

Contents

Inherent Safety in Front End Engineering	1
Introduction.....	1
Timing.....	2
Choice of Guidewords	2
Eliminate.....	3
Minimize.....	4
Substitute.....	4
Moderate.....	4
Simplify.....	4
Removing People.....	5
Implementation Program	5
Team Effort.....	6
Not an “Add On”	6
Safety Moment.....	6
Technical Documents.....	6
Hazard Analyses	7
Challenges.....	7
Simple Design.....	8
Imagination	8
Engineering Standards	9
Focus on Process Engineering	9
Inherent and Passive Safety	9
Inventory Management	10
Value of Backup Equipment	11
Law of Unintended Consequences.....	11
Conclusions.....	12
Citations.....	12

INHERENT SAFETY IN FRONT END ENGINEERING



INTRODUCTION

The topic of Inherent Safety (IS) in the process industries is well established and has been thoroughly described in many publications. Moreover, Inherent Safety is now being included in some process safety regulations, such as that from the New Jersey Department of Environmental Protection.

Facilities regulated by the TCPA program must perform Inherently Safer Technology reviews.

(NJDEP 2010)

It is recognized that removing hazards, or at least reducing their magnitude, is generally a more effective way of improving safety than adding additional layers of instruments and/or improved operator training. Furthermore, hazard elimination or reduction is accomplished by means that are inherent to the design and are thus permanent and inseparable from the process. Add-on safety devices can always fail, but inherent safety is part and parcel of the process itself.

Yet, in spite of its obvious value, the application of Inherent Safety concepts to actual projects poses some challenges. In particular, because Inherent Safety often represents a new way of thinking, management can find it difficult to get engineers and other technical specialists to adjust the manner in which they approach the design of equipment and process systems.



The purpose of this paper is to discuss some of the practical issues and challenges that management faces when implementing Inherent Safety on their projects. The paper was written during the course of a project to do with the initial design, procurement, construction and commissioning of an offshore deepwater drilling and production platform. Client management had emphasized that Inherent Safety was a critical project driver, so the Technical Safety team was required to develop a program for implementing IS as the project moved from the Conceptual Stage into Front End Engineering Design (FEED) and on into detailed design. The team goal was to, “Bake Inherent Safety into the Design Pie”.

Based on the lessons learned on this project, this paper provides practical suggestion and guidance as to how the principles of Inherent Safety can be applied to a project, with a particular focus on how to get project team members to “think that way”.

TIMING

Although the principles of Inherent Safety can be applied to a facility at any time, even after it is in operation (Edwards and Chosnek 2011), it best used during the early stages of a design. It is at this time that fundamental changes can be made quickly and easily. Once detailed design is underway, such changes are harder to make, and they become even harder as a project enters the procurement, construction and commissioning phases. For example, it is relatively easy to change to a less toxic chemical before the Process Flow Diagrams (PFDs) have been finalized; it is much more difficult to do so once the final design has been authorized, or after the system is in operation.

The project described above was a good one on which to apply the principles of Inherent Safety because it was at the concept phase, which meant that most of the design decisions either had not been made or could be changed. Preliminary PFDs and Piping & Instrument Diagrams (P&IDs) had been prepared, but they were far from being finalized. Similarly, a general layout had been prepared, but the design team still had a good degree of freedom to make changes.

CHOICE OF GUIDEWORDS

Inherent Safety programs are usually structured around a set of guidewords. Different authorities and authors use different sets of words. For example, The Center for Chemical Process Safety (CCPS 1996) suggests the following guidewords.

1. Minimize
2. Substitute
3. Moderate
4. Simplify

One of the early decisions made on this project was to allow the team to select its own guidewords. Much of the Inherent Safety literature is written for the chemical industries, yet the safety environment on an offshore platform differs from that of a chemical plant. For example, highly toxic chemicals are not generally used on an offshore platform (although the presence of hydrogen sulfide and carbon dioxide can be a major hazard), but the risks associated with dropped objects and blocked emergency escape routes are high. Therefore guidance that is appropriate for the onshore process industries is valuable, but also limited in usefulness.

