Inherent Safety: It's Common Sense, Now for Common Practice!

David Edwards, John Foster, Daniel Linwood, Mark McBride-Wright & Peter Russell
David.Edwards@Granherne.com
Granherne Limited, Hill Park Court, Springfield Drive, Leatherhead, Surrey, KT22 7NL, UK

We describe some of the barriers to more widespread adoption of Inherently Safer Design (ISrD) and how we have overcome them in Granherne. We have found that it is essential to educate engineers about the benefits of ISrD and to promote ISrD as an attitude of mind. Committed project leadership is also crucial to success. It is important to recognise that ISrD has most benefit early in the design process and that it is an essential first step in the demonstration of 'ALARP' and the safety risk management process. We have developed practical, workshop-based methods that follow the early project stage sequence, for identifying, assessing and recording ISrD features of designs. We provide examples of the significant benefits of the methods to the projects that have used them.

Keywords: inherently safer design, oil and gas, ALARP, risk management, workshop

Introduction

Inherent Safety (IS) is often described as common sense and, according to a comprehensive survey of the field [Gupta, 2002], it is common knowledge. However, as Professor Paul Amyotte comments in his Preface to the Second Edition of the classic book on the subject, 'Process Plants: A Handbook for Inherently Safer Design' [Kletz, 2010], Inherently Safer Design (ISrD) needs to move *'into the realm of common application and practice'*.

According to a recent review of progress since 2001 and opportunities ahead [Srinivasan, 2012]: '*While there is a large body of research on various inherent safety assessment methods, there has been relatively little said on the best ways to incorporate them into the work processes of practicing engineers.'*

This paper firstly sets out why ISrD must now be routinely applied (not least because regulations are increasingly requiring it) and then describes how the engineers at Granherne, which is the conceptual design and consultancy division of KBR, practise ISrD in our designs of upstream oil and gas installations. This has been achieved by making IS an attitude of mind, by the safety discipline working with engineers as part of the mainstream design effort and employing tools to assess the existing features of designs and challenge projects to incorporate further features, where practicable.

We do not give a detailed explanation of IS here; there are many excellent papers and books for reference, such as: the classic work by Kletz [Kletz, 2010], an American Institution of Chemical Engineers Center for Chemical Process Safety (CCPS) guide book [CCPS, 2009], [Srinivasan, 2012] (which has an extensive reference list) and there is a training package available from the Institution of Chemical Engineers (IChemE). Very briefly:

- Trevor Kletz had the idea after the Flixborough accident in 1974, developed it in his many books and papers and tirelessly promoted IS and ISrD right up to his death in 2013;
- Edwards and Lawrence, [Edwards, 1993] were the first to publish a method for assessing IS and they have been followed by many others – but mostly aimed at chemical processes; and
- Graham Dalzell [Dalzell, 2004] put the onus for ISrD back with the people, whether they be leaders – project or otherwise, designers, operators, suppliers, etc. and maintains that it is an *'attitude of mind'*.

Simply put, Inherently Safer (ISr) designers render a plant safer by implementing four principles of ISrD:

1. **Eliminate** the potential for harm (hazards);
2. **Reduce** the **severity** or **scale** of the consequences of the hazards;
3. **Reduce** the **likelihoods** of the hazards occurrence; and
4. **Separate** or **protect** people from the hazards.

They achieve this by careful attention to the fundamental design and layout, with less reliance placed on 'added-on', engineered safety systems and procedural controls, which can and do fail. However, it is difficult to eliminate the major hazard from oil and gas production – it is the oil and gas! Therefore ISrD principles 2, 3 and 4 should be more practised.

An example of an incident where many lives might have been saved by the implementation of principle 4 is provided by the Piper Alpha disaster. Figure 1 shows that the Living Quarters (LQ) of this platform was on top of what became a huge blow torch, which killed 167 people. As Paul Davison, Chairman of the Safety and Reliability Society (SaRS) has pointed out in their Newsletter, number 278 [SaRS, 2014], '*No Lifeboats were used to save the 67 survivors…*' and helicopters could not have helped either. Paul concludes: *'… lifeboat evacuation will never be as reliable as escaping from a hazardous event onshore or on a bridge-linked platform, where you could run away from the danger'*.

If the LQ had been on a separate platform, bridge-linked to the production platform, most would not have died. Therefore, if you cannot eliminate a hazard, then separate people from it. In a case like this, reducing the likelihood of a catastrophic event is not an adequate safeguard, because the consequences are too dire and must be avoided.

ISrD is the foundation of Granherne's hazard-focussed, risk-based approach to design. Where, risk is the combination of an **estimate** of the consequences of a realised hazard and an **estimate** of the likelihood of this happening.

Risk = function(estimated realised hazard consequence, estimated likelihood of realisation)

Risk is often expressed as fatalities per year. For example:

Risk = (Potential Fatalities) X (Estimated Occurrences per Year)

Figure 1. The Piper Alpha platform before and after the disaster

Piper Alpha, with LQ
226 people are on the platform

Piper Alpha, without LQ
165 of the 226 are now dead; 2 rescuers are also dead

Eliminating or separating people from hazards is definitive, because it does not rely on reducing the estimated likelihood of events. Professor Andrew Hopkins (the author of many influential books on the organisational and cultural causes of major accidents) puts it well: 'The fact that you've gone for 20 years without a catastrophic event is no guarantee that there won't be one tomorrow.'

