people (or groups or departments) that are part of the system.

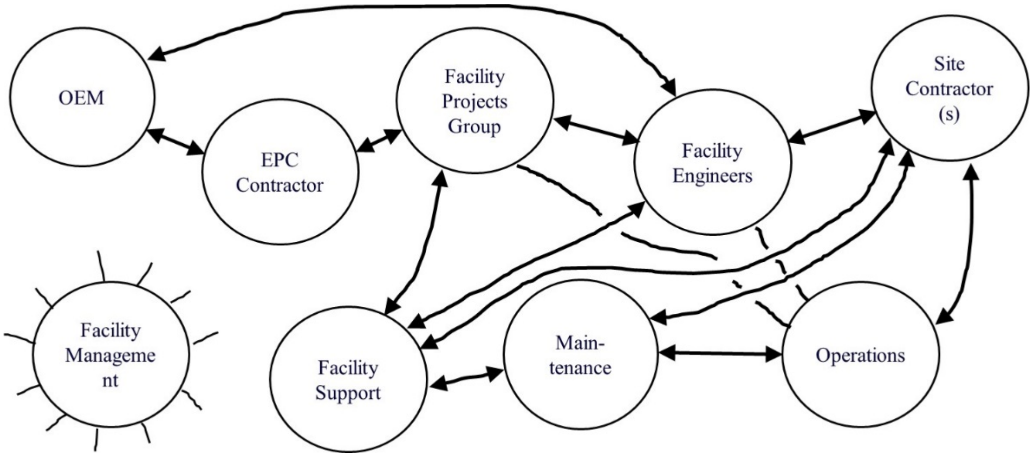

Figure 2. The People in a Barrier System [12]. The physical Barrier is not shown, to recognize the fact that even hardware barriers are fundamentally human. The links between the groups represent task dependencies such as information and expectations that must be communicated. Gaps in the links represent latent failure conditions that could affect one or multiple barriers in the same threat path. The Safety Integrity of the Barrier "emerges" not from its hardware reliability but from the System as a whole.

2 Thinking in Systems

Systems thinking is embedded in the new paradigm known as "Safety Differently" or "Safety 2.0" [1]. New accident models such as STAMP (Systems-Theoretic Accident Model and Process) [2] and FRAM (Functional Resonance Accident Model) [1] utilize systems thinking. Systems thinking is coming to PSM (Process Safety Management), specifically to the way potential hazards are identified, quantified, and controlled. The following is a short list of elements that make up systems thinking [15]. Each element is discussed individually below this list.

- High component reliability is not enough to prevent accidents. Instead, it is necessary to recognize that Reliability and Safety are different properties. Reliability resides at a hardware component level. Safety resides at a system level (it is an emergent property of the system, i.e., it is more than the sum of its parts, it is the product of the *interactions* between its parts). More generally, this is referred to as reductionism vs. holism.
- Safety is not defined by the absence of negative events (e.g., freedom from harm). Instead, Safety is defined by the presence of something (e.g., barriers, reliability, resilience, effort, etc.).
- Accidents are not a linear chain of events. Instead, real accidents are complex and non-linear, often involving drift or "creeping change."
- Probabilistic calculations based on coincidental (i.e., random) failures creates over-confidence (e.g., LOPA). Instead, there are better ways to communicate risk, for example, using qualitative and quantitative Bow-ties.
- Operator error is not the cause of most accidents. Instead, operator error is a consequence of the system (i.e., poor design, production pressure, etc.). At most, normal

operator (human) variance is a local trigger for latent conditions (not necessarily failures) to line-up causing an accident.

- Hindsight bias distorts our view of past events and leads us to believe we can predict future events better than we are able to. Instead, our focus should be on predictive tools, not relying solely on lessons learned from past events to make us safer.

