Session No 746

Using System Safety Techniques to Perform Hazard Analysis

John J. Kolak, CSP
Praxis Corporation

History of System Safety

Systems Safety was developed in the 1940's in response to dissatisfaction with what was known as the "fly-fix-fly" approach to aircraft systems design. The "fly-fix-fly" approach entailed having test pilots fly planes at or near their design limitations and, when a system component failed (which sometimes killed the pilot), they would conduct a post-incident investigation. They would then take the "lessons learned" from the investigation to make design changes to the aircraft. They would then repeat the process until such time as the designs produce satisfactory performance.

Obviously, the "fly-fix-fly" approach to systems design is very inefficient from the design cost and risk perspectives. Yet, this is precisely how many organizations manage safety. Organizations often manage safety almost completely using Reactive measures such as Incidence Rates and "lessons learned" from accident investigations. This mirrors the "fly-fix-fly" approach in that the organization conducts their normal business ("fly") until such time as an accident or system loss occurs. They then investigate the accident to (hopefully) identify and correct causal factors ("fix") and then they re-commence operation of the business ("fly") until another event occurs (Stephenson, 1991).

The costs associated with damaging expensive fighter jets and the development of nuclear energy (where a single system failure was unacceptable) contributed to the concept that ***hazards must be anticipated and controlled before even a single loss occurs***. This was essentially the advent of modern Hazard Analysis (HA) as we know it.

Safety as a System

As Figure 1 illustrates, safety is actually a *dynamic System of processes* that all *simultaneously interrelate.* This means that one cannot change one part of the system without affecting the other parts of the system as well. John Bradshaw, a famous psychologist, uses a mobile suspended from the ceiling to illustrate the systemic nature of families and his excellent illustration is appropriate for use here. In his demonstration Bradshaw touches one part of the mobile and then notes that every other part of the mobile begins to move as well. The message here is that in *interrelated systems*, changing one part of the system will affect the other parts of the system as well. This means that a linear approach to safety management is not appropriate because making any system change will result in a new system that must be ***evaluated as a separate entity***. This is one reason that the concept of "multiple causation" has emerged as important aspect of accident investigations. The concept of multiple causation will be reinforced in the discussion of the MORT chart later in this paper.

The principle concept to grasp relative to Safety as a System is that Safety Performance is a function of how well the various safety process ***interrelate***, rather than the quality of each safety system element as a stand-alone process. For example, having a world-class safety training program within an organization with dysfunctional management systems will most likely result in accidents because the dysfunctional management practices can place workers in proximity to hazards for which training cannot provide adequate protection. Therefore, is it much better to have average-quality safety system elements that integrate well than it is to have best-in-class program elements that do not coherently integrate.

Another important concept is that we use any "system" to replicate system outputs. The point of having any system is to *reproduce things with greater reliability* and at lower

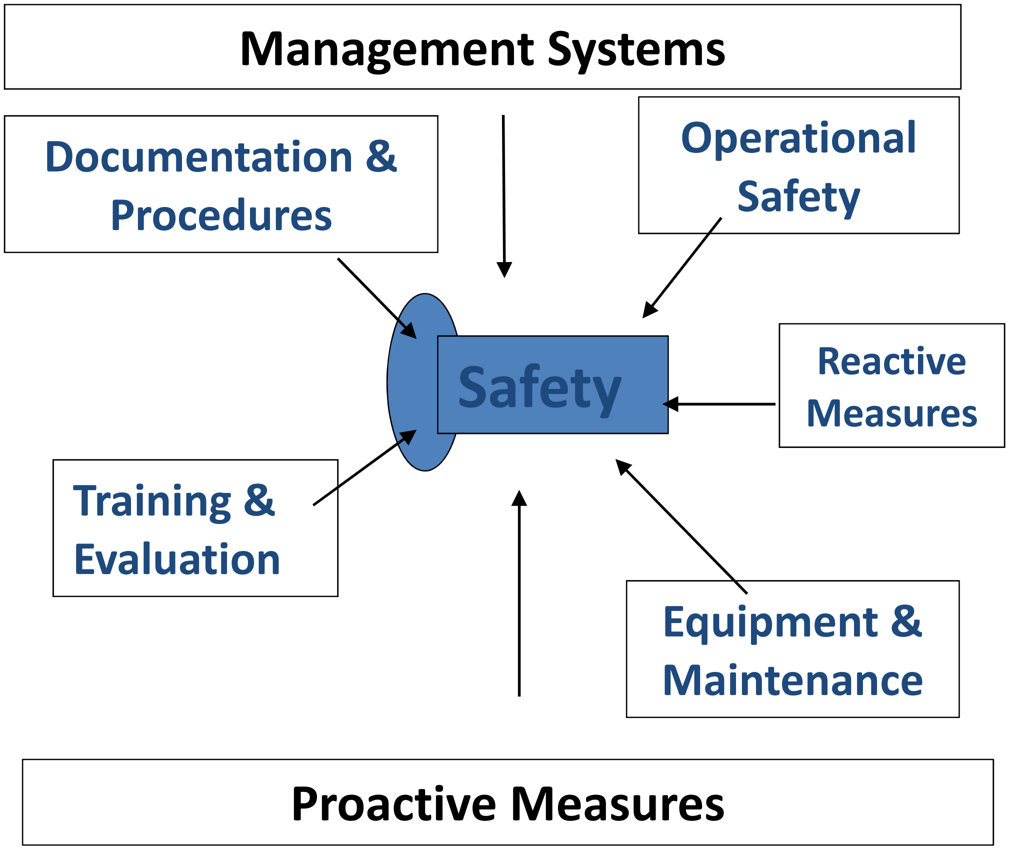


Figure 1. Safety is a dynamic system of processes that all simultaneously interrelate.

costs. Any system produces both “wanted” and “unwanted” products. For example, a manufacturing process produces a product (the “wanted” output) and some waste products (the “unwanted” outputs). The goal of Process Engineering is to maximize the desirable process outputs while minimizing the undesirable process outputs.

