Inherently Safer Design: it's not just what you do it's the way that you do it, and that's what gets results

Craig Skinner, Process Safety Segment Engineering Technical Authority, Downstream Safety & Operational Risk, BP International Limited, Chertsey Road, Sunbury-on-Thames, TW16 7LN.

Summary

Have you ever been asked to undertake an ISD study and wondered why something so simple is so hard to achieve in practice? Presented below is one way ISD can be applied as a team process - not the only way, but one way - and hinges on the premise that the real value of an ISD team study is the thought processes and safety discussions it initiates as part of creating an inherently safer design. In other words, it's not just what you do, it's the way that you do it, and that's what gets results.

Background

Inherently safer design is a fundamental approach to engineering design that works well when ingrained into the every-day decision-making processes. However one of the challenges we face is that the workplace is a complex system[1] demanding decisions spanning the areas of responsibilities of different discipline engineers. So relying on individuals working alone to know when and how to apply ISD in these many different and complex decisions can lack the rigour of a systematic process and the value of team collaboration and engagement. Considering ISD as a lone-activity is also fundamentally different in approach to PHA studies like HAZID or HAZOP which rely on structured processes and multi-disciplined teams - we would never do a HAZOP alone.

This paper presents methods showing how Inherently Safer Design can be achieved using structured processes by multi-discipline teams to encourage better decision making through collaboration. It then examines ISD application in a case study, before closing with a conclusion.

When to apply ISD in the project life-cycle

ISD is most impactful when applied during the early stage of project development because it often involves altering the fundamental design concept (e.g. improving equipment design) or arrangement (e.g. changing layout). However ISD can also be applied during project execution stages (e.g. location of battery limit isolation valves, sloping grade beneath vessels to prevent hydrocarbon pooling, etc).

What to apply ISD to

ISD can be applied to high severity hazards to reduce risk. High severity hazards may be identified in a hazard identification study such as HAZID, or a quantified risk assessment, QRA. Examples include process hazards (e.g. high-low pressure interfaces), reaction hazards (e.g. exotherms), operating hazards (e.g. overfill), or hazards inherent with the chemicals being used, etc. Applying ISD as a process can be done by incorporating its application into such hazard identification studies, or following such a study. An ISD review provides a systematic approach to eliminate or reduce the severity or probability associated with the high severity hazards by applying the principles of ISD to each hazard in turn.

ISD can also be applied as part of the decision making process when selecting options on a project. Such options will differ on each project, however examples include different conceptual designs being studied during earlier stages of a project, the selection of a technology, and, as in the case study below, selection of location.

How to apply ISD - Method 1: ISD Checklists

The value of applying ISD as a process is that it can be planned and executed in a systematic way, can be tailored to reflect local circumstances, and can make safety decisions on design apparent. This could be as simple as a checklist approach which is particularly useful where it has been a while since the team has applied ISD. Generally checklists work well when used to codify knowledge and prevent critical items being overlooked[5], and in this way, can be applied to ISD to help the team work together and align on how decisions can be made. The checklist below is an extract, as an example. The best results are achieved when this checklist is applied as a team activity, as additional value can be captured in the thought processes and safety discussions it initiates as part of creating an inherently safer design - the process of discussion and collaboration with other team members is often an important factor in facilitating making the right decisions. Equally, a checklist should not be considered a substitute for competency, so if the team is not used to applying ISD, any team session should start with a reminder of the ISD principles which underpin the use of a checklist. Checklists should also include checks to prompt discussion[2] of areas outside the items on the checklist. In other words, the team should also be aware that by its very nature, a checklist can constrain thinking in an otherwise creative activity and the checklist should prompt the team to consider the potential for ISD opportunities outside the scope of the checklist.