2.1 Reliability versus Safety

It is a common belief that improving hardware reliability will improve safety. Who could argue against this? The reality is however, even if equipment *never failed*, accidents would still happen, simply due to the human element. We need both, hardware reliability and human reliability. Furthermore, Reliability is a component property, while Safety is a system property that "emerges" (i.e., does not reside at the component level) from the interaction between the parts of a system. In this paper, the "system" is the identified barriers (e.g., hardware) used to protect against a potential accident, and includes the people that directly interface with said barriers (Operations, Maintenance, Technical staff, Purchasing, Stores, Contractors, etc.) as well as more remote people such as Management (see **Fig. 2**).

2.2 How to define Safety

The goal of Process Safety (to prevent catastrophic accidents) suffers from what is called the Problem of Induction [3]. Inductive statements can be verified by, for example, experience or statistics. The issue is, attempting to show that a process is safe (e.g., by predicting a rare event frequency meets some acceptably low target), may not be possible to any significant degree of confidence. It is similar to trying to prove a negative (i.e., show that something, for example accidents, won't or can't happen). Negatives cannot be demonstrated using statistics because there is not enough data (e.g., on rare events) *for my plant*. Justifying a process is safe by experience (i.e., "we've operated for 30 years without that happening") is a weak argument because it takes just one accident to disprove the process was safe, and by then it's too late. The issue is encapsulated by the following saying "Absence of Evidence, is not the same as Evidence of Absence." It is not possible to gather "evidence of absence." What can we do?

The best we may be able to do to validate a process is "safe" is to use a combination of feedback performance (i.e., field data) of our Barriers, along with a short (several years) predictive evaluation of the quality of Barrier management. Bayes theorem could be used.

A Bayesian Prior could be developed from the following conceptual equation:

Prior = Barrier Hardware Reliability + Barrier Human Reliability + Barrier qualitative assessments.

The qualitative assessment can be converted into a quantitative probability distribution because Bayes theorem is an epistemological statement (i.e., based on knowledge) versus a statement of frequencies and proportions. We can use all of our qualitative knowledge of how Barriers are being managed as an input to the Bayes Prior.

Later, as we gather new evidence (i.e., the field data on our Barriers) we can update our Prior to calculate a Posterior. This cycle repeats itself every several years as new data is gathered (i.e., the Posterior becomes the new Prior). See **Fig. 3**.

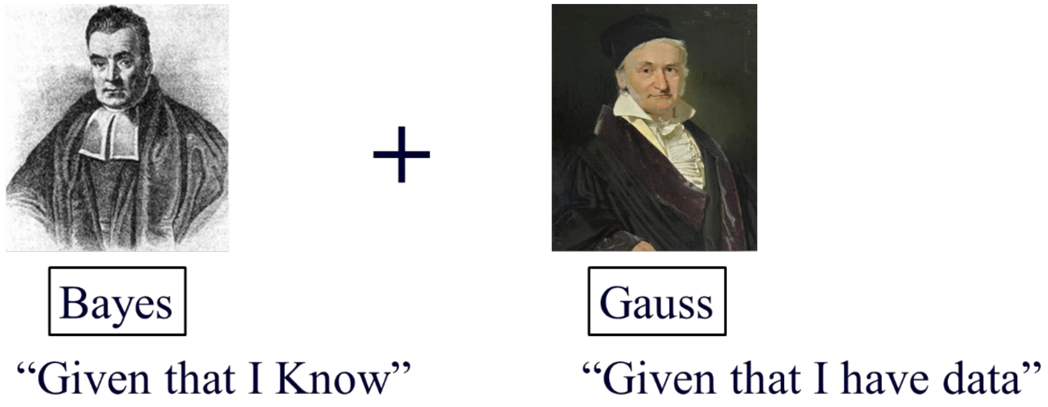

Figure 3. Both Bayes Theorem and Gaussian style statistics are need to demonstrate the confidence in a predicted rare event frequency.