Similarly, the Safety System produces both desirable (safe work) products and undesirable products (accidents). The key point in this discussion is that accidents are a system output and they will be replicated by that system until the fundamental system changes are employed. Making “cosmetic” changes to a system will not significantly change the number and severity of accidents associated with that system. For example, asking delivery drivers to handle packages weighing more than the “human machine” can safely handle will result in increased soft-tissue injuries. Providing a “cosmetic” change, such as training in safe-lifting techniques, when continuing to have workers handle weights beyond the capabilities of their bodies will not correct this problem. A “system change” would be to employ a lift or hoist to exchange the human machine for another machine that IS rated for the loads involved.

It is important to realize that Figure 1 is not inclusive of all the processes that effect safety. The author has derived these 7 elements from the Management Oversight and Risk Tree (MORT) chart which is discussed later in this paper. Figure 1 merely illustrates that there are many processes, each of which are complex in their own right, that all directly-impact the safety performance of an organization. To further complicate matters, these processes also interrelate with each other, thus amplifying the complexity of the safety system.

Despite the complexity of modern organizational systems, System Safety techniques for HA provide reasonably objective ways to study complex systems and quantify Risk. The use of System Safety HA techniques provides an important way of *providing objective data to Management*, who ultimately must make decisions regarding resource allocation and implementation of corporate safety initiatives.

Definition of Risk

Risk is defined as the product of **Hazard Severity** (HS) and **Hazard Probablity (**HP**)**. HS is defined as :*“The worst credible accident that could be caused by the hazard in question.”*HP is defined as: *“The probability that this hazard will produce an accident over the system life cycle.”*

While most organizations probably do a nice job of assessing HS, our experience has been that HA is based upon financial cycles, such as fiscal reporting periods, rather than System Life Cycles. This leads to erroneous Risk assessments and unnecessary losses both to human life and the cost associated with system failure. The importance of System Life Cycles is discussed in the next section.

System Life Cycles

As previously discussed, the HP portion of HA must account for the System Life Cycle (SLC) of the equipment, and the workers, who perform job within that system. The SLC of a system includes the following phases:

- **Concept Phase**: Where system objectives, descriptions and requirements are developed.
- **Design Phase:** Where specific plans, drawings and specifications are developed to achieve the objectives of the Concept phase.
- **Production Phase: w**here the end product is produced from the project designs.
- **Operations Phase: W**here the end product is in use.
- **Disposal Phase**: Where the end product is retired, destroyed or discarded.

Both equipment and humans have a life cycle. The life cycle on a piece of equipment is usually defined by the equipment manufacturer as a function of the number of operations. For example, a typical circuit breaker is rated for up to 50 operations under overload conditions but it is rated for only a single operation under Short-Circuit operations. Therefore, circuit breakers have a reasonably-long life cycle for overload operations but it may have a very short life cycle for Short Circuit operations.

When assessing the life cycle of humans, we use 30 years (Mims, 1993) . Using our circuit breaker example, when assessing the Risk associated with resetting circuit breakers, the analyst must consider the number of times humans will reset that breaker over 30 years or the life of that breaker, whichever is longer. This analysis can be amplified by further studying the number of times that breaker is reset AFTER it reaches its design limitations. The probability of catastrophic failure of that breaker increases sharply if the breaker is operated beyond its design limitations.

As we will see in the Financial calculations section of this paper, money invested to “upstream” resources will likely have a better Return On Investment (ROI) than will resources invested later in the System Life Cycle. For example, it is much more cost effective to correct a system problem when it is in the Design phase than it is to correct the same problem once the system is in the Operations phase. This is so because changing engineering drawings is a lot cheaper than retrofitting equipment and retraining employees to compensate for an “upstream” oversight.

Safety Precedence Sequence

The Safety Precedence Sequence is a Systems Safety concept that specifies the most preferable ways to manage risk. The discussion of this topic also illustrates several key points in the safety process.

The word “precedence” suggests that one thing “precedes” another and in the case of the Safety Precedence Sequence, this is very important. There is a preferential order of prevention activities and following this “precedence” will greatly reduce the risk that must be accepted by management.

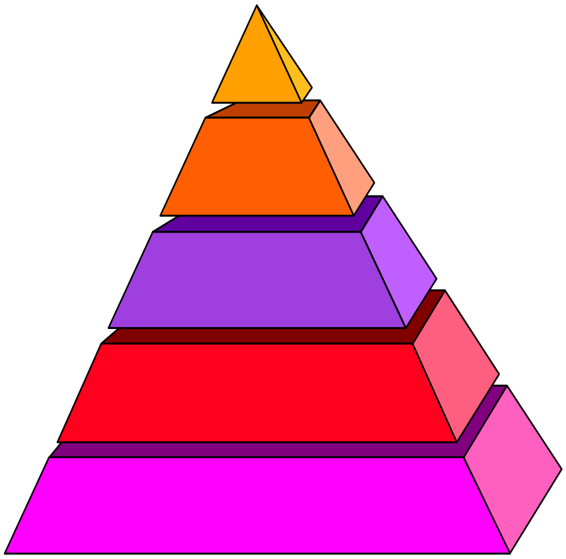


Figure 2: Safety Precedence Sequence.

