Risk Assessment Challenges to 20:20 Vision

Angela Summers, PhD, PE
President, SIS-TECH Solutions, LP
12621 Featherwood Drive, Suite 120
Houston, TX 77034
asummers@sis-tech.com

Prepared for Presentation at
American Institute of Chemical Engineers
2014 Spring Meeting
10th Global Congress on Process Safety
New Orleans, LA
March 30 – April 2, 2014

Risk Assessment Challenges to 20:20 Vision

Angela Summers, PhD, PE
SIS-TECH Solutions, LP
12621 Featherwood Dr, Suite 120
Houston, TX 77034
asummers@sis-tech.com

Keywords: risk analysis, assessment, human factors, automation

Abstract

Decision makers need reproducible, believable results to support investment decisions. A wide variety of hazard identification and risk analysis methods are available to support process safety decisions. All methods require knowledge in the fundamentals of process design and experience in the process operation under consideration. Every method has uncertainty and no method yields any better reflection of the risk than the level of engagement that the analyst or team has in the assessment. Traditional approaches work well on processes with a long history of operation, but are difficult to apply in the rapidly evolving environment of modern manufacturing.

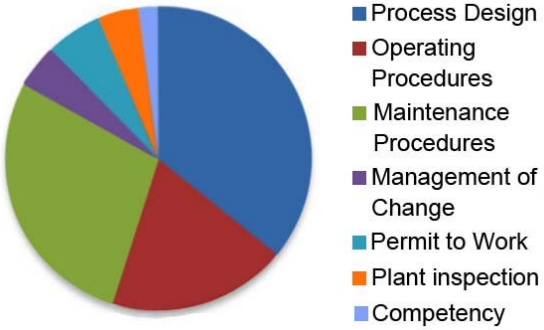
This paper discusses the challenges that the risk analysis process is facing in today's work environment. These challenges include advances in chemical manufacturing techniques, the rapid evolution of vogue practices, the focus on hazard scenarios, the false security of calculations, the rampant pace of technology change, and the increase in complexity of human and automation interaction.

1. Introduction

Process safety is achieved through a balance of inherent and functional safety management. Inherent safety is the academically preferred means to ensure that a production process does not pose risk. Many industry sectors have proven resistant to changing their production methods due to existing knowledge, infrastructure, and cost. The practical limitation is that a significant fraction of chemical processing involves the handling of hazardous chemicals under hazardous conditions. The choice of one production method over another is rarely a choice between one that poses no risk and one that poses high risk; rather it is often the choice of one incident pathway versus another with different degrees of unacceptable risk. Consequently, inherent safety only reduces the process risk so far and the remaining risk is typically addressed through functional safety, where sufficient safeguards are implemented to reduce the probability of event occurrence to a tolerable level. As process risk increases, safety becomes more dependent on functional safety, which relies on thorough hazard identification and rigorous risk management plan.

The belief that all loss events are foreseeable, given sufficient analysis, is very alluring. Throughout the life of a manufacturing process there are opportunities to examine risk; to apply more complex methods; and to give hazard scenarios and their avoidance more thought. The reality is that it is difficult for most people to think outside the box and to honestly look at how the process can misbehave. It is easy to accept that if nothing has happened before, nothing will happen in the future. The harsh reality is that even if it hasn't happened and you don't know that it can happen, it can still happen.

It is not realistic to think that hazard and risk analysis identifies everything that could go wrong. An HSE incident analysis [2] determined that more than 1 in 5 loss events are due to the "organization failing to fully consider potential hazards or causes of component failure." The vast majority of incidents (81%) were the result of the organization failing to adequately plan and implement procedures for risk control, including the design of the process (25.6%), the provision of operating and maintenance procedures (15.6% and 22.6%, respectively), the management of change (5.7%), a permit to work system (4.9%), plant inspections (3.5%), and ensuring competency (1.7%) [2].



Most risk analysis methods rely on a host of design and management assumptions and checklist data from industry benchmarking. The risk analysis process assumes that the process safety management plan and associated procedures are sufficient to lower the risk to a tolerable level. The analysis is intended to be the arbiter, but the choices of the boundary, causes, scenarios, events, performance claims, and criteria provide as many opportunities to get it wrong, as to get it right.