ISrD is the first step in a risk-based regulatory regime, after which risks must be reduced to be As Low As Reasonably Practicable (ALARP) by passive, then active and finally procedural safety measures. A demonstration of ALARP must be made to the regulator as part of a safety case in order to be allowed to operate an installation.

Further Motivation for ISrD

Perversely, it seems that the widespread adoption of ISrD, which is the best available technique for reducing risk to people and the environment, has been prevented by the inherent aversion to commercial risk and the conservatism of the process industries. This aversion and conservatism finds expression most often in the approach to design, with its focus on cost and schedule. However, apart from the obvious safety benefits, there are many other compelling reasons for practising ISrD, which have been written about at length elsewhere, for example in most of the references to this paper and most recently in the IChemE 'Loss Prevention Bulletin', [Edwards, 2014 and Ellis, 2014]. These reasons for ISrD may be grouped by:

- Regulation and investigation;
- Standards and company requirements;
- Cost and weight reduction; and
- Preservation of reputation;

Regulation and investigation

ISrD is a now a requirement of many regulatory regimes with a growing expectation from regulators that IS is assessed and that the measures taken are recorded during the early stages of design. Failure to comply could result in significant delays and costs in the later stages of design.

The United Kingdom (UK) Health and Safety Executive (HSE) 'Assessment Principles for Offshore Safety Cases', [HSE, 2006], advocates a hierarchical approach to managing Major Accident Hazards (MAH), with IS at the top. Principle 16 states that: *'The safety case should explain how inherently safer design concepts have been applied in the design decisions taken',*

and *'Inherently safer design requires the hazard management strategy to be developed at a very early stage in the design process'*.

The HSE 'Safety Report Assessment Manual' (SRAM) [HSE, 2007] for onshore safety reports states that: *'Operators should therefore demonstrate that they have looked at ways of avoiding the hazards or reducing them at source through the application of the principles of inherent safety. It is more likely to be reasonably practicable to take measures to avoid or reduce hazards at source during the design stage of new plant and equipment and as early as possible during the design process. It is at this stage that assessors particularly need to look for evidence of the use of principles of inherent safety to remove or reduce hazards to people and the environment.'*

The need to demonstrate a proactive approach during the design process has been strengthened in the recent EU Offshore Safety Directive [EU, 2013], which requires the Competent Authority to: *'…ensure that the risk management … have anticipated all foreseeable situations including: 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'*.

Furthermore, authorities are focussing on IS during accident investigations. For example, the US Chemical Safety and Hazard Investigation Board (CSB) investigation into the 2012 Richmond refinery fire found that serious sulphidation corrosion was the root cause of the accident due to using an inherently unsafe material of construction for a pipe. The report states that: *'Chevron did not regularly or rigorously apply inherently safer technology, which provides an opportunity for preventing major accidents, in its PHAs* [Process Hazard Analysis], *MOCs* [Management of Change], *incident investigation recommendations, or during turnarounds',* [CSB, 2014].

Standards and Company Requirements

It is notable that one of the widely used, 'added-on' safety standards, 'Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 1 (IEC 61511)' [ISA, 2004], encourages ISrD:

- 'In most situations, safety is best achieved by an inherently safe process design. If necessary, this may be combined with a protective system or systems to address any residual identified risk.' (Introduction); and
- 'If the analysis results in a safety integrity level of 4 being assigned to a safety instrumented function, consideration shall be given to changing the process design in such a way that it becomes more inherently safe or adding additional layers of protection.' (Allocation of safety functions to protection layers).

ISrD appears in most company standards and guidance, for example:

- Statoil GL0282, 'Guidelines for risk and emergency preparedness analysis', [Statoil, 2010], states: 'Safety achieved through inherently safe process design (see I.1) should always be applied whenever reasonably practicable.'
- ISrD is mentioned in many BP Engineering Technical Practices (ETP), including one dedicated to ISrD, '48-04 Inherently Safer Design (ISD)', [BP, 2008].

Cost and Weight Reduction

One of Trevor Kletz's favourite slides was of a Model T Ford, which was the world's first affordable motor car because of its simple, uncluttered design. Henry Ford said: *"what you don't fit costs you nothing and needs no maintenance"*. Safety systems are costly to install and maintain. However, designs often factor in the safety equipment, accepting the capital cost but ignoring the lifecycle cost. Reducing maintenance increases uptime, reduces plant disturbances and reduces exposure of maintenance personnel to hazards. Also, many accidents happen during or after maintenance. Offshore, not fitting equipment also saves weight.

Cost and weight can be saved by designing with smaller inventories, which reduce the hazards. Fully rating vessels and pipework for the highest possible pressure that might be encountered will increase the cost and weight of the process equipment but it will not require heavy and costly pressure relief valves, which will also reduce maintenance.

Preservation of Reputation

The major benefit of ISrD is the preservation of reputation by removal of risk. People who are separated from a hazard cannot be hurt by it. Fully rated pipes and vessels cannot be over-pressurised. This is good for the operators – their lives are not at risk and good for the shareholders – their money is not at risk. An ISrD installation should promote healthy sleep patterns for the Chief Executive too!