Checklist	**Examples of lSD for consideration**
Process Design	Simplify process design (e.g., fewer processing steps, reduced control complexity)
	Reduce equipment count

	Increase design tolerances to cater for excursions from normal operation
	Minimise line size to limit potential leak rate
	Reduce equipment sizes and inventories
	Minimise piping lengths carrying hazardous material
	Reduce the need for storage and intermediate storage
	Avoid sources of ignition by design (e.g., no fired equipment)
	Minimise need for transportation of people and hazardous material
	Adopt less hazardous transportation methods (e.g., pipeline versus road)
Engineering Design	Use of corrosion/erosion resistant materials
	Less small bore connections
	Use of higher reliability rotating equipment to minimise sparing
	Increased component reliability to minimise need for maintenance, disassembly and intervention
	Use of permanent equipment rather than temporary (e.g., for pigging)
	Minimise need for maintenance in hazardous areas
	Adopt simplicity in equipment numbering/layout/HMI design to minimise error potential
	Minimise flanges and unions
	Minimise dead legs and low points
	Eliminate unnecessary instruments
	Bias to non-intrusive instrumentation where practical
	Minimise manual sampling *I* tank dipping *I* chemical injection
	Avoid hot surfaces in hazardous areas
	Bias to automation over manual activity
	Minimise equipment needing frequent inspection
	Provide isolation facilities for safe maintenance, emergency situations
	Design for human error tolerance (e.g., unique connections at multi-connection offloading points)
	Bias for passive over active protection (e.g., fire protection)
	Minimise need for hazardous activity (e.g., pigging, manual handling)
Layout/ Siting	Locate occupied buildings outside hazards zone
	Minimise processing and drains systems in enclosed areas

	Reduce the size of congested areas (reduce VCE)
	Separate equipment to minimise potential for escalation
	Design to direct liquid spills away from hazardous equipment
	Route piping containing hazardous materials away from work areas/vulnerable process equipment
	Route vehicle movements away from hazardous areas and to reduce pedestrian and vehicle interfaces
	Locate critical protective equipment and controls away from process hazards (e.g., firewater pumps/storage)
Activity	Avoid exposing construction workforce to hazards of operating plant
	Use of modular construction to reduce construction workforce exposure
	Minimise activities needing confined space entry, working at height, working in inerted spaces etc.
	Minimise need for scaffolding access in process areas
	Plan to avoid hot work in process areas
	Minimise hot-taps by doing tie-ins during unit outage
	Eliminate or minimise SIMOPS (e.g., drilling while producing wells)
	Minimise need for lifting, elevation and weights
	Minimise temporary clamping
	Minimise work on live equipment
Project Management	Challenge availability targets where they are causing undue complexity and intervention requirements.
	Phasing project execution to avoid simultaneous construction and operation to minimise exposure of construction workforce
	Set construction and start-up philosophy to avoid construction activities during start-up of adjacent equipment

How to apply ISD - Method 2: Apply ISD principles to major hazards

ISD has been refined over the years from the several ISD principles originated by Trevor Kletz[3,4], later aggregated by the CCPS[5], and more recently by the Energy Institute[6] which identifies the following ISD principles: Eliminate, Substitute, Minimise, Moderate, Segregate and Simplify.

Each ISD principle should be applied in turn to each major hazard on a project. Such an ISD review can be undertaken by a small multi-discipline team similar in make-up to a HAZOP team, with involvement of different expertise depending on the nature of the system being reviewed[1]. The selected team would need knowledge of the hazard, of the engineered systems, and how the systems will be operated and maintained in reality (which may differ from the way work is planned to be done).[1] These attributes assist understanding the complexity of the system and are typically not found in a single person, so this is where collaboration by different team members in an ISD review brings value. Members may include process engineering, operations and maintenance representatives, mechanical engineering, and possibly instrument and controls, as well as a process safety engineer. The member of the team with experience in ISD would facilitate the session.