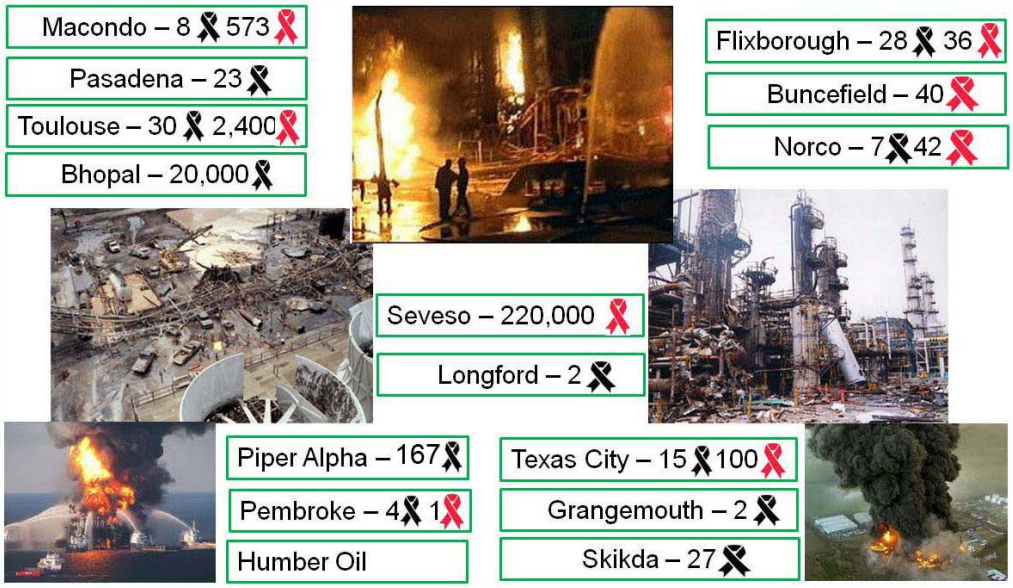
Every new method claims to be better than the last. Intellectual curiosity and the pursuit of a "correct" answer often drive implementation of more complex methods and calculations. Making things more complex can give the illusion of accuracy, but can also create a situation where team members do not understand the method, become disengaged from the process, and allow the facilitator (or analyst) to dominate the risk analysis. Some of the current vogue methods have so many degrees of freedom that a good analyst can get nearly any answer desired. Each method shares the same systematic flaw; the risk judgment is only as good as the data and model certainty, which are highly influenced by the competency, experience and knowledge of team

members and the availability of functional specifications, safe operating procedures, and operating and maintenance history.

2. A history of losses

Over the last 30 years, industry has suffered significant losses due to process safety events. These events have more than high cost and significant impact in common. The attributed causes are similar. Each process had been subjected to multiple assessments of the likelihood and consequence of significant events. The assessments involved different methods, conducted by different individuals and often supported by independent consultants. The hazards were known and accepted, as the way things were with the pervasive belief being that the event was highly unlikely to occur. There was little acknowledgement or planning for event escalation, so when the event began to unfold, the plant personnel who had the greatest opportunity to stop the incident were overwhelmed.

In contrast to the common single cause-consequence paradigm, multiple causes and latent conditions were also present, although a primary root cause was identified for each specific accident. In most cases, the accident was not a sudden failure occurrence, but an evolving set of conditions that lined up in a dangerous manner: instrumented systems relied upon for control and monitoring did not work properly; and operators misinterpreted or ignored available data. Plant personnel often suspected abnormal operation, but investigation and correction were delayed. Unsurprisingly, there was a strong belief that the control and emergency systems were capable of preventing extensive harm. However, this belief was unfounded because the alarm, shutdown, and emergency isolation systems proved to be insufficient when the event unfolded.



In every event, competent people with knowledge of the process, equipment, operation, and history did not acknowledge that the conditions for failure could be (or were) present. Is this a case of culpable ignorance, refusing to acknowledge the unmitigated risk, or confirmation bias, looking only deep enough to confirm the belief that everything is ok as is? A lack of understanding of how a process misbehaves or a refusal to believe that harm is possible

inherently limits the capability of responsible personnel to correctly assess and manage risk. A big risk is not addressed by a big list of poorly managed safeguards or a list of nothing; it is addressed by the right list of rigorously designed and managed safeguards [3, 7, 14].