The Safety Precedence Sequence is as follows (starting at the bottom of the pyramid in Figure 2):

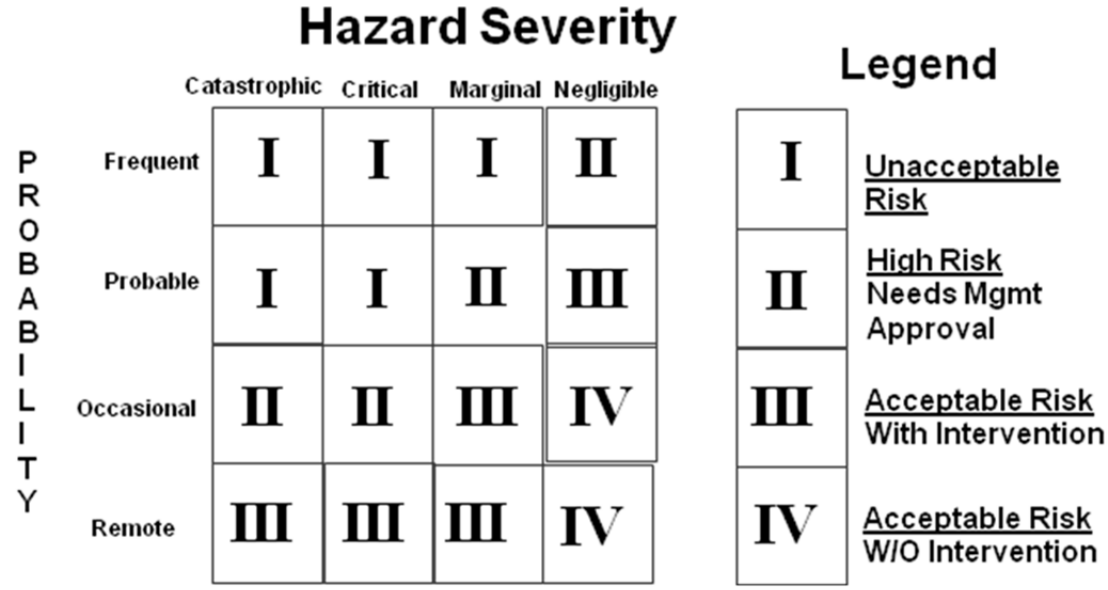
1. Use engineering controls
2. Provide guards or barriers
3. Provide warning devices
4. Control hazards with rules, procedures, or Personal Protective Equipment (PPE)
5. Accept the remaining risk

The most effective way to manage risk is to eliminate hazards through the use of engineering controls. This is so because elimination of hazards negates the need to follow safe work procedures (which human often will not do) or don PPE which may not be rated for the energy produced by equipment failures. The effectiveness of the hazard controls diminishes significantly as one moves down the sequence. Therefore, if an organization chooses to manage safety using less-effective hazard controls, such as PPE, they must overlap controls such that the *redundancy in the control systems reduces the probability* of an accident to acceptable levels. The use of System Safety techniques in HA affords a much more precise way of knowing if the controls systems will in fact produce satisfactory results.

Risk Assessment Codes (RACs)

An important aspect of System Safety HA is the use of Risk Assessment Codes (RAC).

The RAC is a method to evaluate Risk as a function of the relationship between HS and HP. The task for management is to determine *how much risk to accept* given the factors of HS and HP. Figure 3 below provides an example of RAC:



Hazard Severity

PROBABILITY	Catastrophic	Critical	Marginal	Negligible
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	II	II	III	IV
Remote	III	III	III	IV

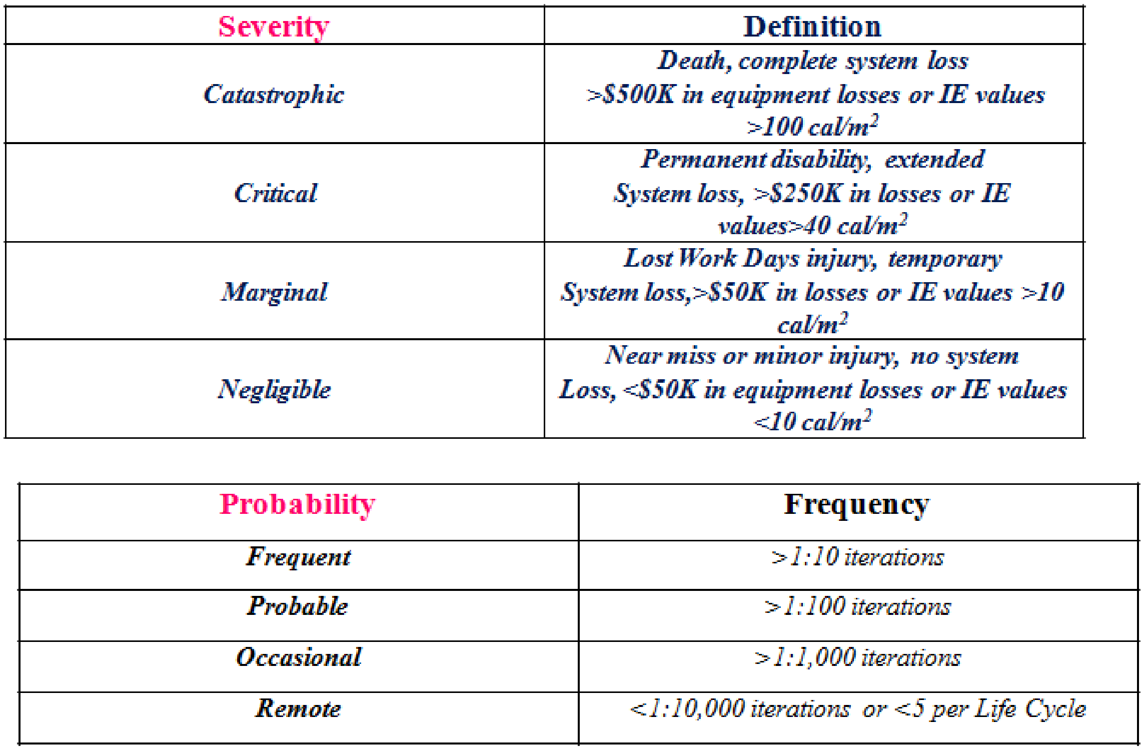
Legend

I	Unacceptable Risk
II	High Risk Needs Mgmt Approval
III	Acceptable Risk With Intervention
IV	Acceptable Risk W/O Intervention

Figure 3. Risk Assessment Codes

It is vitally important for the organization to agree upon Operational Definitions for each category of HS and HP. Preferred method of assessing HS often include categorizing each severity level by the level of injury when humans are involved and by defining the level of financial or system loss when quantifying the severity of damage to equipment.