For this project, the team selected the guidewords shown below.

1. Eliminate
2. Minimize
3. Substitute
4. Moderate
5. Simplify

The hierarchy is significant; the words at the top of the list were considered to have a greater effect than those lower down. For example, completely removing a pump from the process (*Eliminate*) is likely to have a much greater impact on safety than merely making the pump easier to use (*Simplify*).

Eliminate

Generally, the best way of achieving Inherent Safety is to eliminate the hazard altogether, as can be seen from the following risk equation.

$$\text{Risk}_{\text{Hazard}} = \text{Consequence} * \text{Predicted Frequency}$$

Risk is estimated and then reduced by first identifying the hazards, generally through the use of a HAZID or HAZOP. Each hazard has associated consequences (safety, environmental, economic), and also a predicted frequency rate.

The equation shows that, as long as hazards are present, the total risk can never be zero — a truth not always grasped by members of the general public or the news media. Hazards are always present within all industrial facilities. Those hazards always have undesirable consequences, and their likelihood of occurrence is always finite. The consequence and likelihood terms can be reduced in size, but they can never be eliminated. The only way to achieve a truly risk-free operation is to remove the hazards altogether, *i.e.*, to apply the Inherent Safety *Eliminate* guideword.

Overton and King (2006) provide an example in which the liquefaction step in a chlorination process allowed for the elimination of a storage tank containing 750 tons of chlorine.

For the offshore platform project, attention was paid to opportunities for eliminating pumps and valves (although the latter often provide a major safety function). For example, one proposed process design consisted of a system of three knockout vessels in series. The vessels contained very high pressure gas. Serious consideration was given to eliminating two of the vessels and combining their functions in the first knockout vessel. Doing so led to a sizeable reduction in inventory of gas and also reduced problems to do with finding sufficient vertical space for the three vessel set-up (space limitations are always a problem on offshore platforms).

Minimize

‘Minimization’ generally refers to the use of smaller quantities of hazardous substances. The Bhopal tragedy of 1984 was a missed opportunity for application of this guideword. Had the inventory of methyl isocyanate been less than it was, far fewer people would have died.

For an offshore platform there are not as many opportunities to reduce inventories as there are onshore. Platforms generally have little or no storage (oil, gas and water are treated and immediately sent to an onshore facility). Nor do they generally have significant quantities of highly hazardous chemicals on board.

One minimization initiative considered on the project was to connect piping sections with welds rather than flanges. Doing so reduces the number of potential leak sources. (It does, however, make general maintenance more difficult and thereby increase risk.)

Substitute

‘Substitution’ also tends to be more applicable to chemical plants than it is to an offshore facility. Although chemicals such as glycol are used to removed hydrates from subsea piping, these chemicals are usually relatively benign. The same can be said of many of the miscellaneous chemicals that are used for activities such as corrosion control.

Moderate

‘Moderation’ generally refers to the use of a use a less hazardous condition. In many cases, the team will determine if it is possible to operate at lower temperatures or pressures. On this project much of the electrical equipment operated at high voltage. Therefore careful consideration was given to ‘moderating’ high voltage with low voltage.

Simplify

Simplification is the lowest of the levels of Inherent Safety considered by the team. It often relates to making equipment easy to use and tolerant of operating error. Simplification also makes operation of the facility during an emergency less prone to error.

With regard to the offshore project, the design carefully considered the ‘Simplify’ guideword during the procurement stage, particularly with respect to rotating equipment. If one vendor offered a design that used fewer moving parts, for example, then that product was considered favorably.

The project was at too early a stage for simplification to do with human factors and operating procedures to be considered.