3. Challenges to 20:20 vision

Omniscience is not possible, but it is possible to see risk more clearly. 20:20 vision requires removal of the rose-colored glasses, an end to confirmation bias, and a realistic assessment of risk. So, let's examine some of the challenges faced in gaining 20:20 vision.

3.1 Running before you walk

The best of industry pride themselves on innovation, which requires that the process be pushed beyond the norms and typically past the known. The greatest technology leaps involve a crash and fix strategy, where each generation of equipment becomes safer. While processing innovation and quality standards may push the boundaries of automation and its control algorithms, sufficient theory and standards exist to ensure that process equipment can be operated safely [3].

Predictive methods are applied to identify incident pathways that occur during abnormal operation and to determine what must be done to prevent loss events. These methods require knowledge and experience from the process designers, operations, and other experts. An inherent weakness of predictive methods is a vulnerability to: a lack of competency, incomplete information, and deficiencies in hazard awareness and design. Where there is limited operational knowledge, there is an associated limited awareness of how sensitive the process is to deviation. Limited but successful operation with complex processes – no crash – sustains the belief that everything is safe as is.

Risk analysis is a tool to ensure that an appropriate standard of care is applied; it is not a tool to prove whether safeguards are needed or not [13]. The treatment of any analysis as a means to determine the maximum safeguards required rather than the minimum is a bad process safety practice. Risk should be driven as low as practicable and safety controls, alarms, and interlocks are always practicable (though sometimes an alarm may not be sufficiently effective due to human factors). Every process needs a holistic loss event prevention plan that includes:

Inherent safety

- Robust vessel and piping design, so process deviation is tolerable.

Functional safety

- A reliable control system that reduces the frequency of abnormal operation.
- An alarm to notify the operator that the process is experiencing unacceptable abnormal operation
- A shutdown that sequences the process

to a safe state when the process reaches an unsafe condition

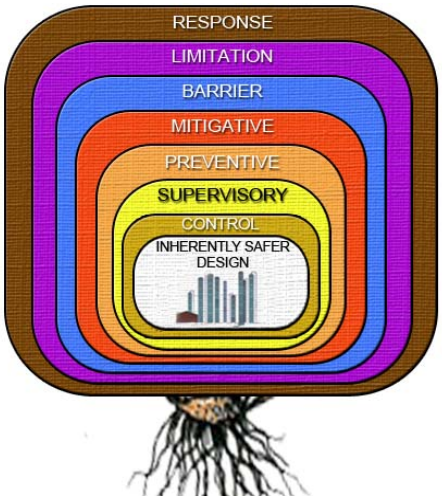
- An emergency shutdown system that isolates the process from its supply when loss of containment occurs
- Other safeguards as necessary to address loss of containment and event escalation

The best engineering processes are agile and adapt as new information becomes available, however some project teams cannot resist the temptation to push the hard, and often costly, decisions to later teams and work activities, especially decisions related to reducing process risk. "For every complex problem, there is at least one solution that is simple, plausible…and wrong," Bill Doyle, the great loss prevention engineer. Consider the limits of what you know, then add a good-sized measure of bad luck. It is wise to have a sense of vulnerability even when you have done your best to design a safe plant [3, 7, 13]. It is sensible to implement safeguards that prevent the loss event rather than simply relying on probabilistic analysis.

3.2 Holy moly, that onion makes me cry

The onion-skin and Swiss cheese models of incidents are ubiquitous to process safety. These models are typically used as an analogy for layers of protection. On first glance, each shows the layers as independent of each other, where the failure of one layer does not impact the other. On further study, the graphics portray much more.