HP is usually defined as a function of the number of unwanted outcomes that will be produced ***over the SLC***. An example, not meant to be definitive, of typical measures for HS and HP appear in Figure 4 below:



Severity	Definition
Catastrophic	*Death, complete system loss* *>$500K in equipment losses or IE values >100 cal/m^2*
Critical	*Permanent disability, extended* *System loss, >$250K in losses or IE values>40 cal/m^2*
Marginal	*Lost Work Days injury, temporary* *System loss,>$50K in losses or IE values >10 cal/m^2*
Negligible	*Near miss or minor injury, no system* *Loss, <$50K in equipment losses or IE values <10 cal/m^2*

Probability	Frequency
Frequent	*>1:10 iterations*
Probable	*>1:100 iterations*
Occasional	*>1:1,000 iterations*
Remote	*<1:10,000 iterations or <5 per Life Cycle*

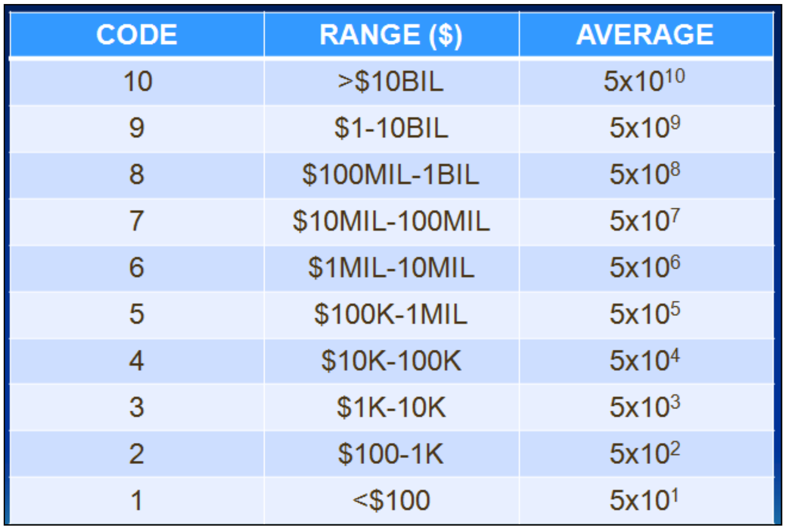
Figure 4. Typical measure for HS and HP

As previously discussed, “Risk” is usually defined as the Product of HS and HP. To enable the use of multiplication the various levels of HS and HP are depicted numerically. The next section of this paper addresses financial calculations that employs this methodology using a simplified tabular method.

Financial Calculations

One of the greatest challenges in Safety is to provide reasonable financial calculations regarding the cost-benefits of a Hazard Control. This is so because safety is one of the few activities that, when it works perfectly, ***nothing happens***. Given that most safety violations do not result in accidents, it is very difficult to assess the number of accidents ***that were prevented*** as a result of a given Hazard Control.

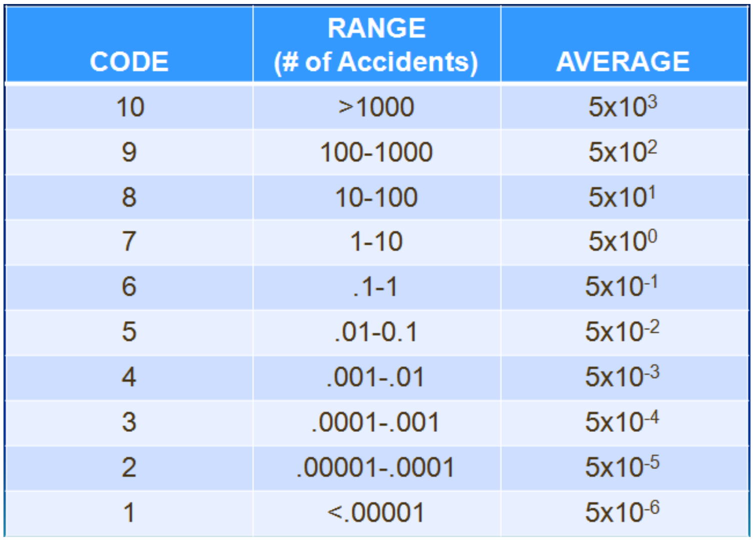
System Safety employs a method known as Total Risk Exposure Codes (TREC) that make calculating total expected losses of a system over a SLC much easier. This approach has inherent calculations that multiply the HS and HP values and integrate additional calculations that estimate the total expected losses associated with a given process over the SLC. The exposure for each hazard is determined by multiplying the probability of a single occurrence (expressed as # of occurrences/100,000 work hours) by the total estimated work hours over the SLC and the number of systems to be produced. Additional definitions appear after the description of each table on the next page.



CODE	RANGE ($)	AVERAGE
10	>$10BIL	$5x10^{10}$
9	$1-10BIL	$5x10^{9}$
8	$100MIL-1BIL	$5x10^{8}$
7	$10MIL-100MIL	$5x10^{7}$
6	$1MIL-10MIL	$5x10^{6}$
5	$100K-1MIL	$5x10^{5}$
4	$10K-100K	$5x10^{4}$
3	$1K-10K	$5x10^{3}$
2	$100-1K	$5x10^{2}$
1	<$100	$5x10^{1}$

Figure 5. Severity Codes.