2.3 Accident Models

A good accident model will have the ability to incorporate system components or layers into its boundary. Reason's [4] Swiss Cheese Model (SCM) is one such model. The SCM is superior to all other system accident models because of its ability to communicate in a simple way the nature of complex accidents through the graphical image of Swiss Cheese layers. The SCM is sometimes mistaken for a linear model, because the failure trajectory is shown as being linear through the holes in the Swiss Cheese. This is a misperception. It is very difficult to draw a non-linear accident model in any meaningful way (i.e., that is useful to practitioners).

LOPA (Layer of Protection Analysis) does not represent a practical implementation of the SCM, although they look similar (i.e., the Onion layers concept). LOPA stops at human error (i.e., does not look at systemic factors), and does not even treat active (front-line) errors effectively (i.e., from a human factors perspective). To be clear, the SCM although popular and well-known, is not being used as an accident model in many Process Safety Management programs.

How do we implement the SCM in a practical way? The answer: HFACS (Human Factors Analysis and Classification System) (see **Table 2**). HFACS was created to make Reason's Swiss Cheese accident model useful to the practitioner. That is, to define the holes in the layers of protection (i.e., the Swiss Cheese slices). 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 HFACS method can be used to identify, classify, and correct these system factors *before* an accident occurs.

2.4 Meta-Uncertainty

When a LOPA calculation shows an event to have a predicted likelihood of occurrence of 1e-4 per year (or less), the result is subject to more than random (classical) uncertainty. At these low numbers, meta-uncertainty (the uncertainty of uncertainty) can begin to dominate [3]. These are the "unknown unknowns" (i.e., what we don't know we don't know) and even worse are the "unknown knowns" (i.e., what we should know (for example, excessive bypassing is occurring), or what we know but refuse to acknowledge is a problem (for example, my LOPA calculation based on coincidental failures is a true measure of my risk)). The issue is referred to as "unsampled-randomness" that no amount of generic data or advanced Markov or Monte-Carlo methods can account for. To be clear, confidence intervals based on classical (frequentist based) statistics are "knowns" and do not represent system uncertainty (i.e., meta-uncertainty).

The Bow-tie graphical presentation which can include safeguards, IPLs (Independent Protection Layers), administrative controls, Degradation factors, Degradation factor controls, audit results, incident results, with the ability to quantify many of these events, makes Bow-tie a far superior tool than LOPA to communicate Risk (see **Fig. 4**). In addition, a Bow-tie diagram can be created for a single barrier or a set of Barriers in a common threat path, showing all the ways the Barriers can fail, including by common system effects, which can be very effective.

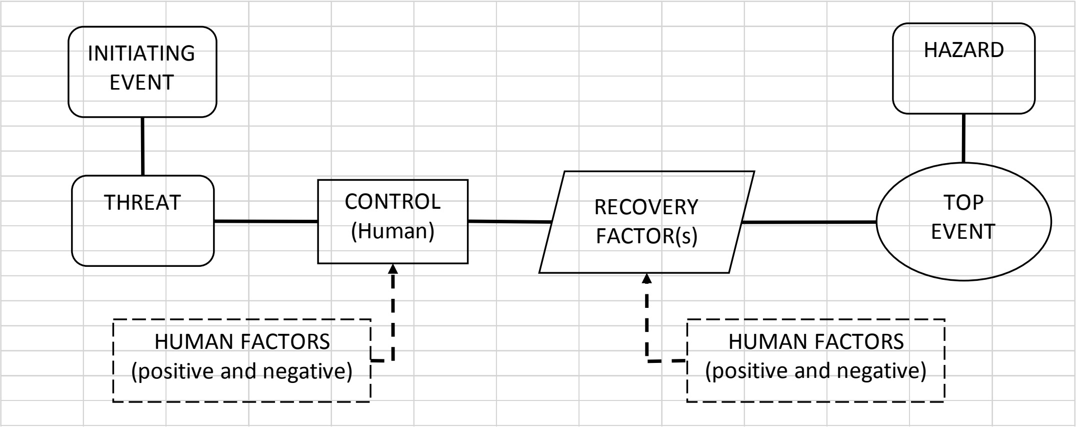
INITIATING EVENT
HAZARD
THREAT
CONTROL (Human)
RECOVERY FACTOR(s)
TOP EVENT
HUMAN FACTORS (positive and negative)
HUMAN FACTORS (positive and negative)