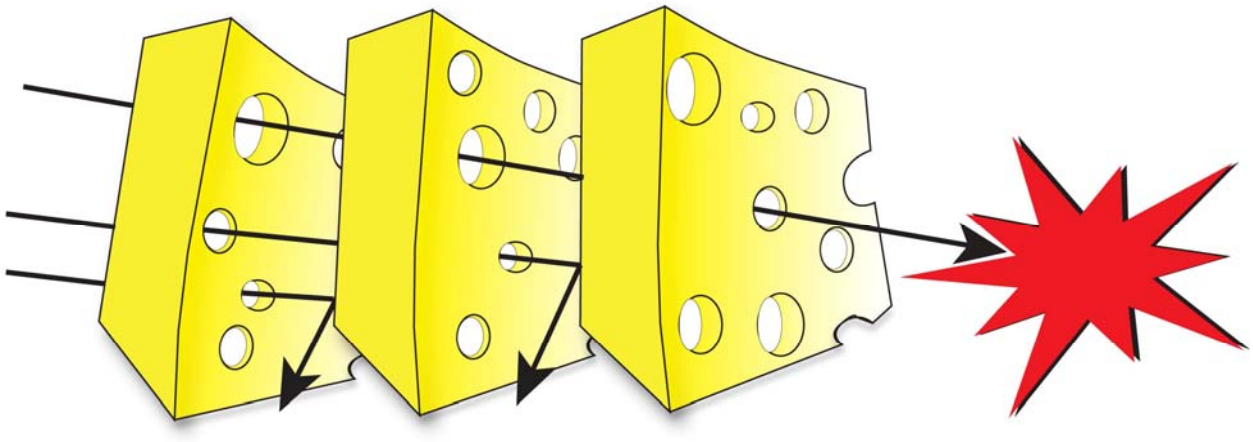
The onion-skin visualizes the sequence of barriers that control, prevent and mitigate major accidents. Layers of protection are as independent as the layers of an onion. However, as any cook knows, the structural integrity of the onion depends on keeping the layers attached to the base. The onion layers originate at the base and without it, the layers fall apart. The integrity of the base of the layers of protection is determined by the functional safety management system applied to prevent human error.



Many human factor issues impact every layer. The more complex or specialized the layer is, the higher the potential for human error. A company's culture toward manual operation of control loops, bypassing safety instruments or continuing operation with known faults can result in multiple risk sources being turned over to operators across a facility. The layers of protection can only be as strong as the rigor applied in identifying and preventing human errors and systematic failures.

James Reason's Swiss cheese model [5] has been adapted to illustrate each barrier as a cheese slice possessing holes that represent deficiencies in barrier performance due to random and systematic faults. Seemingly independent systems can fail due to common systematic mechanisms that degrade or disable multiple similar systems. The graphic emphasizes that barriers are not perfect over their life and that an accumulation of deficiencies (increasing

number of holes in each cheese slice) increase the likelihood that holes will line up, thus allowing an event to propagate past the barriers. The holes open and close dynamically as management systems identify and correct faults, so the better managed the barriers, the fewer, smaller, and more transient the holes will be.



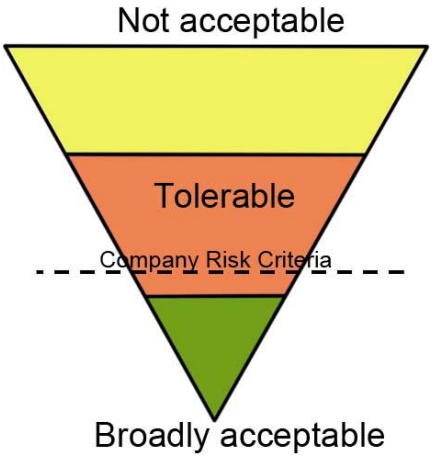
Resources and infrastructure are typically shared as similar equipment, procedures, and people are used to design, operate, maintain and test barriers. All barriers share the operational intent that normal and customary production should occur efficiently with minimal disruption. Dependencies, whether internal or external to the barrier, must be identified and managed throughout the life of the process.

Barrier reliability is affected by the site operational discipline and safety culture. For example, poor maintenance practices will cause numerous devices to operate deficiently across a site. An HSE study [6] determined that 32% of reported "loss of containment" incidents were caused by process and safety equipment failure due to inadequate design and maintenance. To prevent incidents, personnel, procedures, and equipment must be aligned to facilitate rapid identification and response to failures of the system and protective safeguards [7]. Safety is not a one-time effort. Consistently achieving an order of magnitude of risk reduction (let alone multiple orders of magnitude) from automated systems is hard [4]. Safe operation requires diligence: systems change, operations and management expectations change, and the operating environment changes over time.

It is undeniable that safe operation and process reliability are not only compatible but highly interrelated. Reliable production units rarely have safety incidents, whereas unreliable ones tend to repeatedly experience abnormal operation. Safe and reliable performance requires minimization of the root causes that lead to abnormal and emergency operation. The challenges to accomplishing this are considerable, but not insurmountable.