An example of how these ISD principles can be applied to hazards on a project is provided below as a brief reminder of these ISD principles:

- **Eliminate** major hazards or causes of hazards, for example, eliminate overpressure scenarios by increasing design pressure of downstream equipment, and use of seal-less pump technology to improve reliability and reduce risk of high pressure release of flammable materials.
- **Substitute** hazardous materials with less hazardous materials, for example use of aqueous ammonia used for NOx abatement rather than anhydrous, and use of an existing LPG stream to absorb the sulphur components instead of introducing a more caustic chemical into existing units, and use of a new reactor technology with less equipment, less complexity or less hazardous reactant, solvents or catalyst.
- **Minimise** quantities of hazardous material or exposure to potentially hazardous activities, for example, minimize personnel exposure by automating operations in the Coker unit, and minimising the inventory of flammable materials in storage tanks and reactors.
- **Moderate** the conditions to make them less hazardous, for example reduced temperature to avoid high temperature hydrogen attack, create less corrosive conditions, or operate below the flash point or auto-ignition temperature of the hazardous material to moderate the potential impact of any loss of primary containment.
- **Segregate** hazards from people and environment potentially impacted, for example, sour gas inventories and operations away from populations.
- **Simplify** the design of facilities or tasks, for example, simplify the design to remove an intermediate tank by a small increase in the size of a reflux drum, and undertake human factor studies on safety critical tasks to avoid operational complexity and error-traps, and increase system resilience to potential error.

In some organisations, the ISD principle Segregate is addressed as a subset of eliminate and minimise given that the connection to minimising or eliminating the impact by moving a hazard away from the populations or receptor.

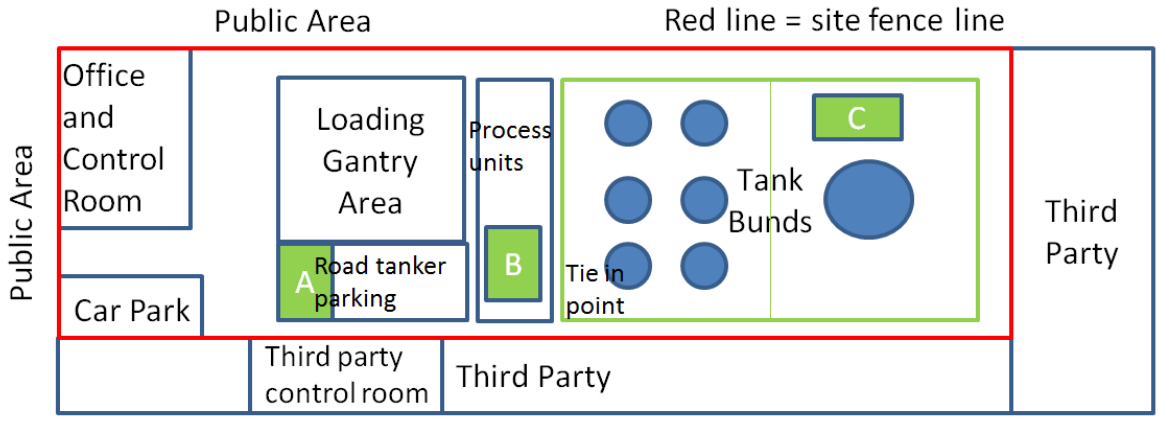
How to apply ISD - Method 3: Applying ISD during option selection on projects

Case Study - how ISD is applied

ISD can be applied during the identification and selection of options on projects. The focus here is to include ISD as one of the factors to be considered as part of the evaluation and decision making process, alongside other criteria such as technology readiness and cost. Whilst all these factors are relevant, the ISD review only considers the safety related factors, and the output of this ISD review is then included in the final decision making by the project team including the other factors.

There are many different ways this ISD review can be done, however the following is one way that has shown to assist decision making. This case study shows how additional value can be extracted from an ISD review in the thought processes and safety discussions it initiates as part of creating an inherently safer design - again, the process of discussion and collaboration with other team members is often an important factor in avoiding silo-thinking and facilitating the decisions being made.

Selection of location often significantly influences the inherent safety of a proposed design, and this case study shows how the ISD process was able to balance different and potentially conflicting safety considerations associated with the location options.