Figure 4. LHS (Left Hand Side) of a Bow-tie. This template can be used for documenting and quantifying a procedural control associated with a catastrophic risk. The human factors from **Section 4.2** can be coded into the spreadsheet. Use **Task Analysis** to complete the template.

2.5 Human Error

Humans (front-line workers) get blamed for 80 to 90 percent of industrial accidents, depending on the report you're reading. Don Norman, the famous Engineering Psychologist, puts the figure closer to 1 to 5 percent [5]. The difference exists because it's easy to stop at "human error" versus looking for (and correcting) the systemic issues that promote or make human error more likely. A different person in the same environment would have made the same error. It's not a front-line operator problem, it's a design problem.

2.6 Hindsight Bias

Hindsight bias is one of the more harmful cognitive biases [6]. It leads us to believe we understand the past more than we really do, and in turn gives us over-confidence in predicting the future (for example, the way potential accidents can happen). The past always appears more deterministic than it really is. When we connect-the-dots to trace back an accident path, we lose the randomness that existed at the time. Hindsight bias presents a serious challenge to (1) how much we can learn from past events, and (2) our ability to predict the occurrence of future events. In addition to learning from past accidents (albeit not as much as we think we do), predictive human factors tools such as Task Analysis paired with an appropriate Taxonomy, provide a systematic way to identify accidents before they occur. This is discussed further in **Section 4**.

3 Is it better to be Lucky or Good in Process Safety?

For a systems thinker, especially one who has practiced Human Reliability methods (see **Table 2**), studied meta-Uncertainty **(see 2.4)**, and the Problem of Induction **(see 2.2)**, probabilistic calculations based on coincidental (random) failure of barriers that purport numbers as low as 1e-4 per year or lower (anytime you have to "count the zeroes"), can look pretty silly. Does anyone actually believe these numbers? There have been many instances reported in the Literature of probabilistic risk assessments showing very low numbers, only to have the accident occur within one year of said calculation [2,7].

You can see how skepticism would creep in, challenging the value, even the necessity of spending resources to produce such unrealistic numbers (for example those produced by Safety Integrity Level calculations, or LOPA).

However, there is a trap in believing calculations based on random failures are useless (*no matter* how low the number is, and regardless of how bad the systemic factors are). The trap is called "ergodicity." Ergodicity is a rarely discussed probabilistic concept. It means "in the long run." And in the long run, rare events (events with low but non-zero probability) that occur only randomly, are *guaranteed* to happen (somewhere), given enough time or opportunity [14]. And in the Process Industries, there is ample opportunity for random accidents to occur. Ergodicity is also the reason to invest in both preventive and mitigative barriers (Left and Right-hand side of the Bow-tie, respectively). Ergodicity is the reason hardware reliability calculations based *only* on random failure, contributes positively to process safety.

So, is it better to be Lucky or Good? In Process safety *we need both*. (The word "Lucky" in this context does not mean haphazard. It means occurring by chance, but also following good reliability engineering principles for hardware Barriers. The "Good" refers to identify and fixing potential causal (deterministic) failure of hardware Barriers (or good human factors for Human Barriers), that can derange random based probabilistic calculations for said hardware or human).

4 Human Factors Tools vs. Traditional PSM Tools

PSM (Process Safety Management) utilizes a variety of tools (see **Table 1**) that have the potential to better incorporate human factors principles and methods. To be clear, PSM tools are not human factors methods (although many PSM tools do incorporate elements of human factors). Human factors and reliability methods such as Task Analysis are well established, see for example Stanton et al. [8] and Grattan [12], for a discussion of said tools. PSM does not need new human factors methods. What it needs however is to adopt some of the said methods into the practice of PSM, by integration or stand-alone use.