3.3 Excessive reliance on risk criteria

According to ISO/IEC Guide 51 [8], safety is “freedom from risk that is not tolerable.” Within the context of the ISO standard, the words acceptable and tolerable are synonymous. Tolerable risk is defined as the level of risk that is accepted in a given context based on current values of



society. Most professional discussions about society values revolve around the probability of occurrence of specific types of harm – physical injury or damage to the health of people, or damage to property or the environment. In the last decade, use of risk criteria to determine the required safeguarding has become endemic within the risk community. In some companies, even safeguards recommended by industry practices are not added unless the risk analysis demonstrates the safeguard is required.

The wise are mindful of the Andrew Lang quote, "He uses statistics as a drunken man uses lamp-posts... for support rather than illumination." Statistics seem concrete and defensible but the estimates are very fragile given the vast range of assumptions in most analyses and the lack of actual process data to substantiate performance claims. Any wrong assumption propagates through the analysis, affecting multiple scenarios and in some cases the fundamental basis of the entire analysis.

Designing by risk criteria is attractive, as it seems to provide a shield against claims that not enough has been done to reduce the potential for an incident. The perceived protection afforded by risk criteria falls short when, post-incident the question is asked whether something else could have been done and the answer is "well, we could have…" The value of the analysis is not the math, but *what is learned about the safety and security vulnerabilities of the operating plan for the process and what is done to improve system resilience against these vulnerabilities.* The intent of the math is to allow options to be benchmarked against one another based on a similar set of assumptions and to demonstrate that risk has been reduced below a maximum threshold. The risk of process safety incidents should be reduced as low as practicable given readily available technology and accepted practices. Then, see *Running Before You Walk* above. You may need more.

3.4 No such thing as a perfect 10

When an onion layer or Swiss cheese slice is cited as a cause of or a protection layer against a loss event, the frequency or probability of failure is estimated. With the emergence of LOPA as a dominant risk analysis method, the habit of selecting values based on the number 10 has become pervasive. Multiples of 10 are easy to understand and anyone can multiply 10 x 10 to get 100. Risk analysis does not have to be easy, but it does need to reflect what is achievable in the actual operation. Few loss-of-control events would ever propagate to loss of containment if the practices necessary to achieve the claims of 10 were as pervasive.

The control layer must reflect industry best practices for control system design and management in order to achieve a failure rate less than 1 in 10 years. As more users track the demands on their safeguards, they are finding that the number of alarms, trips, and pressure relief valve lifts exceeds the frequency assumed in the analysis.

The safety layers must be designed and managed according to good engineering practices documented by recognized industrial organizations. A risk reduction of 1 in 10 means that 1 in 10 times the layer is called upon to work, it will not. Design and manage to achieve 0 failures. Don't assume a risk reduction of 10 without justification, because achieving a probability of failure of 1 in 10 requires planning and discipline.

The potential for loss events is directly related to the operational discipline that ensures the demand rate is less than expected and the assumed safeguard reliability is achieved during actual operation. At plant sites, personnel work to reduce operating and maintenance costs in spite of the higher cost of supporting an aging infrastructure. If maintenance of equipment is reduced the failure rates can escalate.

To demonstrate that the process is operating in a safe manner, procedures should be implemented to evaluate the demand rate on the layers during actual operation and compare the performance of each layer against its safety requirements. Document and investigate abnormal operation that leads to a demand on a layer and the operating and maintenance records that indicate performance problems. Procedures should define the corrective action to be taken if the challenges are too frequent or the actual layer performance does not achieve the necessary risk reduction. Investigate the underlying causes to determine what those involved in plant operation and maintenance think ought to be done to improve the reliability.

3.5 Avoid scenario tunnel vision

An event always seems obvious when the scenario is being evaluated. Most events are treated as discrete, i.e., everything is normal and then one variable becomes bad and the team chases the event down the tunnel. In the real world, process deviations propagate through the process' other deviations and the operator sees an array of events happening simultaneously. The event may be precipitated by other control system failures requiring controller overrides and manual control. An HSE study [6] reported that 37% of the

reported loss of containment incidents resulted from incorrect operator action. The root causes of the actions were inadequate operating procedures, deficient process design, inadequate supervision, and ineffective management of change.

Operators are reliant on control and safety systems for process information. Current control room siting practices are moving operators farther from the production equipment. In highly automated facilities, process safety depends on situational awareness that is provided by a computer screen, flashing lights, and sound. Many studies list human error as a cause for an event without consideration for the automation that is providing the operator with data and status information. Without the control system, the operator cannot act on the process safely. Without the operator, control system malfunction can propagate to an unsafe condition. For many events, it is difficult to separate automation design from human error.