Removing People

Related to the concept of hazard elimination, that was discussed above, is the idea of removing people from the site of a potential incident. The term, “What you don’t have, can’t leak” was used by Kletz (1978). A derivative of that phrase would be, “If a man’s not there, he can’t be killed” (Sutton 2010).

A good example of the application of this concept can be seen with respect to hurricanes in the Gulf of Mexico (GoM). During the period 2003 - 2005 some 164 offshore platforms were either lost or seriously damaged due to hurricanes. Although the economic loss was high, the number of fatalities and serious injuries associated with the storms was zero; the reason being that, whenever a hurricane is brewing and heading toward a platform the crew is evacuated.

In the long-term, one of the best means of improving safety is to develop systems that are so automated that very few humans are required to be in the vicinity of operating equipment so that they are not exposed to hazards. With regard to the offshore project, the platform will have a substantial crew (more than 70 people) during the drilling phase, but will be totally unmanned once drilling ceases and production is the only activity. Control of the operations would be from an onshore facility.

In general manning levels can be reduced by the following actions:

- Simplification of the design;
- Robust design;
- Use of passive rather than active corrosion management;
- Designing out the need for local intervention; and
- Specification of proven, high-reliability equipment.

IMPLEMENTATION PROGRAM

Some of the techniques used to implement Inherent Safety on the project are described in this section. As already noted, the overall project aim was to “Bake Inherent Safety into the Design Pie”. The idea behind this phrase was that Inherent Safety would become part of all project activities, and that engineers and other technical specialists would follow its principles at all times. Inherent Safety would not be an add-on, or something directed by the Technical Safety group.

The Inherent Safety goal was integrated into three other, compatible drivers. They were:

- No injuries to people at any stage of the project or when the facility was in operation.
- A flawless startup.
- No surprises regarding the project budget or schedule.

Team Effort

The first and most crucial decision was to make the application of Inherent Safety a multi-discipline team effort. The Inherent Safety work was managed by the Technical Safety lead, but all decisions of significance, including the choice of guidewords, were a team decision.

Not an “Add On”

It was made clear to the team that Inherent Safety be considered throughout the design — in no way should the concept be an “add on” or as something as being just in the domain of Technical and Process Safety.

Safety Moment

It is commonplace for companies to start formal meetings with a Safety Moment, in which someone describes an event or lesson learned that can help the other people better understand and improve their own safety performance. For this project it was decided that many of the Safety Moments would be to do with Inherent Safety. The person responsible for the Safety Moment would discuss some activity that had been carried out or that was planned that showed how Inherent Safety was being used on the project.

Technical Documents

An early lesson learned was that most lead engineers do not have much training or exposure to the concepts of Inherent Safety, and they tend “not to think that way”. Just telling them to apply the principles of Inherent Safety is not sufficient. In response to this concern a requirement was made that *all* technical documents, regardless of the discipline concerned, should start off with a short preamble showing how the author had considered the elements of Inherent Safety when preparing that document.

Examples included the following:

- An electrical engineer issuing a specification for a compressor motor would demonstrate how he considered the possibility of using lower voltage electricity (“Moderate”).
- A mechanical engineer responsible for designing the facility crane would show how consideration was given to minimizing the maximum weight load so as to reduce the impact of a dropped object (“Minimize”).
- A systems engineer would demonstrate that consideration was given to importing electrical power rather than generating it locally (“Eliminate”).

In practice, many of the lead engineers were not entirely comfortable with the above approach; it represented a new way of thinking. In these cases an alternative approach was used. All the technical leads would gather in a meeting to carry out a traditional squad check of the document. However, in

addition to carrying out the normal engineering review, a technical safety expert would guide the team through a discussion of the Inherent Safety guidewords as they applied to that document.

Team meetings led to a second benefit. The application of the principles of Inherent Safety can lead to unanticipated and unwanted results (the Law of Undesirable Consequences, discussed below). In the case of the three pressure vessel train, for example, merging their functions into one vessel meant that solids removal became more difficult and potentially exposed maintenance workers to greater risk. A team discussion is more likely to generate an understanding of potential increased risks than is a single-person review.