A Practical Approach

Inherently Safer Design is Better Done Early

As stated in the HSE SRAM, ISrD has the most impact when applied at the conceptual design stage. Another of Trevor Kletz's favourite slides, Figure 2 illustrates that the cost of making a design change is relatively inexpensive at the concept phase but it can have a significant impact on reducing risk. Changes further along the process design chain through FEED and detailed design will cost far more once key equipment choices have been made but the potential risk reduction is reduced. This is why it is particularly important that conceptual design specialists, such as Granherne, practice ISrD. However, ISrD measures can be implemented at any time.

An accident during operation will dwarf any costs due to design changes and, as Trevor has said: *"There's an old saying that if you think safety is expensive, try an accident. Accidents cost a lot of money. And, not only in damage to plant and in claims for injury, but also in the loss of the company's reputation."*

Inherently Safer Attitude and Leadership

Although there are many methods for assessing designs for IS [Ahmad, 2014], none take cognizance of design as an interactive team activity, whereas everyone involved in the design: engineers, technicians, operators, management, etc., must be involved in identifying hazards and achieving an ISrD. A mind-set, which is similar to that promoted by many current company behavioural safety programs, such as 'Incident and Injury Free' or 'Zero Harm', is required. These programs are founded on the belief that 'zero accidents' is an achievable goal and that everyone is responsible for safety. Analogously, ISrD provides the means to eliminate the hazards that cause the accidents; it is up to all, designers and others, to achieve the goal of zero accidents by implementing the ISrD principles.

As illustrated in Figure 3, improvements in engineering and hardware, for example the introduction of machinery guarding, over time lead to a reduction in the number of incidents. However, major accidents continued to occur. After the Flixborough explosion in 1974, the Health and Safety at Work etc. Act 1974 [UK Government, 1974] was enacted. This required mandatory reporting of incidents and active risk management. This has led to a further reduction in incident rates, which have again plateaued and, nevertheless, major accidents still occur.

Figure 2. Benefits of ISrD early in the project

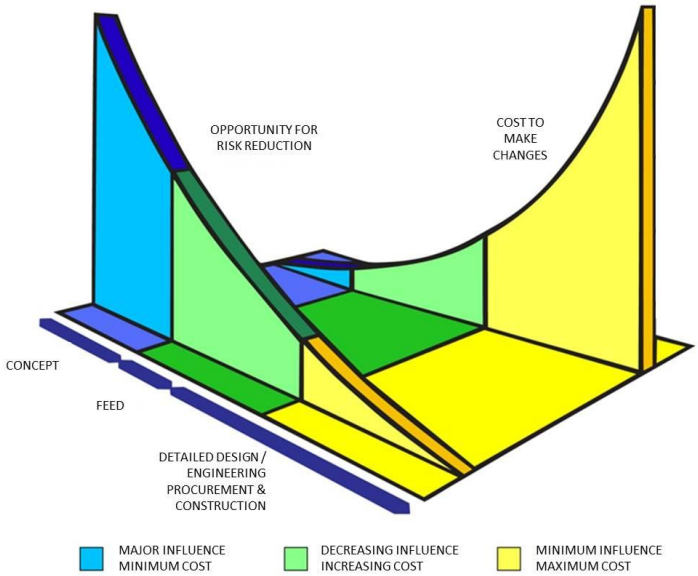
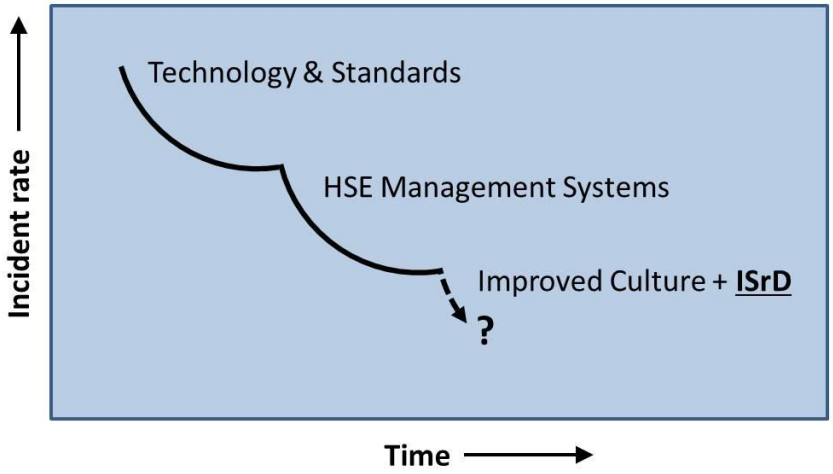


Figure 3: Reduction in incident rate through time



The National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling (NCDH), in its Report to the [USA] President, 'Deep Water The Gulf Oil Disaster and the Future of Offshore Drilling', [NCDH, 2011], highlighted the observation made by the Board that investigated the loss of the Columbia space shuttle that*: 'complex systems almost always fail in complex ways'*. Major accidents still happen, because we cannot anticipate or estimate (design) for every eventuality – complex systems, whether technical or human, also fail in unpredictable ways. We cannot reduce the incident rate further by systems alone.

However, the combination of improved safety culture – the belief that we can achieve zero accidents and the ISrD principles should drive the incident rate further down.

Bringing *ISrD 'into the realm of common application and practice'* has two pre-requisites:

- Knowledge of and commitment to ISrD by the design team; and
- Leadership to make it happen.

