Session No. 513

The Case for Inherent Safety: A Review of the Principles of Inherent Safety and Case Studies of Tragedies

Stephen J. Wallace, PE, CSP
Wallace Consulting Services, LLC
Washington, DC

I. Introduction

In the hierarchy of controls, designing the hazard out of the process is the preferred method. Although this approach makes sense, designers do not always apply this concept to the fullest extent. The only way to ensure that accidents do not happen is to apply the principles of inherent safety (IS) throughout all life cycles of the process. Administrative practices, such as requiring PPE or shielding personnel from hazards, will only be effective as long as all other factors that could affect safety are perfect. Unless a process is inherently safe, accidents will likely happen if enough time is allowed. In addition to preventing accidents, IS principles will also protect processes and the general public from deliberate attacks on manufacturing facilities, such as acts of terrorism. This paper discusses the principles of IS, and discusses case studies where application of these principles would have prevented catastrophe.

II. Background: Principles of inherent safety

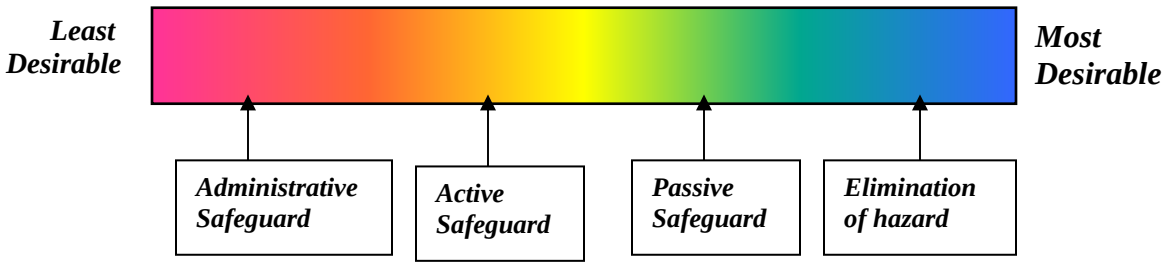
2.1 Introduction

To make a facility inherently safe means to remove hazards so that accidents will not happen. The hazards can be in the form of toxic or flammable chemicals, unsafe process conditions, design flaws that lead to injuries, or work processes that can introduce hazardous situations.

At its core, IS involves analyzing risks and challenging the premise that the hazard should be there. This approach is contrasted with accepting that the hazard exists and deciding how to "work around" it. When safety practitioners consider how process, work practice, or workplace design issues can cause undesirable consequences, they should always examine why the hazard has to be present.

Although the preferred method is to design the hazard out of the system, IS principles may involve making the process inherently "safer" rather than absolutely safe. On the continuum, the safety professional should always be pushing to go to the next level, from using administrative procedures to protect workers, to using active measures such as interlocks, to using passive measures, to the ultimate solution of designing the hazard out completely (Figure 1).

Figure 1. Preferences in Protections from Hazards



The progression of questions that can be asked during a review for inherent safety include:
What is the hazardous material, situation, or procedure?
What administrative and hardware controls are in place?
Are controls passive such that they will never fail? (e.g., dikes to collect spills)
Do the controls require that hardware or a person take an action?
Does the hazard even need to be present, or can it be eliminated?

Safety professionals must work closely with design groups and embed these concepts into engineering and design specifications so that IS principles will be considered. And while it is easiest to make modifications while a facility is being designed, practitioners do not always have that luxury and must work with a facility that has already been designed. This analysis should be applied to existing facilities that have chemicals, work places, and practices, understanding that an interim fix need to be implemented until a more permanent solution can be developed.

2.2 IS applied to hazardous chemicals

Applying IS concepts to reduce the risk of hazardous chemicals means that process designers use strategies of safer chemistry, rather than control systems and operator intervention, to prevent accidents. The different elements involved in designing inherent safety into facilities include:

- Intensification (using smaller quantities of hazardous materials);
- Substitution (replacing material with less hazardous substances);
- Attenuation (using less hazardous conditions or a less hazardous form of a material);
- Limiting of effects (designing facilities that minimize the impact of releases); and
- Simplification/error tolerance (designing facilities that make operating errors less likely or less consequential). (CCPS, 1993)

The first three elements above involve using smaller quantities or less hazardous materials, which can be very effective but challenging to implement. Designers should consider if they can apply intensification to the process, such as keeping smaller supplies of raw materials on hand. Safety practitioners may occasionally encounter resistance from production personnel since a lower inventory of raw material may cause production problems if there are upsets in the supply. But the case has to be made that smaller inventory also means that there is less material that may be released during an accident. However, exercise caution and consider unintended consequence when using intensification. For example, decreasing the size of chlorine cylinders kept onsite may increase the need to have more change-out of cylinders, which is a risk that must be managed. Substitution should always be considered as an option. For example, in the case of water

treatment, designers should consider if less hazardous material can be used in the process, such as sodium hypochlorite rather than chlorine.