In general, PSM tools, while addressing many human factors elements, suffers from the following shortcomings when evaluating human factors:

1. PSM tools related to human factors fail to look at Behavior, instead focusing on States and Conditions **(see 4.1)**.
2. PSM tools related to human factors fail to leverage the predictive ability of human factors methods **(see 4.2)**.

Why do we look at behavior? The intent of observing behavior is *not* to change behavior; that is the goal of Behavior Based Safety (BBS) programs. Instead, the intent is to understand the "work-as-imagined" versus "work-as-done" principle [1]. Work-as-imagined by designers, managers, PHA teams, procedure writers, etc. is *never* the same (*can never* be the same) as the work-as-actually-performed by Operations and Maintenance staff. The differences can reveal latent conditions that will eventually bite.

Using checklists to "do" human factors is a good example of these deficiencies. Checklists presuppose that every human factor or error can be predefined and put into checklist form [2]. A checklist does not evaluate Behavior, and a checklist is certainly not predictive. Checklists are useful, especially for the "knowns," however beyond that they are inadequate. At the other end of the spectrum are Audits. Audits do look at behavior, and are a good candidate to incorporate some of the tools in **Table 2**.

Table 1. PSM Tools that represent an opportunity to Incorporate Human Factors Methods

PSM Tool
Functional Safety Assessments
Audits
Checklists
IPL Validation
Bow-Tie Analysis
Other specialized methods (e.g., Control System HAZOP, Failure

Modes and Effects Analysis, Procedural PHA, etc.) that provide an opportunity to investigate human factors.

Table 2. Some Human Factors Tools that can be used Stand-alone or Integrated with Table 1 to Improve the Practice of PSM related to Human Factors (see Stanton et al. [8])

Human Factors Tool	**Application/ Purpose**
Hierarchical Task Analysis	Understand the difference between “work-as-done” vs. “work-as-imagined”
Cognitive Task Analysis	Evaluate the conscious thinking a task involves (as opposed to the physical work)
Situation Awareness Analysis	Evaluate the “What?”, “So what?” and “What-now?”
Human Error Taxonomy (e.g., HFACS, SHERPA)	Pair with Task Analysis or Human Reliability Analysis
System Error (e.g., NET-HARMS) [13]	Used to identify Emergent failure paths
Human Reliability Analysis (e.g., AEA, Petro-HRA)[12]	Used to quantify Human Error rates for a given Task

4.1 States and Conditions vs. Behavior

One of the goals of human factors analysis to understand how work is actually performed (i.e., behavior). **Table 3** gives examples of the behavior associated with a state or condition of equipment, design, or procedures, etc.

Table 3. Any State or Condition has a corresponding Behavior associated with it

State/ Condition	**Behavior**
Is equipment properly labelled?	Will the operator actually **read** the label?
Are the proper Tools available?	Does the operator or maintenance worker **use** the tools?
Are procedures available?	Does the operator or maintenance worker **use** the procedures?

What-if this step in the procedure is omitted?	How **likely** is the operator to skip that step and **why**?
Is the alarm configured as priority?	How will the console operator **interpret** the alarm?
Is the alarm audible above background noise in the control room?	Will the console operator **turn down** the alarm volume because it is annoying?
Is adequate information about normal and upset process conditions clearly displayed in the control room?	How likely is the console operator to **proactively monitor** said information?

4.2 Error Promoting and Error Likely Situations

Human Factors methods have the ability to be predictive, i.e., to be able to predict that human error will occur (or be more likely to occur) when a given condition(s) exists.