Building knowledge and commitment is a continual process and requires an ISrD champion. In Granherne, the lead author of this paper has a long-standing involvement with ISrD and he takes every opportunity to educate people and promote the application of ISrD. This began with presentations at 'lunch and learn' sessions and using meeting safety moments. Participants at workshops, such as HAZard IDentification (HAZID), Design Review and HAZard and OPerability (HAZOP), are now given an IS and ISrD briefing at the start and are encouraged to seek Inherently Safer (ISr) solutions. Members of the safety department are encouraged to engage with the designers, particularly process and layouts, at the start of a project, in order to influence the design and avoid hazards, rather than wait to be asked to address identified safety issues in the design.

Knowledge and commitment fosters an ISrD attitude, in which everyone asks, [Dalzell, 2004]:

- What is dangerous;
- Why is it dangerous; and
- Is there a safer way?

Having built the attitude and commitment to ISrD, strong project leadership is needed to ensure that opportunities for ISrD are identified, assessed and implemented, if practicable.

To deploy the knowledge and commitment Granherne employs workshops, as recommended by the Energy Institute, 'Guidance on applying inherent safety in design: Reducing process safety hazards whilst optimising CAPEX and OPEX', [Energy Institute, 2014].

Inherently Safer Design Workshops

Granherne is committed to the workshop approach, because workshops:

- Are a conducive environment for creative discussion and brainstorming, which is necessary for considering ISrD;
- Ensure that all disciplines are party to the dialogue, minimising unexpected conflict when changes are implemented in the design;
- Induce engagement by the project team and provide a forum to reinforce the ISrD mind-set; and
    - Are an effective method to:
    - challenge the design and established practice;
    - identify and record existing and new ISrD measures; and
    - assign discipline or personal responsibility for executing actions to implement workshop resolutions.

The opportunities for making plant ISr decrease as the design progresses. The ISrD workshops must be held sufficiently early in the project stage that it is possible to make fundamental design changes, if any are identified that would render the facility ISr. An ISrD workshop should be the first event in the risk management and ALARP process. Also, an early unstructured event allows the engineers to 'think outside of the box' about the hazards, without being constrained by the structure of the HAZID. For these reasons, the ISrD workshop should be held before the HAZID, which is a structured and exhaustive identification and confirmation of hazards, existing safeguards and actions required to correct deficiencies. However, ISrD solutions should still be sought at the HAZID.

The scope of the workshops should encompass the lifecycle of the facilities, from fabrication, through installation, Hook-Up and Commissioning (HUC), operations and maintenance to final decommissioning.

The design concepts should be discussed with the engineers before the workshops. The worksheets should be populated with any identified existing ISrD features and any obvious candidates for consideration by the workshop.

The documentation that is required is, in order of priority:

- Plant layout;
- Expected number of people and locations;
- Process flow diagrams;
- Material properties
- Major equipment specifications; and

- Material and energy balances.

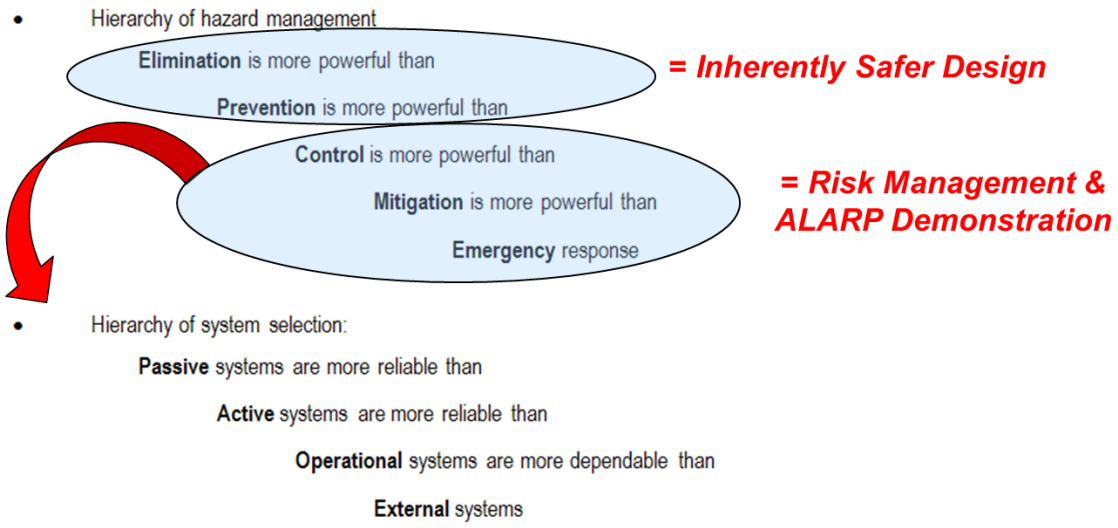
The workshops must be led by a facilitator, who is experienced at running workshops and has a good knowledge of ISrD and they should be attended by:

- Discipline lead engineers, including: process, layout, structural, subsea and safety, in order to enable a complete appreciation of the design during discussions. Others may be called in as needed.
- Representatives for the facility and marine operations.

Anyone who has a good understanding of the project and design in its entirety is particularly useful. There must be someone present who can describe the part of the design under review at any point in the workshop.