Limitation of effects involves designing facilities and equipment in such a way as to minimize the impact of releases. Ensure that separation distances between hazardous material unloading, storage and processing are adequate. Facilities should be designed to minimize the need for transportation of highly hazardous materials. Distances to sensitive receptors, such as residential communities, should be considered in the design. Adequate buffer spaces should exist between sensitive receptors and hazardous installations. Facilities should be located in proximity to utilities, emergency response support, and adequate water supplies.

Finally, equipment in facilities should be designed to minimize errors or make them less consequential. Equipment can be designed so as to ensure that flow rates are within safe limits, by choosing pumps and sizing lines appropriately. Vessels should be designed for a full vacuum (-14.7 psig) if the possibility exists for pumping materials out with the vents closed, or if hot vapor may become trapped and condense. Reactors should be designed to withstand the maximum allowable pressure and eliminate the need for a large emergency relief system. Piping systems may be designed to eliminate components susceptible to leakage, such as sight glasses or flexible connectors.

2.3 IS applied to occupational hazards

Although much of the information on IS principles applies to design issues related to hazardous chemicals, the same principles also apply to occupational hazards such as noise, ergonomics, hard surfaces, and walking/working surfaces. For example, consider the five design strategies discussed in the previous section related to a noisy workplace. Rather than accept that the level of noise is fixed and requiring operators to hear hearing protection, consider if the work could be accomplished by using a smaller or redesigned machine that makes less noise (akin to intensification). Perhaps collections of machines could be separated so that their synergistic noise effects are lessened. If the machine cannot be replaced and the noise level cannot be changed, another approach would be to consider if operators need to work in the area at all.

This same approach can be utilized to address other occupational issues. Many progressive organizations design workstations to prevent musculoskeletal disorders. Also, organizations are taking actions such as purchasing slip resistant flooring for walking surfaces.

2.4 IS applied to procedures

When work must be conducted in a facility, IS principles can be applied to those practices as well. Most organizations have permitting systems to provide checks before the work is performed; however, a more progressive approach is to determine if the work can be performed in a less hazardous area, or if the work needs to be performed at all. For example, if the work involves welding, consider if it can be performed in a maintenance shop rather than a process unit.

III. Case studies

Following are some case studies that illustrate IS principles and show the effect of not applying such principles to the workplace. These and similar incidents show that organizations must undertake comprehensive reviews of their work places to ensure safety.

Case Study 1: Lack of controls for reactive material, location of control room, storage of large quantities of material onsite

Incident Brief
A large fire and explosion occurred at a facility in Pascagoula Mississippi that manufactured dyes, rubber, and agricultural chemicals. A chemical used in the process was mono-nitrotoluene (MNT), which is highly reactive when exposed to heat. Material was left in a reactor while the unit was shut down. Steam leaked through a manually closed valve for several days, which heated MNT left in the bottom of the reactor.

The material exploded, resulting in shrapnel from the reactor being propelled throughout the facility and offsite. The debris hit a storage tank containing a large amount of MNT and caused a fire that lasted almost three hours. One piece of the reactor - weighing about 6 tons - landed a few feet from a large crude oil storage tank in an adjacent facility, almost resulting in an even larger fire. The control room for the unit, located approximately 50 feet from the reactor that exploded, was damaged during the explosion. Operators inside were cut by shattered glass.

Discussion of Inherent Safety Principles
This incident illustrates a number of IS concepts that were not employed. The hazards present included the reactive chemical, surrounding equipment with flammable material inside, and a control room in proximity to the unit. There were insufficient controls on the reactor to positively stop steam flow when the material started heating up. Since operators were relying on a single manual valve to prevent steam flow, there were also inadequate work practices to ensure isolation from the heat source. Such practices would include double blocking and bleeding the line or installing blinds. The practice of leaving inventory in the reactor when the unit was shut down was unsafe. The fire caused by the release of material (after the tank was struck by shrapnel)

illustrates that inherent safety at the source of the explosion was the only way to prevent additional releases.