Two references that are useful for helping to identify bad human factors that can be corrected are found in Norman's [5] discussion of design induced error, and Taylor's [9] discussion of human error syndromes. In addition, Miller's [10] "Basic Human Needs to be Fulfilled in Design," which form the basis for many industrial accidents is an excellent reference. All of these can be applied in an existing operating facility as part of a Task Analysis.

5 Human Factors Tools to Support LOPA Barrier Analysis

The tools listed in **Table 2** can be used stand-alone or in conjunction with the Tools in **Table 1** to analyze any single Barrier identified in LOPA. The Barrier can be hardware or human based (administrative controls, etc.). Even hardware Barriers contain critical human influence (e.g., Operations, Maintenance, Contractors, etc.) that should be recognized (see **Fig. 2**). A human barrier can also be the "Cause" of a catastrophic accident (see **Figs. 5 and 6**). Typically, resources do not exist to evaluate every barrier from a human factors perspective, therefore some prioritization will have to be made.

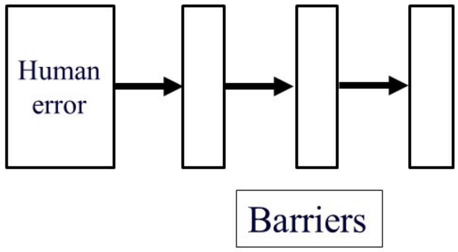

Figure 5. PHA-LOPA viewpoint of Human Error as a Cause (this is a fallacy) [12]

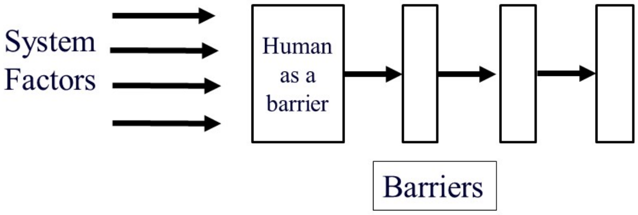

Figure 6. When human error is viewed as a consequence (not a cause), the human becomes an important Barrier in the sequence of events [11]. Any human error which results in a catastrophic consequence should become a candidate for a Human Factors analysis [12].

6 Emergent Failure Paths in LOPA

Fig. 1 gives a generic representation of a barrier system that can create emergent failure, that is, between the links (interactions) of the parts. The Barrier(s) can be hardware or human based.

Networked Hazard Analysis and Risk Management System (NET-HARMS) is unique because it is not a new systems model of accident causation. Instead, it utilizes existing Human Factors tools found in **Table 2** to identify (predict) emergent errors and risk due to interaction between the parts of the system (in this case a system related to Barrier integrity). The same tools can be used to evaluate barrier integrity inside the circles of **Fig. 2** as well.

Let's sharpen the pencil and look in detail at some of the latent conditions that can exist between the parts of **Fig. 2** (the links). **Fig. 7** shows that expectations related to a barrier must be communicated to (in this case) Facility Support, so that, for example, adequate maintenance, failure tracking, and management of change for the Barrier can occur.

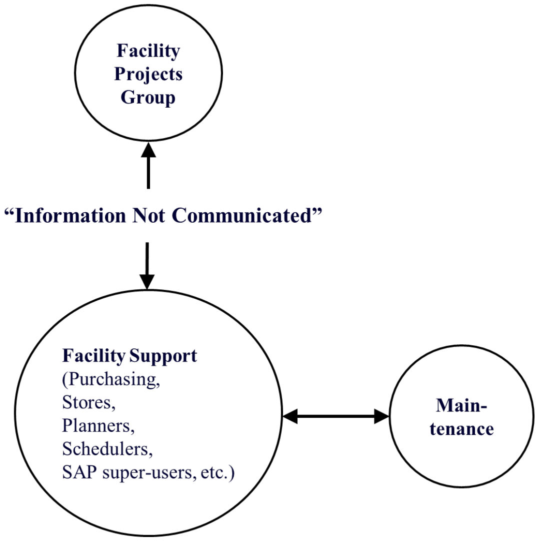

Figure 7. Facility Support personnel are a common link in all barriers. Not communicating expectations to Facility Support personnel will create Latent failure conditions that can eventually fail multiple barriers in the same threat path.

