Making Facilities Safer by Design

Graeme Ellis, ABB Consulting, Daresbury Park, Warrington, Cheshire WA4 4BT, UK

KEYWORDS: Inherent Safety, Design, Workshop, Energy Institute

Introduction

Process safety accidents normally involve the failure of several protective barriers, leading to tightening of management controls to assure performance. This paper supports an alternative inherently safe approach, i.e. one that removes hazards or minimises their consequences by better design rather than relying on 'bolt-on' protection that can and does fail.

Inherent Safety principles were introduced into the process industry by safety guru Trevor Kletz in the 1970's with his motto, "What you don't have, can't leak". Whilst there are good examples of inherently safe process designs in the process industry, there is a lack of design methods to ensure opportunities are systematically identified and exploited.

This paper is by the author of guidance for Inherent Safety in Design (ISD) published in 2014 by the UK Energy Institute. It is targeted at Project Leaders in the upstream and downstream Energy Industry and aims to change the design culture that currently favours 'bolt-on' safety features. The guidance highlights the benefits from applying ISD at a very early stage of the design process, reducing the major accident potential whilst reducing the overall capital and operating costs.

For major projects in the Energy Industry, the guidance introduces an Inherent Safety workshop at the concept selection stage, before HAZID studies during the subsequent FEED stage. A team identifies potential hazardous events based on a Process Block Diagram, and applies Inherent Safety principles to identify improvement options, following the hierarchy; Elimination, Substitution, Minimisation, Moderation, Segregation and Simplification.

The paper will illustrate the benefits of Inherent Safety being applied to typical processes and hazardous events in the Energy Industry. Several example events will be described with the typical design solution involving 'bolt on' safety features, plus an alternative inherently safety design with the benefits in terms of reduced hazards and lifecycle costs.

Lessons from the past

The toxic gas release in Bhopal, India in 1984 remains the most serious accident in the process industry in terms of the number of people killed. Several risk control systems failed to prevent an intermediate storage vessel over-pressurising and releasing a cloud of highly toxic gas via a scrubbing tower and flare system to atmosphere. The tank design and protective systems were common throughout the world on similar facilities, where the hazard associated with a large inventory of toxic material was justified on the basis that the likelihood of the event was reduced to an acceptable level.

History has shown that reliance on multiple layers of protection can lead to complacency, and there are many examples of accidents where controls have eroded over time leaving facilities exposed to high levels of risk. Following the Bhopal accident, the operating company Union Carbide took the decision to reduce and eliminate the requirement for intermediate storage of toxic material on all similar facilities globally. This raises the question of why this inherently safer approach of eliminating hazardous inventory is not taken more proactively in the process industry, rather than waiting for a serious accident to occur.

There is growing evidence that investigations into major accidents are focussing on the need to improve the inherent safety of processes, as discussed in a report [CSB, 2013] on the 2012 explosion at the Chevron Richmond refinery. A pipeline rupture released hydrocarbon fluids leading to a vapour cloud covering 19 people in the immediate area, who narrowly escaped before the cloud ignited causing an explosion and large fire.

In the Chevron incident a carbon steel pipe operating at high temperature failed due to sulfidation corrosion. Although Chevron knew about sulfidation corrosion and the need to use higher specification materials, the hazard had not been recognized by the Process Hazard Analysis team. The CSB report states "*Upgrading metallurgy to a more corrosion resistant material may be a high ranking, inherently safer choice for certain corrosion mechanisms, such as sulfidation corrosion*", and despite some good examples of inherent safety at Chevron, "*the CSB has not identified any documented, thorough analysis of the proposed inherently safer solutions*".

Inherent safety principles

Inherent Safety in the process industry dates back to the 1970's, a concept generally attributed to Process Safety guru Trevor Kletz, who gave a lecture in 1977 titled "What you don't have, can't leak". Despite an acceptance of the importance of Inherent Safety principles, application of structured reviews during the design stage of projects has not gained general acceptance in a similar way to traditional approaches such as Hazard Identification (HAZID) and Hazard and Operability (HAZOP) studies.

Detailed guidance for the application of inherent safety in the chemical process industry is available from the US Center for Chemical Process Safety [CCPS, 2009]. This provides tools to be used by companies to better understand and implement inherent safety concepts, and covers the early stages of chemistry route development. The latter is highly relevant to new processes in the wider chemical industry although less relevant to the Energy sector targeted in the EI guidance.

