# Inherently Safe Design
# A Common Sense Approach

**Danny C. White, P.E.**
**RMT Inc.**
**Houston Office**

Most safety professionals associate Inherently Safer Design (ISD) with preliminary design of new processes. Indeed, in most cases, ISD concepts can have the greatest impacts in the early stages of process design. However, it is important to always consider ISD even for mature processes. In many instances processes can be made inherently safer with minor modifications. Mature processes can also become less inherently safe over time due to lack of maintenance of key systems or from or from out-of-date information. This paper presents a common sense approach for applying ISD techniques to mature processes and day-to-day operations.

## BACKGROUND OF ISD

ISD is not a radical new idea that has only recently been discovered. Good process design has always incorporated inherently safer design techniques. However, with the advent of computerized controls and other sophisticated equipment during the past fifty years, there was an era in process design where many engineers felt all hazards could be eliminated with mechanical controls, interlocks, and other technologies. Several famous accidents in the 70s and 80s changed that view. After the Flixborough explosion in 1974 many in the industry were calling for increased technological controls for hazardous chemical processes. Mr. Trevor Kletz proposed a completely different approach – to change the process to eliminate the hazard completely or reduce its magnitude sufficiently to eliminate the need for elaborate safety systems and procedures. The classic definition of ISD begins with the title of one of the first lectures on ISD concepts given by Mr. Kletz after the Flixborough explosion:

"What you don't have, can't leak" Trevor Kletz, December 14, 1977

While ISD was not invented or discovered by Mr. Kletz, he did start a new thought process where ISD could systematically applied. While it is true that you can't leak what you don't have, in many cases the only way to "not have" something is to shut the plant down and drain all of the vessels. This paper focuses on the application of ISD principles to existing processes and includes several common sense examples.

## ISD STRATEGIES

Traditional process safety efforts have sometimes been focused on reducing risk by adding protective systems. Several infamous chemical disasters have shown that even elaborate protective systems can and do fail. ISD uses a different approach by addressing the hazard directly.

A hazard is an inherent characteristic of a material, system, or process that has the potential for causing injury to people and/or property, or environmental damage. The risk of a hazard is typically defined as the product of the likelihood of the event and it's severity:

$$Risk = (event\ likelihood)(consequence\ severity) \quad (1)$$

However, the likelihood is a product of the event frequency and the probability of a failure of the protective system:

$$likelihood = (event\ \ frequency)\begin{pmatrix} probability\ of \\ protection\ \ system\ \ failure \end{pmatrix} \quad (2)$$

Therefore, risk can be defined as:

$$Risk = (event\ \ frequency)\begin{pmatrix} probability\ of \\ protection\ system\ \ failure \end{pmatrix}(consequence\ severity) \quad (3)$$

The first step in ISD is to evaluate any options to eliminate or reduce the hazard directly by a fundamental change in the process. There are four major strategies for incorporating ISD into a process:

Minimization
Substitution
Moderation
Simplification

One easy way to remember these strategies is to use the formula:

$$ISD = (MS)^2 \quad (4)$$

As shown in equation 3, ISD reduces the severity and/or the frequency of a hazard directly rather than decreasing the likelihood. For example, minimization or substitution will generally reduce the severity of a hazard while moderation or simplification might reduce the event frequency. In some cases, both the frequency and severity of a hazard are reduced by one action, such as minimization or substitution.

After these options have been exhausted, ISD is then applied to the protective systems. While protective systems are not inherently safe, some protective systems are inherently safer than others. For example, a dike is inherently safer than procedures to minimize the impact of a tank overflow. Protective systems can be ranked in terms of ISD according to the following hierarchy:

| | |
|---|---|
| Inherent | Most Robust |
| Passive |  |
| Active | |
| Procedures | Least Robust |

The hierarchy above shows that inherent systems are the safest, passive mitigation is the next best protection, followed by active mitigation, and lastly procedural measures.

To illustrate ISD concepts, a case study is presented. The case study will be discussed throughout the remainder of the paper.

## CASE STUDY: PROPANE-POWERED FORKLIFTS

A warehouse uses several forklifts to transport chemicals. Each forklift is powered by a 5 gallon propane cylinder. When empty, cylinders are taken to a refill area that includes a propane cylinder storage rack for empty and full containers and a 500-gallon propane tank. Operators manually re-fill the 5-gallon cylinders using propane from the 500-gallon tank. Approximately twice per month, a large truck of propane enters the plant and re-fills the 500-gallon tank.