Hazard Analyses

The principles of Inherent Safety were also applied during the normal HAZID (Hazard Identification) process and in the early HAZOPs. HAZIDs traditionally aim to identify hazards such as high level in a vessel, total loss of power or a spill of a toxic chemical. The team then considers the consequences and likelihood of such events and, if necessary, generates findings and recommendations. On this project the Inherent Safety guidewords listed above were explicitly called out during the HAZID.

Implementing the principles of Inherent Safety during the routine HAZIDs helped make the final design safer. However, there was a second, and more subtle, benefit that resulted from this activity. As the project progressed most of the engineers and other technical specialists started to “get” the principles of Inherent Safety, and start to apply them in all situations, and at all times.

Such a way of thinking is ultimately what Inherent Safety is all about, and is analogous to what occurred as HAZOPs were introduced. The immediate benefit of a HAZOP is to identify and correct high risk hazards. However, a more subtle, and ultimately much more important, role of a HAZOP is to inculcate a way of thinking that is baked into the way all personnel act and work. People learn to “think the unthinkable”. So it is with Inherent Safety; use of the techniques discussed above help make the topic “part of the furniture”.

CHALLENGES

Although the concepts of Inherent Safety were accepted intellectually without much difficulty by the project team members; the practical application of these concepts was more of a challenge. Some of the issues faced included the following:

- Simple design
- Need for imagination
- Engineering standards;
- Focus on process engineering;
- Inherent and passive safety; and
- Value of backup equipment.

Simple Design

Although large, the offshore platform that was being designed was quite simple in its overall design, and it was quite similar to other platforms of the same type. Therefore, it was difficult at times to come up with ideas for the application of the Inherent Safety guidewords. The lack of opportunity for finding new ideas tended to dampen the enthusiasm of the team members.

Imagination



On September 25th 2001, just days after the 9/11 attacks, the New York Times columnist Thomas Friedman wrote,

The World Trade Center is not the place where our intelligence agencies failed. It is the place where our imaginations failed.

Prior to that attack very few people had even conceived that terrorists could take over airplanes and use them to hit large buildings. They lacked imagination. The same problem can apply to the use of Inherent Safety.



By its very nature the technique requires that people come up with new ideas, that they “think the unthinkable” — but not that “they think out of the box” (anyone who uses the phrase “thinking out of the box” shows by the staleness of their imagery that they are well inside the box). Simply put, thinking is hard work — yet such thinking is at the heart of any Inherent Safety program. In the words of one of the Monte Python Gumbys, “My brain hurts!”

Most people prefer to work in a well-established system using previous designs and proven engineering standards. Yet Inherent Safety requires that people use their imagination, particularly with regard to the ‘Eliminate’ guideword. This is difficult.

In addition, many processes — including offshore platforms — are quite similar to one another. There is considerable pressure on the team simply to repeat previous designs on the basis of, “It it’s not broken, don’t fix it.” Moreover, the strict discipline that engineers and technical specialists must follow with regard to the application of industrial standards can discourage imaginative thinking.

A further difficulty is that a person who is skilled and experienced at leading a standard risk management program such as a HAZOP analysis, may not be as effective in having team members think creatively. It is relatively easy to define the hazards, estimate their consequences and likelihood, come up with an assessment of overall risk, and then generate some recommendations. A different

patter of thinking is needed when applying concepts such as eliminate or simplify, and the HAZOP team leader may not be the best choice of person to lead the activity.

Rather than having a good knowledge of risk management, as most HAZOP leaders do, the person leading an Inherent Safety analysis needs a detailed understanding of the different engineering disciplines.