The operator's ability to maintain situation awareness is continually challenged as many operator interfaces have become clouded with excessive graphic detail and data reporting. How does the operator recognize which scenario is occurring and respond with the right action at the right time? Situational awareness is necessary and this comes from experience and process simulation, not from probabilistic analysis of a single process deviation.

3.6 Beware vogue methods

Nassim Taleb [9] uses Aristotle's black swan as an expression of a rare and unpredictable event and discusses the tendency everyone shares to look for simplistic explanations after their occurrence. Many hazards and risk analysis studies appear to be:

- Checklist oriented
- Focused on filling out analysis workbook
- Ignorant of human factors and systematic issues
- Naïve concerning complexity of the actual event and its potential for escalation

To address these problems many have proposed that more complex analytical methods be applied. Every year it seems that someone is proposing a new practice destined to become another vogue solution to identifying risks and preventing their occurrence. It is easy to fall into the intellectual trap of believing in an analytical perfection in which one "knows" what the risk is. This is unrealistic. Every study has a defined purpose and boundary, and current practice dictates that the analysis focus on individual deviations from intended operation rather than the event as an evolving scenario affecting the process as a whole. Do not become enslaved by the analytical method.

The chosen analytical method can affect outcome quality, but the relationship of the results to the real-world has a great deal more to do with the experience of the people participating in the study

than to the methodology itself. Some methods are simple, easily adapted to a wide variety of applications and yield fast results. Repeatability can be a problem since simple methods typically do not have the rigid framework and information structure of more complex methods. However, their flexibility means that they can support a wide range of risk decisions during process design, equipment, procedure, and organizational change, operation and maintenance plan change, etc. Complex methods often present the analyst with a more detailed framework for the assessment, but are time consuming and error prone due to the level of skill required in executing the method correctly. Given the procedure and a set of data assumptions, complex methods yield a high degree of repeatability, so complex methods are typically relied upon to support major investment decisions, such as facility siting or the use of non-customary protection layers.

A problem with the complexity of the latest methods is that too much time is being spent fitting data into a fixed framework of how an event evolves. The use of various factors has become rote to the point where no one seems to question the validity of the assumptions. Freethinking is rarely encouraged, because everything needs to fit within a cell in a data table. Hazards and risk analysis is only beneficial in identifying hazards and documenting the prevention strategy if applied with a freethinking attitude of a private detective. Brainstorming on common cause and human factors should be encouraged otherwise only the obvious is assessed and less obvious mechanisms are ignored.

3.7 Beware hypnotic lure of calculations

Quantification is not a panacea. Manipulating numbers can make loss events seem more theoretical and probabilistic rather than real events that hurt real people. The detachment afforded by a calculation encourages confirmation bias unless the methods are backed with real data. Anyone with experience knows that there are significant limitations to what is considered in most quantitative analysis and that there is a high degree of uncertainty associated with the data. Calculations are only good for estimating things that can easily be measured. For this reason, human factors are often excluded from risk calculations even though human factors are typically the dominant cause of failure.

Certainty in the estimate only comes when the data are justified by real measurements rather than theoretical. In order for a risk model to come close to reality those participating and leading the analysis must understand how the method works and its underlying assumptions. Benefit is derived when a method is used in the right way for the right application. Risk analysis is not easy and no one should be fooled into thinking that anyone can facilitate a hazard identification study or do risk calculations because the equations are simple or because software is perceived to take care of it. Computer software is available that takes care of the calculations, reduces math errors, speeds data entry, and produces consistent documentation. These benefits do not take away the hard part that involves understanding the assumptions, limitations, and proper application of the risk analysis method.

3.8 Don't depend on luck factors

Conditional modifiers are considered when the risk analysis is estimating the frequency of the loss impact rather than the loss occurrence. Impact analysis has its application within certain decision-making processes, but the goal of process safety management is, or at least should be, the prevention of loss events. Consider that the worst credible scenario is one where the conditional modifiers approach 1. Even a minor release can escalate into a large loss event under the right conditions at the wrong time. Event escalation is rarely, if ever, discussed and in most cases events are assumed to only cause damage to the equipment under assessment.