### Minimization

The presence of a 500-gallon tank of propane and the routine presence of a large tanker truck of propane introduces a relatively high severity of a fire and/or explosion hazard. The most typical initiating event would be a release of propane during refilling of either the large tank or a small cylinder. An example of minimization would be to remove the tank and contract with a vendor who would bring only full 5-gallon containers into the plant and pick up the empty cylinders for refilling offsite. This eliminates the 500-gallon stationary tank and the presence of the large propane tanker truck.

Eliminating the need to transfer propane between the tanker truck and the 500-gallon stationary tank and between the 500-gallon tank and 5-gallon cylinders has also reduced the event frequency.

### Substitution

Substitution has been used successfully for many existing processes. Examples are common, such as the replacement of chlorine with bleach for water disinfection or the replacement of chromium with phosphate for cooling water corrosion inhibition. Using the propane-fueled forklift case study, the process might become inherently safer by converting to electric-powered forklifts. However, electric-powered forklifts could potentially introduce new hazards, such as battery acid, that did not exist before. Therefore, applications of substitution need to be carefully examined to insure the new hazards are factored into the risk equation.

**Moderation**

Moderation reduces hazards by reducing the process conditions such as pressure, temperature, or pH. Examples of moderation include cryogenic storage of ammonia as opposed to storage under pressure or the use of catalysts to lower reaction temperatures. In some cases, mitigation might be considered as a "moderation." For example, a containment area to reduce the surface area for evaporation would result in a more moderate air release if spilled.

For the forklift case study, one moderation application would be to provide a roof over the propane storage rack to reduce the temperature of the stored 5-gallon cylinders. Keeping the cylinders at a lower temperature reduces the pressure and decreases the risk of a leak.

**Simplification**

Simplification reduces the likelihood of an accident or hazardous event by eliminating unnecessary steps and therefore reducing the opportunities for a hazardous event to occur. Examples of simplification include the use of dedicated lines for complex product loading operations. Undedicated lines sometimes require complex valving and line cleaning operations when switching products. Dedicated lines reduce the complexity and eliminate the need to clean lines prior to switching products.

For the forklift example, simplification occurred when operators were no longer were required to re-fill individual 5-gallon propane cylinders. Additional simplification measures might include using separate cylinder storage racks for full and empty 5-gallon cylinders.

**ISD FOR PROTECTIVE SYSTEMS**

As previously mentioned, after the opportunities for applying ISD to the fundamental aspects of a process have been exhausted, ISD concepts can be applied to protective systems for a hazardous process. Referring to equation 3, the probability of protective system failure affects the likelihood of a hazardous event and thereby reduces risk.

**Passive Mitigation**

The most robust and dependable, and therefore inherently safest, protective measure, is the use of passive mitigation. Passive mitigation requires no human, mechanical, or other energy input to function. An example of passive mitigation is a dike or containment area surrounding a storage tank. Even though passive mitigation is more desirable than active mitigation, passive mitigation systems usually still require maintenance and adherence to operating procedures to function correctly. For example, a dike filled with water or a dike with a drainage valve always left open will not function correctly in an emergency.

For the forklift operation, passive mitigation measures might include a sloped drainage surface beneath the propane cylinder storage rack to prevent pooling of any spilled propane beneath the storage rack. Personal protective equipment, such as protective eyewear, might also be considered as passive mitigation.

**Active Mitigation**

After passive mitigation, the next best protective system is active mitigation such as a process control interlock or automatic sprinkler system. Active mitigation requires some type of energy input to function. Active mitigation can function automatically, such as a process control interlock, or may function manually, such as with a fire extinguisher. As with passive mitigation, proper maintenance of active mitigation is essential.

For the forklift example, active mitigation might include the placement of fire extinguishers near the propane storage rack.

**Procedures**

Incorporating safety considerations into procedures can provide another layer of protection. Operating procedures are also necessary to assist in the proper maintenance and operation of the protective equipment.

For the forklift example, procedures might include steps such as the proper method of connecting the 5-gallon cylinders to the forklifts.

## OPPORTUNITIES FOR INHERENTLY SAFE DESIGN

As previously mentioned, ISD can often have the greatest impact during the initial process design phase of a new process but even mature processes have opportunities for ISD improvements. The list below highlight occasions or opportunities where ISD can be applied:

- in the design stage (early)
- after a major accident
- incident investigation (near miss or actual incident)
- regulatory drivers (e.g. RMP)
- Process Hazard Analysis/SHE reviews
- Visual observations/routine safety inspections
- PSM audits
- Employee feedback or suggestion programs
- OSHA/EPA inspection or audit
- Turnaround preparation
- debottlenecking projects
- analysis of routine maintenance activities

## SUMMARY

ISD is not just for new processes. ISD techniques can be applied to mature processes to reduce risk. Safety professionals should implement training of ISD techniques to operations, maintenance, and engineering teams within hazardous processes or locations.