Engineering Standards

Engineers organize their work around the hundreds of standards from bodies such as the API, ASME, NFPA and IEEE. Since these standards (and their regular updates) have typically been in service for many years engineers tend to instinctively follow them, rather than look for fresh ideas. For example, when faced with a pressure control problem on a vessel, an engineer designing an offshore platform will instinctively tend to reach out for API Recommended Practice 14C rather than think through whether the instrumentation in its present form is even needed.

Focus on Process Engineering

Much of the literature to do with Inherent Safety is published in chemical process journals, and therefore tends to look at process-related issues, such as the replacement of a hazardous chemical with one that is more benign. Other industries have a different set of safety concerns. As already discussed, offshore platforms and drill rigs do not typically handle highly toxic materials, and their process steps are relatively simple when compared to a chemical plant or refinery. However, they have serious concerns with dropped objects (usually when items are being transferred from a service boat by crane). Also, if there is an emergency offshore, escape can be a major problem. Movement on the deck could easily be obscured by smoke, and finding a safe location can be a challenge. The Inherent Safety program for an offshore drill rig or platform needs to reflect these realities.

Inherent and Passive Safety

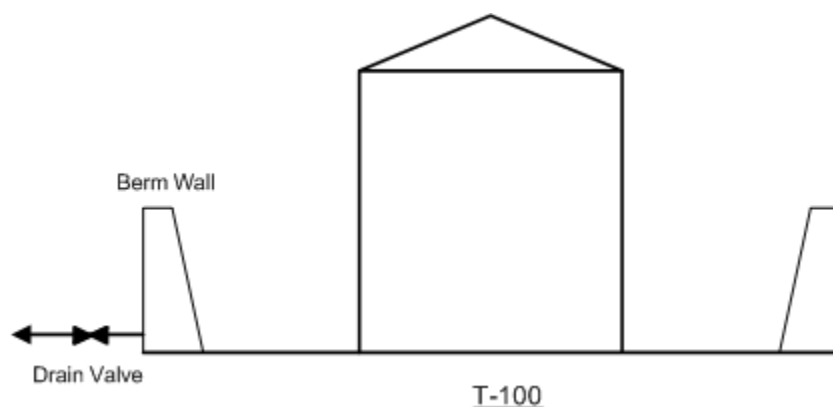
Hendershot (2006) places safety strategies into one of four categories:

- Inherent
- Passive
- Active
- Procedural

It was found on the offshore project that the team members readily understood the philosophical differences between Inherent and Active Safety. For example, removing a vessel from a process is likely to be more effective in improving safety than adding instruments to prevent incidents to do with high pressure and high level.

However, the distinction between Inherent and Passive Safety is more subtle. Using an example from a typical onshore operation, it is standard practice to put a containment (berm or bund) wall around a tank that stores a hazardous chemical. This concept is illustrated for Tank, T-100, in the sketch below.

The wall is often an earthen berm, although concrete is sometimes used. The capacity of the containment system is generally 110% of the capacity of the largest tank. This means that, if the tank leaks for reasons such as corrosion or impact with a vehicle, the liquid will be contained.



This system is *passively* safe, *i.e.*, it does not rely on the active response of equipment items such as a level gauge on the tank, or a pump to remove spilled liquid. The berm wall will remain in existence regardless of what is going on around it, and will work effectively, even if all the other control systems have failed. However, the system is not *inherently* safe. The spilled liquid may be contained, but it could still be hazardous (for example, it may catch fire or emit toxic fumes). Also, there is usually a drain valve placed in the wall so that rain water can be removed. This drain valve could be inadvertently left open. Indeed, it is possible that a large explosion at the facility could destroy the wall itself. The use of a containment wall has reduced risk both by reducing the likelihood of a spill to the general environment, and by mitigating the risk in case something does go awry. However this system is not “inherently safe” — it is just much less risky. An inherently safe system would be one in which the process was redesigned such that there was no need for a tank at all.