Ten Severity Codes represent cost per single loss event from $10 to over $10B with each Severity code increasing by an order of magnitude. This allows for assessing losses ranging from minor accidents to catastrophic losses such as those associated with the Gulf oil spill of 2010. These are “loaded” costs including things such as direct medical costs, litigation costs, administrative costs, etc.



CODE	RANGE (# of Accidents)	AVERAGE
10	>1000	$5x10^{3}$
9	100-1000	$5x10^{2}$
8	10-100	$5x10^{1}$
7	1-10	$5x10^{0}$
6	.1-1	$5x10^{-1}$
5	.01-0.1	$5x10^{-2}$
4	.001-.01	$5x10^{-3}$
3	.0001-.001	$5x10^{-4}$
2	.00001-.0001	$5x10^{-5}$
1	<.00001	$5x10^{-6}$

Figure 6. Probability Codes

Ten Probability Codes represent total number of losses for the system over the SLC. For example, a Probability code of 1 means that there is less than 1 chance in a 100,000 that an accident of a given severity from the hazard in question over the SLC. A Probability code of 10 means that it is expected that more than 1,000 accidents will occur in this system over the SLC. Each Probability Code increase represents an order of magnitude increase in the probability of loss event associated with the identified hazard. The TREC table appears below for reference:

	EXPOSURE CODE									
SEVERITY CODE	10	9	8	7	6	5	4	3	2	1
10	20	19	18	17	16	15	14	13	12	11
9	19	18	17	16	15	14	13	12	11	10
8	18	17	16	15	14	13	12	11	10	9
7	17	16	15	14	13	12	11	10	9	8
6	16	15	14	13	12	11	10	9	8	7
5	15	14	13	12	11	10	9	8	7	6
4	14	13	12	11	10	9	8	7	6	5
3	13	12	11	10	9	8	7	6	5	4
2	12	11	10	9	8	7	6	5	4	3
1	11	10	9	8	7	6	5	4	3	2

Figure 7. Total Risk Exposure Table.

Obviously, the TREC table is simply an additions table that adds the HS code to the HP code. The TREC code is then used to calculate the expected losses associated with the process being evaluated using the following formula:

Total Risk Exposure (TRE)= 5 X $10^{(TREC-5)}$

The TRE is useful in estimating the losses associated with a system in its current state but it is most useful in *determining the ROI associated with a given Hazard Control*. For example, if the TREC associated with a given hazard is 10 the TRE calculates to expected losses of $500,000 5 X {$10^{(10-5)}$} If the TREC for that system can be reduced to a 9 through the use of Hazard Controls, the expected losses for that system drop to $50,000 5 X {$10^{(9-5)}$}. This means that an expected savings of $450,000 should be realized over the SLC. This also means that, if the loaded cost to implement that Hazard Control exceeds $450,000, then *the proposed Hazard Control is not cost-effective*. Of course, there may be moral or legal reasons for implementing a Hazard Control that is not cost-effective but we are limiting this discussion solely to financial considerations.

Other Useful Financial Calculations

There are a few additional financial calculations that use the calculated TRE values. They include: (Stephenson, 1991).

These calculations are helpful to “load” the costs of producing end products with the expected losses from the corporate safety performance. In many cases, this information is quite helpful in conveying that concept of Safety as a ***profit center*** rather than an overhead expense.

Hazard Analysis Techniques

An exhaustive overview of all 13 System Safety HA techniques is beyond the scope of this paper but we will provide an overview of 3 of the more-powerful HA tools in this section. These techniques include:

- Energy Trace & Barrier Analysis
- Failure Modes & Effects Analysis
- Management Oversight & Risk Tree

Energy Trace & Barrier Analysis (ETBA)
ETBA is used to identify all energy sources with potential to cause harm and evaluate the Barriers that are intended to contain unwanted releases of energy. As was discussed in the Safety Precedence Sequence section, the use of Barriers placed between humans and energy sources is the second-best method of managing hazards. So, evaluating the effectiveness of barriers in a system is vitally important because it will indicate whether hazards are adequately controlled by barriers or if additional interventions are needed if the barriers will not effectively protect workers.

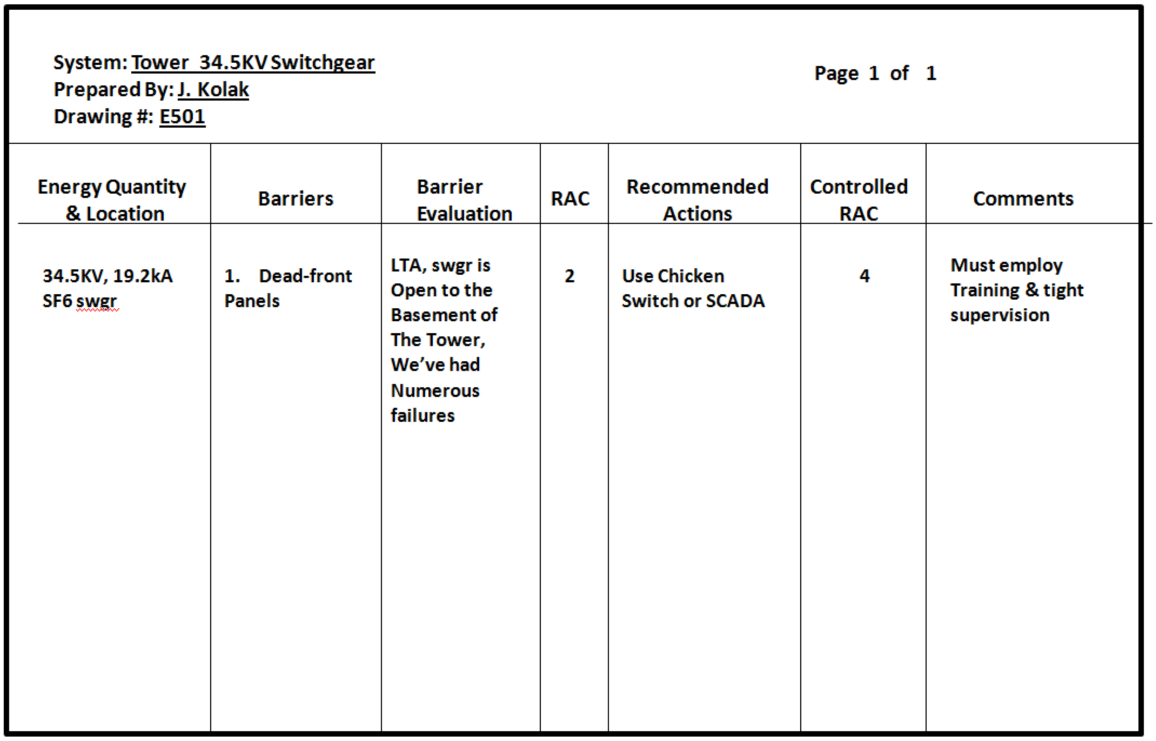
In some cases, ETBA may be needed because systems or sub-systems may contain energy sources that have not been identified by other methods of HA. One example of this phenomena would include “sneak circuits” in electrical equipment where an electrical circuit is wired-into a piece of equipment that isn't supposed to be there.