Do not use conditional modifiers in the risk analysis without justification. The rationale should consider event dispersion and flammability analysis, assessment of the loss prevention and emergency response plan, and the site culture in controlling and monitoring the conditions that increase the likelihood of the worst-case scenario [10,14]. Dr. Clifford Nass, a Stanford professor who pioneered research into how humans interact with technology warned, “denial is the greatest enabler.” Every effort should be made to install equipment that has a reduced potential to serve as an ignition source, but during a loss of containment ignition sources are freely available. P. F Urben[11] wrote, “It is hubris to imagine that we can infallibly prevent a thermodynamically favoured event." In the process industry, ignition sources are so freely available that Trevor Kletz[12] believed that the fire triangle should be “Air + Fuel = Bang.”

4. Functional safety management

Many companies have well-established training and employee motivation programs around the safety message of “zero” whether related to loss of containment, injuries and fatalities, or environmental impact. The expectation is that each individual will choose to act safely when executing their daily tasks if the company emphasizes the importance of safety. History has shown that these messages do not carry the same weight as the message of what gets resource and budget allocation and what does not.

A variety of factors are considered in determining whether a company has acted reasonably to prevent the loss event. These factors include the company’s care and skill in producing its product, its awareness of the harmful event prior to the incident, the activity being performed, the specific circumstances that led to the incident, and whether the company did what it could to prevent the incident’s occurrence. Proof of safe operation is gathered by monitoring and reporting actual performance over the life of a process. Benchmarked values provide an initial basis and rationale for the design, but operating history yields the actual frequency of root causes (or initiating causes), process deviations (or initiating events), and work orders related to safeguards (or failures on demand) [1]. Data feedback to the risk analysis process is critical to credible decision-making.

An effective process safety management program uses a systematic approach to understand and control the risk of the whole chemical process. The ultimate goal is to prevent the unwanted release of hazardous chemicals, materials, or energies, which impact people, the environment, or the process equipment. Success depends on rigor of the systematic approach applied to develop a loss event prevention plan, to prioritize risk reduction opportunities, and to support the

organizational discipline necessary to fully implement the plan. With good methods, realistic risk criteria, and appropriate data feedback processes, management is well-equipped to see clearly the amount of resources and money needed to achieve zero losses.

5. References

[1] Summers, Angela E. and William H Hearn, “Quality Assurance in Safe Automation,” Process Safety Progress, 27(4), pp. 323-327, December 2008.

[2] Health and Safety Laboratory. “Loss of Containment Incident Analysis.” Sheffield UK, P.5, 2003.

[3] Summers, Angela E., “Safe Automation Through Process Engineering,” Chemical Engineering Progress, 104 (12), pp. 41-47, December 2008.

[4] Summers, Angela, “Safety controls, alarms, and interlocks as IPLs,” Process Safety Progress, published online, October 2013.

[5] Reason, James. “Managing the Risk of Organizational Accidents.” Haut UK, Ashgate Publishing Limited, 1997.

[6] Health and Safety Executive, Findings from Voluntary Reporting of Loss of Containment Incidents, 2004/2005, 2005.

[7] Summers, Angela E., “Safety Management is a Virtue” Process Safety Progress, 28 (3), pp. 210-13, September 2009.

[8] ISO/IEC. *Guide 51 Safety aspects – Guidelines for their inclusion in standards.* P.2, 1999.

[9] Taleb, Nassim N., The Black Swan: The Impact of the Highly Improbable, 2 edition, Random House Trade Paperbacks, ISBN: 978-0812973815 May 11, 2010.

[10] Summers, Angela E. and William H. Hearn, “Risk criteria, protection layers, and conditional modifiers,” Process Safety Progress, 31(2), pp. 139–144, June 2012.

[11] Urben PG. “Learning from accident in industry: Trevor Kletz.” Journal of Loss Prevention in the Process Industries, Vol 2, No 1, P. 55. Jan 1989.

[12] Kletz, Trevor. *Learning from Accidents*, 3rd edition. Gulf Professional Publishing, 2001.

[13] Murphy, John F., “Beware of the Black Swan,” Process Safety Progress, pp. 330–333, Dec. 2012.

[14] Summers, Angela, William Vogtmann, and Steven Smolen “Consistent consequence severity estimation,” Process Safety Progress, 31(1), pp. 9–16, March 2012.