Inventory Management

The ‘Moderate’ guideword would suggest that small quantities of hazardous materials be used wherever possible. Then, if there were to be a leak, the consequences would be less severe. However, the use of small quantities may actually reduce safety. For example, a facility that uses a toxic chemical in liquid form may have the choice of either bringing in one large shipment every week, or multiple small deliveries ten times a week. The latter would appear to be the inherently safer of the two operations. However, the latter operation involves many more deliveries, and opportunities for error during the connection and disconnection operations. In other words, the risk reduction

associated with having lower consequence events may be erased due to the higher likelihood of an event taking place.

A detailed discussion to do with the tradeoff between storage size and the number of loading/unloading activities is provided by Englund (1991).

Value of Backup Equipment

Many equipment items are provided with an on-line spare or backup. On the offshore project, for example, critical pumps were spared so that, if the primary pump were to fail, the second pump could be brought on line quickly.

From an Inherent Safety point of view, the spare item poses an unnecessary hazard — it could leak or otherwise cause a problem, and it will require routine maintenance, which always involves a risk to the maintenance workers. However, if it is removed, and the primary pump fails then a new set of safety problems can arise. These could include the possibility of high level or low level in associated vessels and the need to blowdown equipment to the flare.

Law of Unintended Consequences



The “Law of Unintended Consequences” is a term that is generally used somewhat ironically or tongue in cheek, but that should be considered when applying the principles of inherent safety. The basic idea behind this “law” is that human intervention in complex systems tends to produce a range of unexpected outcomes, most of which are undesirable, and which could readily lead to losses which negate the benefits many times over. For example, the rabbit was introduced into Australia for food, but eventually became a highly destructive pest.

The unintended consequences generally fall into one of three general categories.

- *The unexpected outcome is desirable.* Such a consequence is sometimes referred to as serendipity. An example could be to do with a pumping system. The original design may call for two pumps: one operating and the other serving as a backup. If the pump can be redesigned such that it is much more reliable, then the spare pump can be removed, thus improving Inherent Safety. But it may also be found that the new design results in much less maintenance, thus reducing the number of times maintenance workers have to be put at risk. Or it may be found that the reduced pump downtime results in increased catalyst life in a downstream reactor because it is subject to fewer swings in flow rate and temperature.
- *The unexpected outcome is undesirable.* Using the same example to do with the pumps, it may be found that, because the workers now have to work on the item less frequently they are less experienced, and so, when they have to do so they therefore are more likely to make a mistake and increase their chances of being hurt.

- *The outcome is one that makes the original situation worse.* Once more using the pump example, it may be found that having a spare pump makes the operations personnel more willing to operate the system closer to the safety limits.

CONCLUSIONS

The concept of Inherent Safety is well understood and has been extensively discussed in the process safety literature. Its application to actual projects can certainly lead to reduced risk, and improved safety in particular. However there are challenges, of which probably the biggest is that it can be difficult to persuade senior engineers and other highly qualified professionals to adopt a new way of thinking.

CITATIONS

Center for Chemical Process Safety (CCPS). Inherently safer chemical processes: A life cycle approach. D.A. Crowl (editor). American Institute of Chemical Engineers. New York, 1996.

Edwards, V.H., J Chosnek. Making Existing Process Plants Inherently Safer. 7th Global Congress of Process Safety. March 2011.

Englund, S.M. Design and Operate Plants for Inherent Safety - Part 1. Chemical Engineering Progress. March 1991.

Hendershot, Dennis, C. An Overview of Inherently Safety Design. Process Safety Progress. June 2006.

Kletz, T. A. What you don't have can't leak. Chem Ind. May 1978.

NJDEP. Rules and Regulations. <http://www.state.nj.us/dep/rpp/brp/tcpa/tcpadown.htm>. December 12th 2010.

Overton, T., G.M. King. Inherently Safer Technology: An Evolutionary Approach. Process Safety Progress. June 2006.

Sutton, Ian S. Process Risk and Reliability Management. Elsevier, Oxford. 2010.