Workshops should start with an introductory presentation in which the facilitator explains ISrD and why it is important. Do not assume that people at the workshop will know what is required of them or be motivated to contribute; however, an overview of regulatory and company requirements and the relation of ISrD to cost might help. ISrD should also be placed in the wider context of technical safety and demonstration of ALARP. We have found that the graphic shown in Figure 4 is useful for explaining the ISrD principles and relating them to the hierarchy of measures used for demonstration of ALARP and risk management. Figure 1.1, '*A systematic approach to loss prevention (hierarchy of controls)'*, on page 16 of Kletz and Amyotte's book [Kletz, 2010] is also very good in this regard. Finally, the workshop process must be described and it must be stressed that, despite the title, the purpose is not to do design work but to document existing ISrD features and brainstorm to identify further possibilities for ISrD.

Figure 4. ISrD in the Context of Risk Management and ALARP Demonstration



The discussions are recorded in a spreadsheet, which provides the structure for the event. We use the traditional keyword approach that started with Kletz. However, the 4 principles, which are listed in the Introduction, were recast into 3 categories: hazards, plant and people, with associated keywords, and 3-letter mnemonics, which are presented in Table 1. These keywords are a permanent part of the workshop spreadsheet display.

Table 1. ISrD Keywords and Mnemonics

ELIminate / REDuce **Hazards**,
SIMplify / improve RELiability of the **Plant**,
SEParate / PROtect **People** from hazards and aid their ESCape.

ELImination of hazards is the most desirable ISrD aspect, although it is also the most difficult to achieve. For example, eliminating the gas might mean that we do not produce a field at all! Each subsequent word can be considered as generally less desirable in terms of ISrD. However, if elimination of a major hazard is not possible, SEParation or PROtection is clearly a priority.

REDuce includes any method of diminishing hazards, including substitution of chemicals or processes and moderation.

SIMple plant offers fewer paths to failure and RELiable equipment ensures that there are fewer deviations from normal operations, less exposure of maintenance personnel to hazards and greater plant uptime.

Though PROtection of personnel and means of ESCape are desirable design principles, they are part of risk management and reduction to ALARP, rather than ISrD measures, because the hazard and occurrence likelihood are unchanged.

The keywords can be supplemented by lists of principles and explanatory guidewords and phrases, such as those in Table 2.

Table 2. ISrD Principles and Guidewords and Phrases

Principle	Guidewords and Phrases
Avoid / eliminate / contain the hazard	Eliminate separation (multi-phase pumping), eliminate stages, error tolerance (fully rate), safest location (away from shipping)
Minimise / reduce the hazard severity	Intensify, substitute, attenuate / moderate
Simplify	Fail safe, reduced exposure, reduced likelihood, life cycle cost, reduce instrumentation, multi-phase metering
Reliable and robust	Maintenance, life cycle cost, long life, reduced exposure, flangeless piping
Segregate / protect	Distance, barriers, subsea processing

The early project stages answer two questions:

- Is there at least one viable project definition; and
- What is the optimum concept?

The project stages (in chronological order) at which workshops should be held are:

- **Appraise:** to determine project feasibility, alignment with business strategy, understand risks and uncertainties and generate design concepts;
- **Select:** to develop concepts sufficiently to select the preferred project concept and do the pre-Front End Engineering Design (FEED); and
- **Define:** to finalise the project scope, cost, schedule and budget and do the FEED for the selected concept.

Appraise

In Appraise, the aim is to determine if the project is feasible and to generate design concepts. This is when there is maximum influence on the IS of the final design. Therefore, consideration of IS must be integrated into the concept generation process, for example at project framing workshops, otherwise feasible ISr concepts may be rejected on perception of cost or practicality. An ISrD perspective might also be the catalyst for discovering new concepts.

Some examples of ISr project choices which may be mooted in the Appraise phase are:

- Keeping hydrocarbons subsea:
    - multiphase (oil, gas, water) pumping to shore, where ISrD is easier and cheaper to achieve;
    - because there are no risers, vulnerable inventories are reduced;
    - subsea separation can offer topsides weight savings and vessel wall thickness reductions (through lower gauge pressures);
    - however, operability and maintenance must be carefully considered and a philosophy of using Remote Operated Vehicles (ROV), rather than diver intervention, should be adopted.
- Facilities designed to operate unattended or accommodation is provided on bridge-linked platforms.
- Separation of gas at the earliest possible stage and simplification of gas processing.
- Removal of test system and separator(s) through provision of multiphase (fiscal) metering.
- Trade off frequency of supply, e.g. of diesel, against inventory size / alternative generation equipment and associated maintenance, e.g. wind turbines.
- Comprehensive field development planning to prevent piecemeal alterations later, e.g. Piper Alpha was never designed as a gas collection hub.
- A location remote from shipping routes.
- Structures and equipment designed for ease of inspection and maintenance.

Options proposed and discussed at Appraise workshops should be subject to later analysis, for example normally un-staffed facilities reduce exposure of people to hydrocarbon hazards but increase transport risks.

Select

The Select project stage involves making fundamental choices about field development and determining the preferred design out of several concepts, which have been obtained by elaborating on ideas from the Appraise stage. Therefore a comparative method is most helpful in discussing ISrD at this stage.

The aims of the Select ISrD Workshop are to:

- Determine ISr features of the alternative concepts;
- Generate ideas for making the designs ISr;
- Rank the alternative concepts for IS; and
- Document the ISr features of the alternative concepts in the ISrD register.

One possible further outcome of the workshop is a new ISr concept.

Two different approaches have been trialled, which are described below. Whereas the first was more prescriptive and excluded ranking or scoring of results, the second was more freely formed to encourage idea generation and included a comparative scoring system for overall appraisal of each concept.