A more comprehensive analysis also shows that the placement of the control room 50 feet from the reactor was inherently unsafe. Also, process engineers should consider if another less reactive chemical could be used in the process, or if smaller quantities could be used and stored onsite. On a larger community-wide scale, this incident illustrates that the proximity to an adjacent facility meant that zoning requirements should have considered the potential synergistic effects of having two facilities with hazardous materials located side-by-side.

Case Study 2: Containment of release, placement of trailers near operating unit, tolerance of operator error

Incident Brief
A large explosion occurred in the Isomerization Unit at a refinery in Texas. Operators inadvertently sent too much material to a vessel during a startup. The column overpressured and the material flowed to a knockout drum, which overfilled. The material then flowed into a stack, which was open to the atmosphere. The cloud of flammable material then flowed out the stack and contacted an ignition source nearby. A series of explosions occurred, impacting contractor trailers that were in the area. Fifteen people that were in and around the trailers died, and several people were injured.

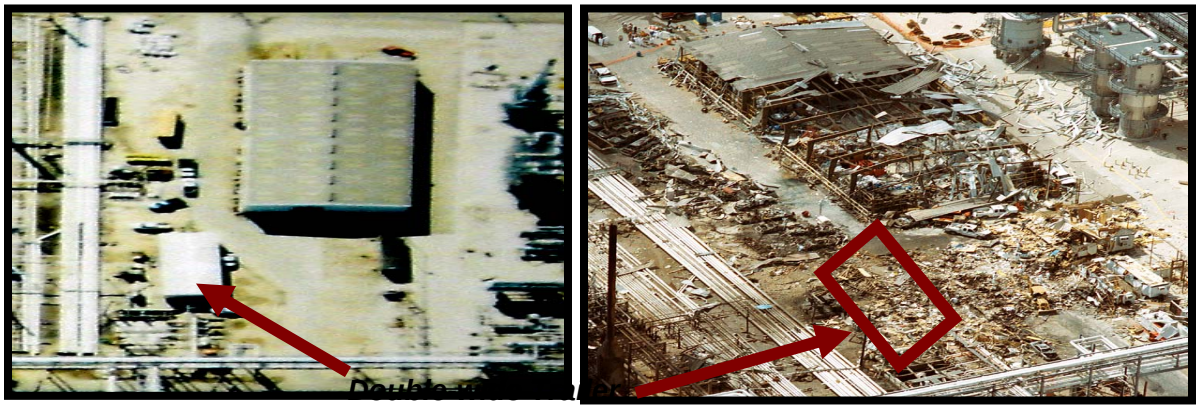


Figure 3. Pre and Post Incident Damage to Trailer

Discussion of Inherent Safety Principles
This tragedy illustrates the consequences of not applying IS to processes. The presence of an open atmospheric relief stack with a poorly designed system upstream created an unsafe condition. While the operator overfilled the column, the process was not error tolerant because the knockout drum was not designed to withstand the amount of material that could potentially be sent to it.

The placement of the trailers close to the operating unit was also a hazardous situation. Some trailers were only about 120 feet away from the process unit. If the policy had forbid them from being located so close, this tragic loss of life could have been avoided. This situation clearly illustrates the need to challenge the premise of existing situations. It had been a common practice to have the trailers located in the area.

Case 3: Errors in material delivery and defeat of inherently safe fittings

Incident Brief
A tragedy occurred in a medical facility in Ohio when four patients were asphyxiated. During a delivery of oxygen cylinders, a supplier mistakenly delivered a cylinder of nitrogen. The cylinder had a nitrogen label that was partially covering an oxygen label. The tank had nitrogen-compatible fittings, but the maintenance employee assumed the cylinder contained oxygen and made an adapter to connect the nitrogen cylinder to the oxygen delivery system. The patients breathed the pure nitrogen and quickly died.

Discussion of Inherent Safety Principles
This incident points out a couple of IS principles. First, there were ineffective checks in the delivery and receiving process for the cylinders. The fact that the oxygen would assist patients with respiratory problems, made these checks essential. Furthermore, this incident also shows that sometimes inherently safe systems can be bypassed if employees make incorrect assumptions. Often employees put tremendous faith in upstream systems, and assume that they should work around any problem they encounter. In this case, the series of failures started with the delivery of the wrong cylinder, and ended when the employee mistakenly hooked nitrogen to the oxygen delivery system via an adaptor. This accident shows that IS concepts must be practiced throughout the entire process, from delivery to operations and maintenance, and decommissioning if applicable.