In this case study, an ISD process was used to select a location for new third party operated and maintained equipment on an existing transportation fuels storage tank farm terminal from 3 options, A, B or C, as shown on the diagram above. The objective was to limit the potential hazards to onsite and offsite populations. Prior to the ISD study, the team had identified that:

- Location A is easier for the third party operator to access, however A is nearer an existing third party's control room on a neighbouring site.
- Location B is nearest the incoming pipeline and tie in point to storage tank
- Location C is within a bund to capture any leakages but is the hardest for the third party operator to access.

The problem facing the team was how to balance these differing and potentially conflicting safety considerations and select a location? The solution is to apply ISD to the selection of options.

Case study - method

The basis of this method is selection of the option based on alignment with ISD goals, so the technique starts with identifying these ISD goals. This is typically done at the outset of the project. Each location option is then ranked on alignment to these goals.

Is it worth recognising that sometimes ISD goals can be in tension with each other and/or other project drivers, however the process of identifying the ISD goals is an important part of bringing transparency to such tensions and in doing so, support the overall decision-making process.

On this project, the ISD goals were:

1. Minimise impact on populations, including third party neighbouring sites; (*the terminal had third party light industry populations in buildings on 2 sides*)

2. Minimise congestion to reduce the likelihood of Vapour Cloud Explosion (*given the relationship between congestion and VCEs*)

3. Minimise the potential for safety incidents during construction (*given simultaneous operations and construction - shutting down the site for the period of construction was not a realistic separate option to not conducting the project in this case given the project economics*)

4. Minimise potential for leak sources and containment (*reduce the likelihood of leaks, and contain it if it leaks*)

5. Minimise third party operations on site (*because control of third party operations involves an interface that needs to be managed throughout the lifetime of the plant operation, and relies on the lowest rung in the hierarchy of risk reduction techniques, procedural controls*).

Each location option was then ranked by the team against alignment to these goals using the following scoring. The scores were then summed for each option, and the option with the lowest score considered the inherently safer design on the basis of alignment with these ISD goals. There is no scientific approach to the selection of the numerical values in the chart, except that a high score of 10 provides an indicator of higher relative risk. This is something that we wish to avoid since it does not align with our ISD goals. A low score indicates stronger alignment with the ISD goals and a potentially lower relative risk. Not all goals are considered equal, so often teams decide to apply a weighting to rank one goal higher than another.

Ranking	Description (*)
10	Option not aligned with ISD goal, and/or major accident risk cannot be effectively controlled or reduced with high integrity engineered systems and/or rigorous operations and maintenance procedures
7	Major accident hazard can be managed by high integrity engineered systems (SIF etc) and/or rigorous operations and maintenance procedures
5	Hazard of medium risk that can be managed by standard engineering design, operation and maintenance procedures, and safeguards (however no requirement for high integrity engineered systems)
2	Hazard of lower risk that can be managed by standard engineering design, operation and maintenance procedures
0	Option strongly aligned with ISD goal, and/or hazard is low risk not requiring extensive systems and controls to manage risk

(*) Many organisations have ranking criteria defining major accident hazards, and severity and probability that can be used to determine whether hazard is lower risk, medium risk, etc.

Case Study - findings

Using this analysis, location B had the lowest score and so was selected. However the results were almost equal and although there is the potential for undue focus on the numbers and scoring, it is suggested that the real value of the ISD study was in the thought processes and safety discussions it initiated to understand the hazards associated with each option, and create an inherently safer design. This is explained as follows.

Goal 1: the team was able to agree that Option A is least aligned with the goal because this location is nearest the third party control room on adjacent property, and option C is furthest away so most aligned with this goal.

Goal 2: the team was able to agree that Option A is least aligned with the goal because it reduces the space for road tanker parking so tankers would have to park directly next to each other, potentially creating a congested volume below the tankers sufficient to support a VCE in the event of a loss of primary containment LOPC. This discussion was enabled by involvement of an engineer with process safety expertise familiar with the major industrial accident that occurred in 1991 at St Herblain involving 6 trucks parked next to each other - so showing the value of a multi-discipline team approach.