Key requirements for the workshop are to ensure that for the alternative concepts:

- The design development is to the same level of detail;
- The documentation is consistent; and
- There are people present, who are knowledgeable about each concept and who are able to describe them to the workshop.

Project 1

This project was about installing new compression capacity to increase the gas production rate from an offshore gas field to shore. The Concept Safety Review (CSR) began with a multi-disciplinary ISrD Workshop, which was attended by Granherne engineers and design and operations representatives from the project clients. The aim was to provide an initial safety screening and comparison of the project design concepts, which are listed in Table 3.

The workshop considered the concepts with respect to a list of ISrD aspects around: the design definition, operation and maintainability and Installation and HUC. An extract from the aspects list is presented in Table 4.

Table 3. Compression Installation Concepts

Concept	Description
1	Limited (by available space) compression facilities on an existing Platform A
2	Full compression facilities on a new Platform B, which is bridge-linked to Platform A
3	Limited (by lower pipeline operating pressure) compression facilities at the onshore reception facilities

Table 4. Operational and Maintainability ISrD Aspects / Guidewords

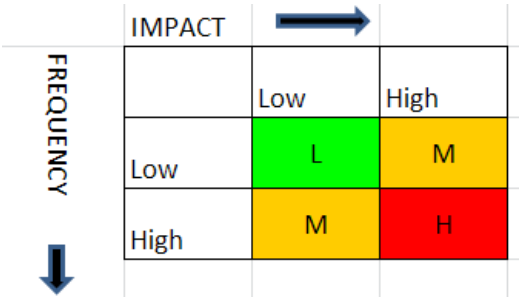
Weighting	Definition
H	Eliminate / Minimise additional helicopter transport (helicopters account for about 1/3 of all offshore risk)
M	Eliminate / Minimise boat transfer between facilities.
M	Minimise operational / maintenance hazards - incompatibility with existing equipment & materials - new / novel equipment – proven, requires training? - high human / machine interaction.
M	Optimise control room and Integrated Control and Safety System (ICSS) - multiple control points - point of command - conflict between old / new systems.
L	Optimise the working environment / minimise human-machine interface - Living Quarters (LQ) module location and design - minimise access requirements at height / overboard - high noise / vibration equipment remote from LQ.
L	Other - to be defined

The ISrD Aspects were given a 'Weighting' which is based on coarse impact and frequency categories, which were:

- Impact
    - High = multiple fatality
    - Low = single fatality / injury
- Frequency
    - High = constant / frequent activity
    - Low = intermittent / rare activity

The Aspect 'Weighting' is according to the matrix shown in Table 5.

Table 5. Aspect Weighting Matrix



The workshop process was as follows.

1. Agree and confirm the ISrD Aspects and related Guidewords to be applied in the workshop.
2. Review each concept with respect to the Aspects and Guidewords.
3. Record the qualitative 'Pros' and 'Cons' of each concept for each aspect.
4. Form a consensus opinion about the degree to which each concept achieves an ISrD; the concept either complies with most, some or few ISrD principles, this last outcome indicating that the concept is inherently unsafe.

The workshop considered:

- Primarily the new and modified equipment operation and layout;
- Both hazards presented by the proposed new compression facilities to the existing Platform A or onshore facilities and hazards presented by the existing operations to the new facilities; and
- Installation and HUC hazards at a high level only.

The CSR report included the ISrD workshop findings and identified the design safety implications with respect to MAH categories for each of the concepts. The CSR conclusions for each option are summarised as follows.

Concept 1 – The addition of a compression module directly adjacent to the new LQ was deemed to be not IS (nor would it be considered best practice for a new-build installation). ALARP demonstration would have been difficult and a robust assessment would have been required to determine the impacts of MAH events, due to the new compression module, on the LQ / Temporary Refuge (TR) and adjacent primary evacuation systems, which are Totally Enclosed Motor Propelled Survival Craft (TEMPSC) and a helideck. There were also additional safety considerations in relation to the impact on helicopter operations, crane operations and well intervention activities.

Concept 2 – This concept presented a significantly ISr development. The new hazards associated with the new compression facilities were remote from the LQ / TR and primary evacuation facilities by virtue of the bridge separation. A new build platform would allow the layout to be arranged to achieve an optimum safety gradient (hazardous to non-hazardous) with physical fire / blast segregation as required.

Concept 3 – Onshore processing is generally the safest since people can be given maximum separation from potential MAH events. However, given that the onshore concept was likely to represent only an interim solution and at some later stage offshore compression would be required, the ISrD aspects of the eventual overall concept should also be considered.

A principle benefit of the ISrD workshop was that it convinced the client to move away from a layout which was not IS. Concept 1 sited a compression module next to the planned location for a new LQ which would not have reduced the risk to ALARP. Also, this analysis was documented and so would be difficult to subsequently ignore.

Building the new Platform B (Concept 2) is more expensive than adding more equipment on to existing Platform A. However, increased space available on Platform B could be an enabler for future field development, which would provide greater revenues from the field. The benefit of upfront investment for future field development would perhaps not have become clear to the clients had the ISrD workshop not taken place.

Consequently, Concept 2 was further developed when more information on future prospects was available and this was the recommended concept for transition to the next project stage.