Success Stories

Along with the tragedies that have been discussed to show the results of not utilizing IS principles, there have been successes. Many companies see the benefits in comprehensively addressing problems and correcting situations so that the hazard is eliminated or greatly minimized. It is more difficult to find information on what did not happen (rather than what did), but successes can demonstrate real benefits for the safety practitioner to promote IS concepts.

The Occupational Safety and Health Administration published information on its website about an ergonomic success story at Dow Chemical. In 2000 the company chose the Dow Design and Construction Business Unit for an ergonomic intervention. Dow used the “Six Sigma” process, which is a disciplined approach to problem solving. Six Sigma emphasizes the reduction of defects by applying a four-step improvement methodology, and recommends sustainable results over short-term fixes.

The four steps of Six Sigma are measure, analyze, improve, and control. The project team began by defining the current process to see how people were becoming injured. They identified key variables affecting the process outcome for workstations users, including user attributes (such as time at workstations); user behaviors (such as posture and force); and environmental factors. They set goals for improvements in these variables.

The team analyzed survey data to determine differences in workstations, work environments, user training, and behavior at different sites. They identified causes
and emphasis that management put on ergonomics. The team developed a series of improvements, including both work-related and personal risk factors. Workstation deficiencies were addressed by implementing a workstation upgrade plan. The team elevated the focus on

ergonomics by improving awareness and altering behavior and work habits through increased accountability. The team then developed a long-term control plan to sustain the achievements. The plan addressed the causes of injuries and added performance standards, measures, responsibilities, and contingency plans.

The results were impressive. The identified risk factors were reduced 64% as compared to the baseline measurement. In two years the company went from 53% of ergonomic injuries resulted in lost work time or advanced medical treatment to only 30% being severe (www.osha.gov). This case study illustrates the benefit of proactively analyzing a hazardous occupational situation and taking steps to eliminate the hazard by changing the work station and behaviors. This approach is in contrast to simply working around hazards, which yields only short term solutions.

IV. Conclusion

The principles of inherent safety should be employed at all stages of the process, from design to end of life. Although these concepts are often related to hazardous chemicals, they can be easily applied to occupational environments and work procedures. If the process cannot be made inherently safe, then the goal becomes making it inherently safer by taking it to a less risky state. The safety practitioner and designer must always ask why is the hazard present, and can it be eliminated. Do not accept that the hazard is there and simply determine how be to protect against it. Employing IS principles is the only way to ensure safety.

V. Bibliography

British Petroleum. *Fatal Accident Investigation Report: Isomerization Unit Explosion Final Report*. December 9, 2005. (www.bp.com)

Center for Chemical Process Safety. *Guidelines for Engineering Design for Process Safety*. New York: American Institute of Chemical Engineers. 1993.

U.S. Chemical Safety and Hazard Investigation Board. *Explosion and Fire, First Chemical Corporation, Pascagoula, MS.* Report No. 2003-01-I-MS. Washington, DC. CSB. October 2003.

U.S. Chemical Safety and Hazard Investigation Board. *Hazards of Nitrogen Asphyxiation*. Report No. 2003-10-B. Washington, DC. CSB. June 2003.

Wallace, S. *Optimize Faciltiy-Siting Evaluations*. Hydrocarbon Processing, A Journal of Gulf Publishing. Houston, TX. Gulf Publishing. May 1994.

Wallace, S. *Take Action to Resolve Safety Recommendations*. Chemical Engineering Progress, a Monthly Journal of the American Institute of Chemical Engineers. New York, NY. AIChE. March 1999.

Wallace, S. *Catching Near Hits*. Professional Safety, a Monthly Journal of the American Society of Safety Engineers. Des Plaines, IL. ASSE. November 2000.

Wallace, S. *Using Quantitative Methods to Evaluate Process Risks and Verify the Effectiveness of PHA Recommendations*. Process Safety Progress, a Quarterly Journal of the American Institute of Chemical Engineers. New York, NY. AIChE. March 2001.

Wallace, S. *Know When to Say "When": A Review of Safety Incidents Involving Maintenance Issues*. Process Safety Progress, A Journal of the American Institute of Chemical Engineers (AIChE). New York, NY. AIChE. December 2003.