Table 4 list the taxonomy published for NET-HARMS [13] that can be used to identify latent failures between parts of the Barrier system. This taxonomy should be used along with a Task Analysis for those parts of the system where latent weaknesses are suspected.

Table 4. NET-HARMS Taxonomy to Apply to the System Links [13]

Code	Description
T1	Task mistimed
T2	Task omitted
T3	Task completed inadequately
T4	Inadequate task object
T5	Inappropriate task
C1	Information not communicated
C2	Wrong information communicated
C3	Inadequate information communicated
C4	Communication mistimed

7 Conclusion

A Barrier system is more just hardware reliability. It is a collection of people (system elements) that are linked together in such a way that the Barrier integrity emerges through the interactions between the people, and between people and hardware. This is a systems perspective.

Generally, PSM Tools are not Human Factors methods, in that PSM tools cannot predict the likelihood of human error, nor they do not focus on said behavior. However, Human Factors methods can be used in select applications, for example, Barrier Analysis, to provide an improved evaluation of the integrity of the Barrier(s). In this way, both hardware reliability requirements and potential systemic failures, are addressed.

NET-HARMS was presented as a unique Systems tool that can be used to identify emergent failure in a single Barrier or System of Barriers protecting a common threat path. NET-HARMS uses Task Analysis paired with a modified SHERPA Taxonomy to identify potential latent failure conditions between parts of a system.

Experienced PSM practitioners should begin to use Human Factors methods, and with practice will improve Process Safety related to Barrier integrity.

8 References

[1] Hollnagel, E., 2014. Safety-I and Safety-II The Past and Future of Safety Management, CRC Press, Boca Raton.

[2] Leveson, N.G., 2012. Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, Cambridge.

[3] Taleb, N.N., 2004. Fooled by Randomness – The Hidden Role of Chance in Life and in the Markets. Random House, New York.

[4] Reason, J., 1990. Human Error. Cambridge University Press, Cambridge.

[5] Norman, D., 2013. The Design of Everyday Things, Revised and Expanded ed, Basic Books, New York.

[6] Kahneman, D, 2011. Thinking Fast and Slow. Farrar, Straus & Giroux, New York.

[7] Perrow, C., 1984. Normal Accidents - Living with High Risk Technologies. Princeton University Press, New Jersey.

[8] Stanton, N.A., Salmon, P.M., Rafferty, L.A., Walker, G.H., Baber, C., Jenkins, D.P., 2013. Human Factors Methods – A Practical Guide for Engineering and Design, second ed. Ashgate, England.

[9] Taylor, J.R., 2016. Human Error in Process Plant Design and Operations – A Practitioner's Guide. CRC Press, Boca Raton.

[10] Miller, Gerry, 2017. Presented at: Forum on Human Factors to Support Safer and Effective Offshore Energy Operations, OESI, TAMU MKO, 2017.

[11] CIEHF (Chartered Institute of Ergonomics & Human Factors), 2016. White Paper: Human Factors in Barrier Management. United Kingdom.

[12] Grattan, David, 2018. Improving Barrier Effectiveness Using Human Factors Methods, Journal of Loss Prevention in the Process Industries, 55 (2018) 400–410.

[13] Dallat, C., Salmon, P.M., Goode, N., Identifying risks and emergent risks across sociotechnical systems: The NET-worked Hazard Analysis and Risk Management System (NET-HARMS).

[14] Bennett, Deborah J., 1998. Randomness. Harvard University Press.

[15] Meadows, Donella H., 2008. Thinking in Systems, A Primer. Chelsea Green Publishing, Vermont.

[16] Chapman, Jake, 2004. System Failure, second ed., Demos, London.