Project 2

The Project 2 ISrD workshop considered four concepts for the addition of a new bridge-linked platform and associated subsea flowlines for enhanced oil recovery, using new technology, to an existing installation in the North Sea. The workshop began with a presentation by the facilitator about IS and ISrD. The Project 1 list of guidewords was not used, in order to enable a more free flowing brainstorming session. The workshop was guided by the Table 1 keywords and the aspects of the design were considered in categories, such as: *Field configuration, Environment* and the project engineering disciplines (*process, mechanical, etc.*).

A comparative coarse ranking system with associated scores, which is shown in Table 6, was used to capture the workshop participants' consensus about the level of IS in the design of each concept for each aspect. The aspect weightings were assigned 'Multipliers', which are listed in Table 7. A total weighted score for each concept was obtained by summing the product of the Coarse Rank Scores and Aspect Multipliers over all the aspects.

Table 6: Coarse Ranks for Impact of Design Feature on Safety

Coarse Rank	Score	Implication for Inherent Safety
++	5	Significant benefit / highly inherently safe
+	4	Marginal benefit
+/-	3	There are pros and cons
-	2	Marginal degradation – improve the design
--	1	Significant degradation – change the design / very poor inherent safety

Table 7: Coarse Ranks for Impact of Design Feature on Safety

Weighting	Explanation	Multiplier
High	High Impact AND High Frequency	5
Medium	High Impact OR High Frequency but not both	3
Low	Low Impact AND Low Frequency	1

If the IS of a concept could be improved without fundamentally changing it (or arriving at one of the other concepts under review) then the further measures were described under a Possible Improvement (PI) column in the workshop worksheet and the resulting new score (absolute, not relative) was determined.

It is emphasised that this scoring system is both coarse and somewhat subjective. It is an attempt to quantify the feeling of the workshop regarding different aspects of the design while taking into account the importance of such design features for IS. While it would be possible to expand such a system to incorporate a company's full risk matrix, this is considered undesirable and is likely to lead to an impression of false precision in the results. Concept alternatives cannot be conclusively ordered based on small differences in overall score for each design. However, in use, this system has illustrated clear divides between concepts considered broadly acceptable from an ISrD perspective and those which have more undesirable aspects.

The concept with a new LQ on a relatively benign utilities and water injection platform was selected as the inherently safest. Key aspects in this selection were:

- The number of Persons On Board (POB);
- Diversity of escape routes, muster areas and evacuation means;
- Supply vessel access;
- Complexity of subsea infrastructure, for example flowline crossings;
- Number and complexity of lifts using a heavy lift vessel;
- Platform crane location near to flowlines; and
- Purpose built versus extended control room.

Define

The purpose of the project Define activities is to develop further, define and document the business case based on the selected concept to such a level that final project sanctioning can take place, the applications to the authorities can be submitted and the FEED made, which establishes the basis for detail engineering.

The aims of the Define ISrD workshop are to:

- Record existing ISr features of the design;
- Generate ideas for making the design ISr;
- Contribute to a robust justification for the selected concept; and
- Provide the basis for the ALARP demonstration.

The features which have been identified in previous project stages should be entered in the worksheet before this workshop, together with any subsequently identified features.

A fragment of the worksheet for Project 2 is shown in Table 8. The worksheet is split into sections (by the green dividers), such as *Field configuration* and the main disciplines, which are considered in turn. The *Existing Features* can be positive or negative for safety. *Key* is the key word which best describes the feature; it is not vitally important to record this attribute of a feature but it is useful for classification and later analysis. The *Rank*s, which are listed in Table 6, express the consensus of the meeting about the contribution to IS (or not) of the feature.

If the IS of the facility could be improved, then the further measures are described under *Possible Improvement (PI)*, are categorised by *Key* (word) and the resulting new *Rank* relative to the existing design is determined. Where a possible improvement exists but is not deemed feasible, a *Justification for keeping current (J)* is provided. The *Action* that must be taken to make the improvement and who should do it, the *Actionee*, are decided by the workshop team.

Sufficient time must be allowed to review the pre-populated items in the worksheet, follow up any ideas that are generated from these items and brainstorm further ISr improvements.

During the Define stage of Project 2, two workshops were held; the second reviewed the design as updated after the first workshop and made further recommendations.

After the Workshops

The workshop actions should be entered into the project action management system and the findings communicated to the project; the coarse ranks may be used for prioritisation. Any fundamental changes to the design will require significant effort to implement and so there might be push-back after the workshop. The project safety lead and workshop facilitator must ensure that design changes are made, or else very good reasons are provided for non-implementation, which will satisfy the regulator and leave the residual risk ALARP.

An ISrD register should be instigated after the workshop to record the existing and possible ISrD features, why they are ISr, necessary actions and justifications for not implementing certain measures. This is a ‘living’ document that will be added to and updated throughout the design, not just in workshops.

Eventually the ISrD findings must be transposed into the ALARP process and the ISrD register becomes the starting point for the ALARP register.

Future Work

We see four main areas for further work. The first is to develop better tools for ISrD analysis. Better methods for evaluating designs for IS are needed, for which three pieces of information are required.

The **number of people at risk** on the proposed development – we are working on a concept POB estimator, which will provide approximate numbers of people located in the areas of a facility, over the field life and taking into account reservoir depletion and asset ageing.

The **Major Accident Scenarios (MAS)** for the proposed development – these should be based on what has happened in the past (and can therefore happen again) for similar facilities, as well as postulated high consequence events.