Traditional process safety approaches generally require 'add-on' risk reduction measures that are costly to install and maintain. By comparison, Inherent Safety in Design provides the opportunity to eliminate hazards or reduce their severity by better design, reducing the overall Capital and Operating Expenditure.

The following definition of Inherent Safety has been provided by the UK Health and Safety Executive (HSE) [Mansfield et al, 1996]:

> *"An 'inherently safer' approach to hazard management is one that tries to avoid or eliminate hazards, or reduce their magnitude, severity, or likelihood of occurrence, by careful attention to the fundamental design and layout. Less reliance is placed on 'add-on' engineered safety systems and features, and procedural controls, which can and do fail".*

Whilst process designers will point to examples of inherent safety features considered to be good practice, it is generally believed that opportunities for applying Inherent Safety in Design are not being systematically assessed. This is potentially due to a lack of awareness of this topic or lack of tools to be applied during normal projects to encourage inherent safety thinking. Design teams may also believe there is a lack of opportunity to apply Inherent Safety in Design for established technology, particularly when the basic design is 'standardised' or provided under license. Inherent Safety in Design can however be applied to all stages of the design lifecycle, although it is generally agreed that the greatest benefits will be obtained during the early concept stage.

Based on HSE guidance, Table 1 provides a standard hierarchy of inherent safety principles, which can be applied to specific hazardous events when searching for design improvement options.

Table 1: Inherent Safety Principles

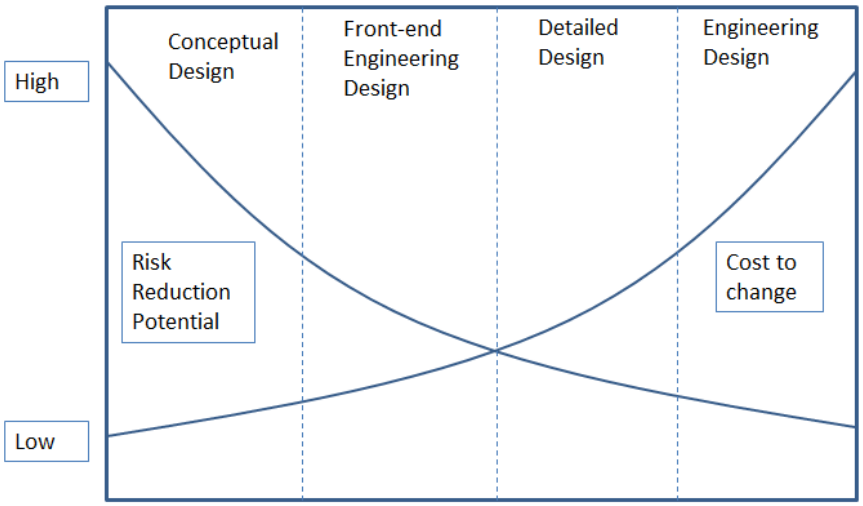
Principle	Interpretation	How
Elimination	Avoid the hazard completely	Change the process, design, layout or activity
Substitution	Reduce the hazard severity by changing nature of hazard	Use less hazardous substance or process equipment
Minimisation (Also called 'Intensification')	Reduce the hazard severity by changing quantity of hazard	Reduce the inventory of hazardous substance.
Moderation (Also called 'Attenuation')	Reduce the hazard severity by minimise the impact of a release	Use less hazardous form of a substance or moderate the processing conditions
Segregation	Limitation of effects reducing potential for hazard to cause harm	Use of physical separation distance or physical barriers between source of hazard and people/environment
Simplification	Reduce the hazard likelihood	Design of equipment and procedures to reduce complexity or reduce frequency of hazardous activity or eliminate opportunities for error or increase the chance of recovery

Codes of practice do not generally encourage the application of inherent safety principles. The hazards associated with inventories of hazardous substances tend to be accepted as essential for the design, and the code focusses on provision of suitable risk reduction measures, and how these are designed and maintained as reliable throughout the facility lifecycle. For this reason design teams should not rely on applying codes of practice in order to optimise the inherent safety of a process, and should consider additional tools such as those as described in this paper.

Benefits of inherent safety

Figure 1 demonstrates the benefits from applying Inherent Safety early in the project before decisions have been made on the choice of equipment. At this stage the design only appears 'on paper', allowing significant changes to be made achieving substantial reduction in risks, at relatively low cost. As the design progresses and the process is increasingly fixed, it becomes difficult and costly to make changes, and the benefits in terms of hazard and risk reduction on the overall process become limited.