There are also situations where the Barriers that are intended to contain energy releases are inadequate due to the magnitude of energy being greater than the withstand ratings of the Barriers. An example of this is depicted by the picture below:

Here we see where an electrical arc was generated that breached the metal enclosure that was intended to contain energy releases such as this. Obviously, the Barrier was not up to the task and residual arc-energy was released outside the enclosure. ETBA is intended to

Figure 8: Electrical Arc Breaching Metal Enclosure

identify situations such as this.



System: Tower 34.5KV Switchgear
Prepared By: J. Kolak
Drawing #: E501

Page 1 of 1

Energy Quantity & Location	Barriers	Barrier Evaluation	RAC	Recommended Actions	Controlled RAC	Comments
34.5KV, 19.2kA SF6 swgr	1. Dead-front Panels	LTA, swgr is Open to the Basement of The Tower, We've had Numerous failures	2	Use Chicken Switch or SCADA	4	Must employ Training & tight supervision

Figure 9. Steps in the EBTA

- **Column 1** includes the location and magnitude of ALL energy sources present.
- **Column 2** identifies the type of barriers employed. In this case, the barrier was a "dead-front" panel. Dead-Front enclosures do not have any exposed parts energized to 50 volts or more. Other barriers could include fire-rated walls, machine guards, etc.
- **Column 3** evaluates the effectiveness of the barriers. In this case, the barriers were Less Than Adequate (LTA) because they did not protect personnel located in the "basement" of a wind turbine tower.
- **Column 4** is the RAC in the current configuration.
- **Column 5** includes any recommended changes to the barrier (if necessary).
- **Column 6** includes a "Controlled RAC" which re-evaluates the barrier system after the recommended changes are employed.
- **Column 7** is simply a comments cell. However, if the Controlled RAC was still not adequate, then this would be noted in this column.

Failure Modes & Effects Analysis (FMEA)

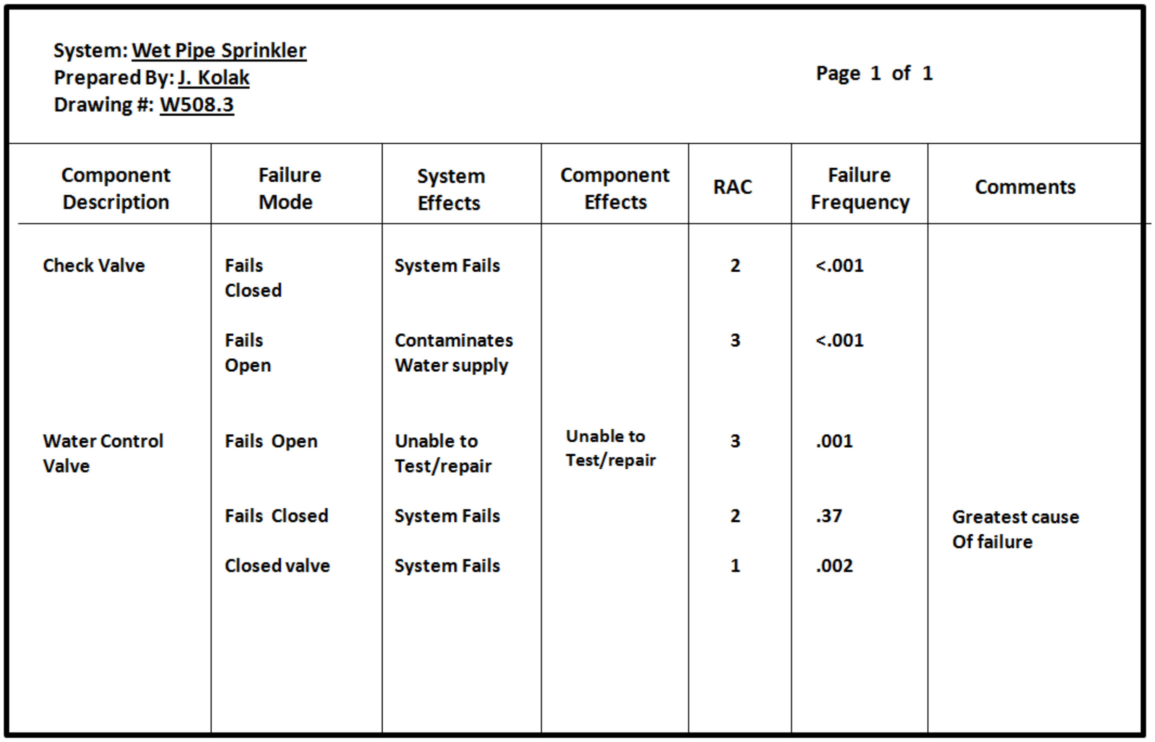
FMEA breaks processes down into individual assemblies and then evaluates the various ways in which these systems could experience failures. Some examples of common "failure modes" include:

- Fails to Open or Close
- Fails to Operate
- Fails to Start or Stop
- Partially operates
- Operates at the wrong time
- Unable to contain energy releases
- Etc.