Goal 3: the team was able to agree that Option A is most aligned with the goal because of ease of access. Option C is least aligned because of more complex design involving extensive pipe runs into an adjacent bund and back to the tie in point near to location B.

Goal 4: the team was able to agree that Option C is least aligned with this goal since although within a bund, it had most flanges and a complicated routing – however this discussion also meant the team agreed to reduce the number of flanges as an ISD opportunity, whatever option was selected.

Goal 5, the team was able to agree that Option C increases potential for interface issues between third party and the operator during third party maintenance/ testing of their equipment inside the tank bund undertaken under operator's control of work system.

Option B was selected at the end of the ISD review on the basis of the lowest total score on alignment with ISD goals, and this was rationalised as this location being within an existing process area, and maximizing the distance from personnel without requiring a complex piping design. In a way, the team could see this option was a compromise between the differing benefits and downsides of Options A and C with respect to the ISD goals.

Case study - lesson learned

This approach to ISD discussions can also be used earlier in the project when first defining project options. Team discussion of ISD can facilitate identifying project options that are well aligned with ISD goals.

Time can be wasted considering options in an ISD study that are not technically feasible, so this should be avoided. Other locations were also considered prior to the ISD review including offsite, however only those that were technically feasible should be included in the ISD review. An example here was locating the equipment in the car park, but this was not technically feasible since the business requires this space to park the tanker driver's own cars and no space was available offsite.

The scoring process also helps the team to identify specific safety concerns with each project option, which in turn offers opportunities for the team to identify ways to further reduce risks of a project option by applying ISD principles. For example, in this case study, the selection of option B was not the end of the ISD process - once Option B was selected, an ISD checklist was applied to further reduce the risk; for example, flanges, dead-legs and temporary equipment were minimised, and this discussion highlighted a further option for the business to consider - ownership and operation of the equipment by the site operator itself to avoid the need for additional third party operations at the site.

Conclusion

Whilst ISD remains a fundamental approach to engineering design that all engineers should adopt as part of their ingrained behaviours, additional value can be gained in applying it as a team through the thought processes and safety discussions it initiates as part of creating an inherently safer design. Applying ISD as a process involving a team creating a systematic way to apply ISD opportunities and unlock the potential value to create an inherently safer design as part of a balanced and robust decision making process.

Designing for safer operations means everyone returns home safely without harm after a day at work - a goal we all wish to achieve. However achieving this goal is not always simple, and starts in the design stage with ISD and how it's applied. In other words, it's not just what you do, it's the way that you do it, and that's what gets results.

Acknowledgments

The author would like to acknowledge the team effort and expertise of fellow colleagues who have contributed to developing and refining the ISD methods detailed in this paper over many years, with a special mention to colleagues Dave Fargie and Milton Vogel; and addition, a thank-you to Zaf Iqbal for the feedback which inspired the writing of this paper.

References

1. Eurocontrol, "Systems Thinking for Safety: Ten Principles. A White Paper, Moving towards Safety-II", European Organisation for the Safety of Air Navigation (EUROCONTROL), www.eurocontrol.int, 2014

2. Gawande, A. "The Checklist Manifesto: How To Get Things Right", Metropolitan Books of Henry Holt and Company LLC, 2009

3. Kletz, T. A. "What you don't have, can't leak", Chemical and Industry, 1978.

4. Kletz, T.A. Process Plants, A Handbook for Inherently Safer Design, Bristol, PA, Taylor & Francis, 1998.

5. Centre for Chemical Process Safety (CCPS), Inherently Safer Chemical Processes: A Life Cycle Approach, 2nd Edition, American Institute of Chemical Engineers, 2009.

6. Energy Institute, Guidance on applying inherently safety in design: Reducing process safety hazards whilst optimising capex and opex, 2nd Edition, London, 2014