Figure 1: Benefits of Inherent Safety in Design early in the project



Based on EI guidance [Energy Institute, 2014], effective application of Inherent Safety in Design can provide the following benefits.

- Unlike traditional approaches to process safety that require expensive 'add-on' risk reduction measures, Inherent Safety in Design provides an opportunity to identify improvements that can reduce overall Capital and Operating expenditure.
- The principle of 'minimisation' challenges large inventories of dangerous substances and promotes smaller equipment with reduced cost and weight, particularly beneficial for offshore platforms.
- Eliminating or reducing hazards early in the design will avoid potential delays caused re-design to meet risk criteria.
- Reduction in process equipment and 'add-on' safety systems reducing the time for design, procurement, construction and installation.
- Less 'add-on' safety systems decreases maintenance, repair and inspection costs during facility lifecycle.
- Reducing the number of hazardous activities and hence number of personnel exposed to risks and the likelihood for human failure, and

In many cases the benefits of an inherent safety improvement option will be clear, whereas in other cases there may be conflicts between options that need detailed assessment to resolve. There may be also be conflicts of interest on the project team, including factors such as; cost implications, operational flexibility, personal preferences, available information or pressures due to project schedule.

The most inherently safe process will not always be the most attractive economically and the technology may be unproven. Design teams should be aware that technology continues to evolve, and inherent safety options that are not economically attractive for a current project should be retained for consideration on future projects.

Legislative drivers

There is increasing expectation from Regulators that inherent safety is assessed during the early stages of design, as shown by quotes below from European and US regulatory bodies. Failure to comply with these requirements could result in significant delays and costs at later stages of the project.

The EU 'Seveso' Directive for onshore plants requires duty holders to demonstrate 'all measures necessary' to prevent and mitigate Major Accident Hazards. The Major Accident Hazard Bureau guidance [MAHB, 2005] on the preparation of a safety report, states that "*inherent safety should be considered first, when feasible (i.e. hazards should always be removed or reduced at source*".

The EU Offshore safety directive 2013 related to offshore oil and gas operations requires: '*a description of the design process for the production operations and systems, from an initial concept to the submitted design or selection of an existing installation, the relevant standards used, and the design concepts included in the process*;' and later requires the Competent Authority to ensure: '*how the design decisions described in the design notification have taken account of risk management so as to ensure inherent safety and environmental principles are incorporated*'.

US OSHA PSM standard requires companies handling hazardous substances to carry out Process Hazard Analysis to identify and assess hazards, but has no specific requirement for Inherent Safety in Design. CSB Interim Investigation report [CSB, 2013] on the Chevron refinery fire, states that inherent safety reviews are currently mandated for high-risk facilities in New Jersey and Contra Costa County California, and there is a trend towards this becoming a federal requirement.

Updated EI guidance

The first issue of EI guidance on Inherent Safety [Energy Institute, 2005] was sponsored by the UK HSE and UK Offshore Operators Association and aimed to reduce the occurrences of adverse findings in design safety cases for the UK Offshore oil and gas sector. The scope of the second issue [Energy Institute, 2014] has been broadened to large and small organizations in the global energy industry, including offshore production platforms, onshore refineries, fuel storage facilities, and power generation stations.

The guidance proposes that companies should develop procedures to ensure that options to improve Inherent Safety are systematically reviewed throughout the design lifecycle. Inherent Safety options should be systematically identified and assessed throughout the design stage to ensure that all opportunities to eliminate or minimize hazards at source have been assessed. For any residual risks, a risk management approach is then needed to ensure that the likelihood has been reduced to a tolerable level in line with appropriate risk tolerability criteria.

It is recognised that implementation of improvement options will in practice be subject to cost, schedule and technology constraints. Assessments should consider total project and lifecycle costs, as inherent safety options may require more expensive major equipment items whilst reducing the overall capital and operating expenditure. Table 2 provides an example of a common hazard associated with overpressure of a vessel, and contrasts the traditional approach taken by design teams with an alternative inherently safer approach that could be adopted.

Table 2: Example of Inherent Safety reducing overall costs

Hazard	Traditional Approach	Inherent Safety Approach
Overpressure and rupture of vessel resulting from increased pressure due to loss of temperature control and contents heated towards temperature of heating medium	Vessel designed for normal operating pressure and provided with high temperature trip isolating heating medium and pressure relief system designed for maximum rate of vapourisation. Comment: This has additional costs to provide safety systems and maintain these systems during the facility lifecycle.	Elimination Provide vessel with design pressure above maximum credible pressure with contents at heating medium temperature. Comment: The cost of the vessel will increase due to requirement for thicker plates, and this may not be a cost effective option for large storage vessels.