Figure 10 illustrates an example of where one pole of a 3-pole circuit switcher on a 500,000 volt transmission line failed to open:

Figure 10. Example of one pole of 3-pole circuit failing to open

Here we see the unwanted release of energy (electric arc) caused by the failure of one part of the switch to open as the switch was designed to do. FMEA (see Figure 11) would evaluate the “effects” of this type of energy release on the system. The effects of this type of release can result in loss of system function, equipment damage and the potential loss of life should workers be in the vicinity of the arcing elements.



System: Wet Pipe Sprinkler
Prepared By: J. Kolak
Drawing #: W508.3

Page 1 of 1

Component Description	Failure Mode	System Effects	Component Effects	RAC	Failure Frequency	Comments
Check Valve	Fails Closed	System Fails		2	<.001	
	Fails Open	Contaminates Water supply		3	<.001	
Water Control Valve	Fails Open	Unable to Test/repair	Unable to Test/repair	3	.001	
	Fails Closed	System Fails		2	.37	Greatest cause Of failure
	Closed valve	System Fails		1	.002	

Figure 11. Steps in FMEA

- **Column 1** lists the component description.
- **Column 2** identifies the failure mode. There may be more than one failure mode per component.
- **Column 3** evaluates the effects of the failure mode on the system
- **Column 4** evaluates the effects of the failure mode on the component itself.
- **Column 5** is the RAC for the system in the failure mode.
- **Column 6** includes the expected failure frequency. Although the RAC does take into account the Probability of the equipment failure, this column is useful to compare known operations against the life expectancy for maintenance purposes.
- **Column 7** is a comments cell.

MORT Analysis

The Management Oversight and Risk Tree (MORT) chart is, by far, the most comprehensive accident investigation tool available to safety professionals (author's opinion). Perhaps the most powerful aspect of MORT is that it can be converted to an incredibly-powerful *planning tool* as is explained later in this section. From a practical standpoint, MORT is a graphic representation of the entire Safety System. At last, safety professionals can now understand how the myriad of contributing processes inherent to the Safety System interrelate!

The MORT chart was first developed in 1973 by Bill Johnson, a retired manager for the National Safety Council. MORT was developed to integrate the best aspects of the safety systems within the Atomic Energy Commission and the Department of Defense. MORT

also standardized the approach to Safety Management within high-risk industries such as nuclear and aerospace industries (Stephenson, 1991).
MORT is a “fault tree” in that the “initiating event” is an accident, which is of course a negative or unwanted system output. MORT employs Boolean logic “gates” to evaluate the relationship of safety system elements while also identifying the effectiveness of the various system elements. The two logic gates used are known as “OR gates” and “AND gates.” An “OR gate” means that any of the events below the gate, or any combination of those events, would cause the event that appears immediately above the gate. The event immediately above the logic gate is known as the “Output Event” while the event(s) immediately underneath the logic gate are the “Input” events. Conversely, the “AND gate” means that ALL of the events below the gate MUST occur in order for the event immediately above the gate to occur.

The top two tiers of the MORT chart are depicted in Figure 12 below:

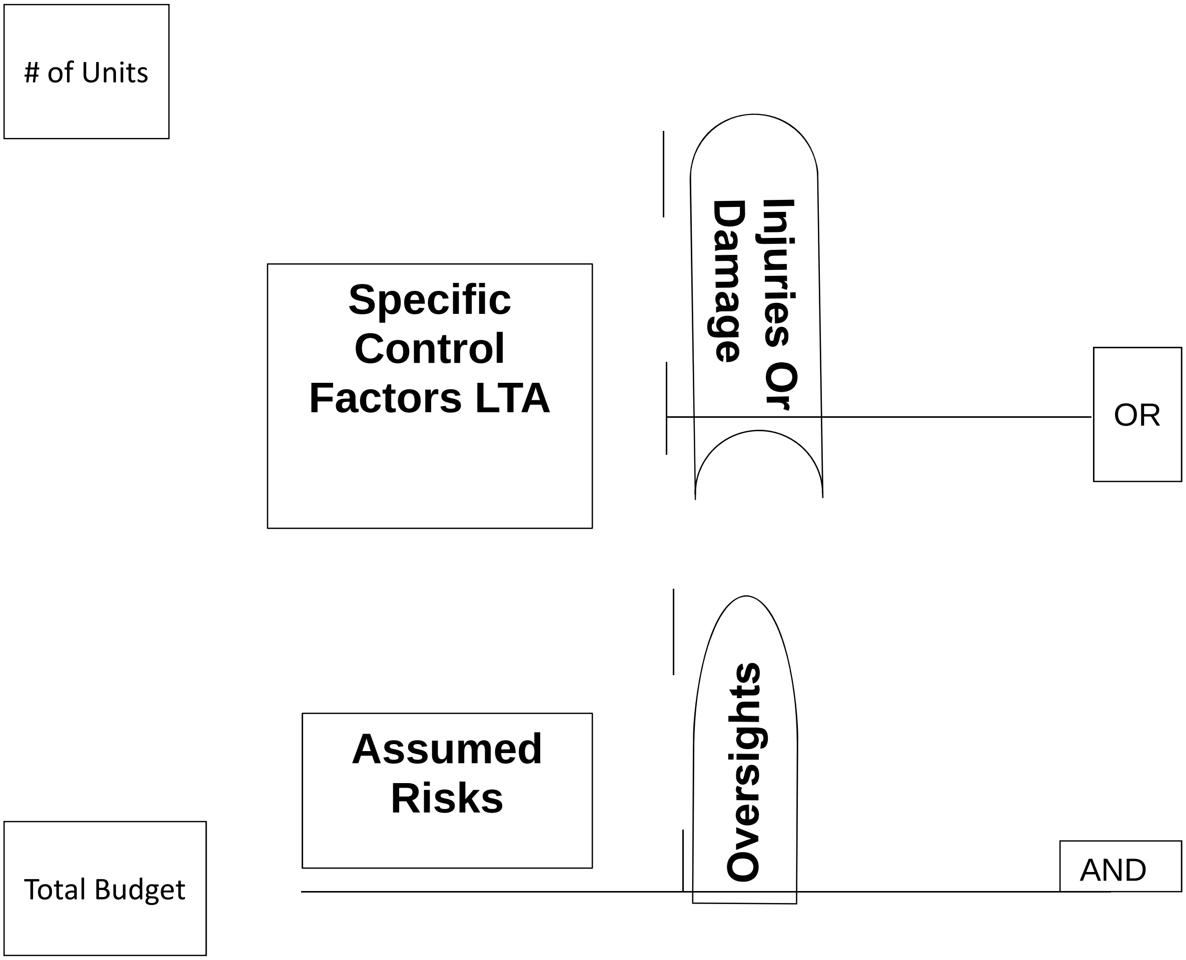


Figure 12. Top two tiers of the MORT chart

The top box (Initiating event) is the accident or system loss. There is an OR gate underneath the Initiating Event that includes “Oversights & Omissions” along with an event called “Assumed Risks”. The correct interpretation of this part of the chart would read like this:

“In order for this accident to occur, either an Oversight or Omission occurred OR management assumed too much Risk, or both.”

Underneath the *Oversights and Omissions* event there is an AND gate and two more Initiating Events called “*Specific Controls Factors LTA*” along with “*Management Systems LTA*”. A proper interpretation of this section of the chart would read as follows:

“In order to an Oversight or Omission to occur, a Specific Control Factor had to be Less Than Adequate (LTA) AND the Management Systems were also LTA”

The words “What Happened” are associated with Specific Control Factors LTA while the words “Why It Happened” are associated with Management Systems LTA. The AND gate associated with these factors reveals two very important points:

1. EVERY accident has at least two causal factors. There had to have been a Specific Control factor failure AND a Management System failure. As was previously discussed, the concept of “multiple causation” in accident investigations is reinforced by MORT here.

2. The “What Happened” includes a failure of one or more Specific Control factors such as Training, PPE, Safe Work Practices, etc.)

3. The “Why” of an accident always includes a failure of one or more Management system. The concept of the General Duty clause included in the OSHact indicates that management is responsible to provide a workplace that is free from hazards that could result in serious injuries and this concept is reinforced by MORT here.

The MORT chart actually consists of over 1,500 items that are all connected to either Specific Control Factors and Management System via logic gates. This configuration allows for two more very powerful uses for MORT, namely:

1. Following the logic gates from baseline events to the accident event allows investigators to *connect seemingly unrelated events to the accident* itself. Many times accident investigations identify various system elements that are LTA but they are unable to make the connection between these dysfunctional elements and the accident event due to the complexity of the system. MORT solves that problem.

2. Because Boolean logic gates are used in MORT, *it is possible to use statistical*

analysis to calculate the probability of the accident event if the probabilities of subordinate events are known.

Perhaps the most powerful aspect of MORT is that it can be converted to a “positive tree” simply by reversing all the logic gates. Converting all the OR gates into AND gates and vice-versa converts MORT from an accident investigation tool to a powerful ***Planning*** tool. This affords safety professionals the most complete “blueprint” of the Safety System that is available (author’s opinion).

Obviously, there is much more to understand about MORT before using it in your organization. There are many publications, including a “MORT Users Manual” and one entitled; “MORT-based Root Cause Analysis” that are valuable tools to assist analysts in getting the most out of this very powerful tool. The purpose of including the discussion of MORT in this paper was to simply introduce MORT to a new generation of safety professionals who will then use this tool to better-protect the employees whom they are privileged to serve.

Conclusion

System Safety techniques are among the most powerful tools available to safety professionals today. They provide a very effective means of assessing Risk along with quantifying the effectiveness of the various hazard controls that may be used to manage hazard exposures.

Use of System Safety tools removes much of the subjectivity out of safety management thus improving the validity of risk-related data that can be provided to management. This adds credibility to safety-related analysis and improves the probability that resources invested in Safety systems will net the desired results.

This paper serves only as a primer for System Safety and the readers necessarily must endeavor to achieve a much-deeper understanding of these powerful tools and concepts. This will take additional effort but the ROI on those efforts cannot be overstated.

Finally, anyone interested in becoming fluent with System Safety tools need not “go it alone” in that there are many safety professionals around the world who regularly use System Safety tools and would likely be happy to assist anyone interested in better-protecting their people.

References

Mims, A. (1993). “System Safety Engineering”. University of Wisconsin-Whitewater. (Lecture).

O’Keeffe, D. (2001). “MIL-STD-882, Its History and Importance.” New England Chapter of the System Safety Society. pp. 9-10.

Welch, N. (2002). “What Is System Safety?” New England Chapter of the System Safety Society. pp. 6-9.

Stephenson, J. (1991). *System Safety 2000*. New York: Van Nostrand Reinhold,. pp. 126-130.