EI guidance [Ref 1] provides a staged methodology for applying Inherent Safety in Design, starting at the early Concept stage, and working through the through the subsequent Front-end Engineering Design stage, Process Design stage and Engineering Design stage. The main additional requirement promoted in the guidance is an Inherent Safety workshop during the concept stage. The guidance also describes how Inherent Safety can be effectively evaluated at the later project stages as part of established Process Hazard Analysis techniques such as HAZID and HAZOP studies.

An Inherent Safety workshop will not be appropriate for all projects. The following questions should be addressed at the concept stage, and a structured inherent safety workshop considered if any apply:

- Lack of a clear understanding of project objectives and the processes involved;
- Project significantly impacts on existing facilities;
- Process safety incidents have occurred on similar projects or using similar technology both within the company and within other companies/sectors;
- New hazardous substances being introduced in significant quantities, as raw materials, intermediates, products or utilities/services;
- New process technology required which has a lack of experience for application in this process;
- Significant changes to processing conditions, e.g. pressure, temperature;
- Lack of understanding of the consequences of 'loss of containment' or 'release of energy' in terms of effect on people and the environment;
- Requirement to prepare or update regulatory process safety documentation, e.g. safety case or safety report;
- Increased transportation of hazardous substances, e.g. by road, rail, pipeline or ship;
- Increased hazards to people located in occupied buildings on the facility or people in adjacent facilities or the local neighbourhood;
- Proposed location for the facility subject to external hazards such as; earthquake, aircraft crash, flooding, breach of security, etc.;
- Lack of previous experience and suitable Design Guidelines, Codes of Practice, and Standards, and
- Existing emergency facilities not adequate to meet increased demands.

An Inherent Safety workshop at the concept stage has the objective of identifying process safety hazards and assessing options to eliminate the hazard or reduce severity. The methodology is similar to a traditional HAZID study, except the focus for improvement is elimination and reduction of hazards rather than provision of ‘add on’ risk reduction measures.

A Process Block Diagram for each process option should be prepared in advance of the workshop. For example a new offshore production well may include options for subsea facilities, a normally unmanned installation, or a fully occupied platform. Each block should represent a process system, e.g. storage, heating, separation, or transfer. The blocks and connecting lines should show basic process parameters such as pressure, temperature and fluid composition.

The Inherent Safety workshop team firstly 'brainstorm' potential hazardous event at each process block based on their knowledge and experience. Inherent safety principles in Table 1 should be applied to assess process design options, focussing on elimination or reduction of the hazard, rather than reducing the likelihood by providing 'bolt-on' risk reduction measures. A check should be made that the options considered are towards the top of the hierarchy of controls, i.e. Elimination, Prevention, Control, and finally Mitigation.

Table 3 provides a typical record of the Inherent Safety workshop, detailing the specific hazardous event that has been assessed, with potential improvement options that require further assessment, and any comments on the feasibility of these options.

Table 3 – Inherent Safety workshop record

Block	Hazardous Event	Guideword	IS Option	Feasibility
Condensate bulk storage	Internal explosion causing rupture of atmospheric storage tank due to presence of air and ignition source	Eliminate	Floating roof storage tank to eliminate a vapour space in tank during normal operation	No floating roof tanks on this facility, but this is established technology in the sector

The initial focus during the Inherent Safety workshop should be the operational phase, including start-up, normal operation, shutdown and any other non-routine operations. For each process option, the team should then identify further hazards on the full process during other stages of the lifecycle, including:

- Construction
- Commissioning
- Maintenance
- Inspection
- Decommissioning

Following the Inherent Safety workshop several design options may need to be assessed, for either a process system or an entire process route. Some form of cost-benefit analysis will often be required to choose between options, although in many cases a simple qualitative judgement by an experienced study team should be sufficient.

A HAZID study at the subsequent FEED stage further identifies credible hazard scenarios, and assesses if further measures are required to reduce risks to a tolerable level. HAZID study teams often default to providing additional 'add-on' risk reduction measures to reduce the event likelihood, rather than first looking for inherently safer options. It is recommended that procedures for HAZID studies are reviewed, to ensure that the team is encouraged to fully explore inherently safer design options.

Table 4 provides an example of a hazardous event identified during a HAZID study related to brittle rupture of a process system, and contrasts the traditional design approach to an approach based on inherent safety principles.

Table 4: Example of Inherent Safety during HAZID study

Hazard	Traditional Approach	Inherently Safe Approach
On high pressure crude oil transfer lines, large pressure drops through control valves cause excess cooling due to Joule-Thompson effects leading to pipe temperature below design limits with potential for brittle fracture	Provide temperature sensor on downstream pipework with low temperature trip of valve on upstream supply to prevent design limit being exceeded. Comment: This involves the cost of designing, installing, testing and maintaining a trip system throughout the life of the facility.	Elimination Use higher specification steel pipework with design temperature below minimum credible temperature. Comment: The starting point should be to assume this design spec, unless the cost is excessive and the risks can be shown as tolerable, rather than simpler accepting the traditional approach.

Although opportunities to apply Inherent Safety in Design are limited in the later Process Design stage when HAZOP studies are normally carried out, teams should be encouraged to consider further inherently safer design opportunities. The inherent safety mind-set of the HAZOP study team will be improved if they have been involved in the earlier HAZID study and the proposed Inherent Safety workshop.

Table 5 provides an example of a hazardous deviation identified during a HAZOP study related to 'high pressure' from a pump system, and contrasts that traditional design approach to an approach based on inherently safety principles.

Table 5: Example of Inherent Safety during HAZOP study

Hazard	Traditional Approach	Inherently Safe Approach
Positive displacement pump for liquid transfer with high 'dead head' pressure capable of causing overpressure and rupture of the downstream pipeline if isolated	Positive displacement pumps generally have an internal relief valve. As this is difficult to inspect an external pressure relief system is normally installed, or a high pressure trip system designed to stop the pump. Comment: This type of pump may be required due the nature of the process materials.	Moderate Provide alternative pump type with limited 'dead head' pressure that will allow the pressure to be contained within the design limits of the piping system. Comment: This option will eliminate the overpressure hazard and avoid the need for 'add-on' safety systems

The potential benefits from applying Inherent Safety are further limited at the subsequent Engineering Design stage. However, design teams should be encouraged to have a mind-set that searches for inherently safer options, and the following are provided as examples of inherent safety improvements that can be applied during this stage:

- Components of a safety instrumented system loop should have a 'fail-safe' position that causes the system carry out the required shut-down action;
- Automated valves should have a 'fail-safe' position, typically fully open, fully shut or stay-put, that puts the process into a 'safe' state;
- For pressure relief systems, the design team should be encouraged to challenge the need for the system rather than simply designing a suitably sized system. For example, is it possible to increase the design pressure of the system to contain the highest credible pressure, and
- During hazardous area classification, the design team should challenge the need for a zoned area. For example, could the zoned area around a pump seal be avoided or minimised using a seal-less pump.

Conclusion

Inherent Safety is not a new topic but the process industry has often failed to maximise the hazard reduction potential from this approach and reap the benefits including reduced lifecycle costs. Whilst international codes of practice often fail promote inherent safety and can perpetuate risk reduction using 'bolt-on' safety systems, global regulators are now requiring demonstrations that inherent safety improvement options have been effectively assessed using structured techniques.

This paper has described updated guidance on Inherent Safety in Design published by the Energy Institute and targeted at Project Leaders in the global energy industry, although the approach would be appropriate to all companies in the process industry. The main additional requirement for design teams is to carry out structured Inherent Safety workshops during the concept stage when the greatest opportunity exists to benefit from applying inherent safety. The inherent safety approach has less benefits during the latter stages of design, but should nevertheless be actively encouraged during HAZID and HAZOP studies as a preferred option in place of traditional 'bolt-on' safety systems.

References

1. CCPS, Jan 2009, Inherently Safer Chemical Processes – A Life Cycle Approach, 2nd edition
2. CSB, April 2013, Interim Investigation report: Chevron Richmond Refinery Fire, Draft for public release
3. Energy Institute, June 2005, 1st edition, Guidance for Safer Design of Offshore Installations: An Overview
4. Energy Institute, 2014, 2nd edition, Guidance for Inherent Safety in Design: Reducing process safety hazards whilst optimising CAPEX and OPEX
5. HSE, March 2006, Assessment Principles for Offshore Safety Cases (APOSC)
6. HSE, 2008, Safety Report Assessment Manual (on HSE website)
7. MAHB, 2005, Guidance on the preparation of a safety report to meet the requirements of Directive 96/82/EC as amended by Directive 2003/105/EC (Seveso II)
8. Mansfield, D. Poulter, D.L. Kletz, T. 1996, Improving Inherent Safety, HSE Offshore Technology Report OTH 96521