Table 8. Inherently Safer Design Workshop - Define

Key Words: ELIminate / REDuce Hazards :: SIMple / RELiable Plant :: SEParate / PROtect People ESCape									
No	Area	Existing Inherently (/Less) Safer Feature	Key	Rank	Possible Improvement (PI)/ Justification for keeping current (J)	Key	Rank	Action	Actionee
Field Configuration									
1	PB	Accommodation on bridge-linked platform with largely benign processing remote from hydrocarbon production / processing on PA / WA and future PC.	SEP	++	Consolidate existing (WA) accommodation with new, all on PB	SEP	++	Granherne have produced a TN demonstrating the costs of extending to 199 POB. Client to produce a decision paper for the optimum accommodation	ANO
2		Bridge landings on top of decks, require steps		-	PI: Make bridge landings flush BUT: Additional support structure required - additional fabrication and construction risks and possibly non-direct evacuation route, if a dogleg is required.	ELI	+	Remove steps from bridge links.	AKA
3		Dual helidecks.	ESC	+	J: Redundancy & diverse evacuation & reduced POB transit through process areas but increased logistical complexity.			No action	
4	PA	Both PA bridge landings can be affected by the same MAH events.		+/-	J: Bridge landing dictated by PB location (technical justification in preparation). This means that repositioning is not possible. No different from current setup. PI: Improve evacuation provisions (escape chute / rafts) on PA.	ESC	+	Review evacuation provisions on PA	XYZ

The combination of these two pieces of information provides the potential worst loss of life for the installation. The maximum monetary loss, due to loss or damage to asset and production interruption, could also be estimated. Quantification of reputational damage should also be attempted.

The Likelihood of the MASs should be estimated based upon statistical data for past incidents. The combination of the estimates for: the potential loss of life, likelihoods and the life of the installation provides an idea of the risk of catastrophe.

The above estimates for the alternative concepts could be presented to the ISrD workshops for discussion and to stimulate further debate about the relative IS of the concepts.

The workshop processes need further development, for example in use of checklists and provision of guidewords to participants, which may be too prescriptive, versus allowing ‘space’ for brainstorming and lateral thinking.

More promotional work is needed to foster the zero accidents / harm mind-set for design work. Design team leadership must be encouraged to think beyond up-front cost and schedule and to embrace the practicality of removing the possibility of MASs and to set this as a project goal.

In a wider project context, life-cycle costing is essential for demonstrating that ISrD measures are cost effective over the life of a facility.

Conclusions

This paper has described some of the barriers to more widespread adoption of ISrD and how we are overcoming them in Granherne. We have found that it is essential to educate engineers about the benefits of ISrD and to promote ISrD as an attitude of mind. Committed project leadership is also crucial to success.

It is important to recognise that ISrD has most benefit early in the design process and that it is an essential first step in the demonstration of ALARP and the safety risk management process. We have developed practical workshop-based methods that follow the early project stage sequence, for identifying, assessing and recording ISrD features of designs. These methods have provided significant benefits to the projects that have used them.

Maybe one of the reasons for the success of the workshop approach is that design is a social activity and, as Trevor Kletz maintained, people perform much better when they are actively involved with a task.

Piper Alpha was not just a catastrophe for the people who died and their families; it was also a huge production and financial loss. The accident knocked out 10 percent of UK oil and gas production, which was 1 percent of United Kingdom gross domestic product at the time. The total insured loss was $3.6 billion (2013 prices) [Lloyd's, 2013]. Similarly, The Deepwater Horizon incident is still having a huge cost impact on BP. We really cannot afford such accidents – let us strive to make them impossible by ISrD.

To this end, we are currently working on methods for evaluating IS which use the offshore installation POB, MASs potential number of fatalities and likelihoods.

References

Ahmad, S.I., Hashim, H and Hassim, M.H., September 2014, Numerical Descriptive Inherent Safety Technique (NuDIST) for inherent safety assessment in petrochemical industry, *Process Safety and Environmental Protection*, **92**, 379-389.

BP, 5 June 2008, Inherently Safer Design (ISD), GP 48-04.

CCPS (Center for Chemical Process Safety), 2009, Inherently Safer Chemical Processes – A Life Cycle Approach, 2nd edition, Wiley.

CSB (U. S. Chemical Safety and Hazard Investigation Board), October 2014, Regulatory Report: Chevron Richmond Refinery Pipe Rupture and Fire, 2012-03-I-CA, U. S. Chemical Safety and Hazard Investigation Board.

Dalzell, G. A., 2004, Inherently Safer Design; Changing Attitudes and Relationships, *Seventh SPE International Conference on Health, Safety, and Environment in Oil and Gas Exploration and Production*, Calgary, 29–31 March 2004, Society of Petroleum Engineers.

Edwards, D.W. and D. Lawrence, 1993, Assessing the inherent safety of chemical process routes: is there a relation between plant costs and inherent safety?, *Trans Instn Chem. Engrs B*, **71**, 252-258.

Edwards, David W., December 2014, Export inherent safety – not risk, *The Loss Prevention Bulletin*, **240**, pp 21-24, IChemE.

Ellis, Graeme, December 2014, Are we doing enough to reduce hazards at source?, *The Loss Prevention Bulletin*, **240**, pp 30-31, IChemE.

Energy Institute, 2014, Guidance on applying inherent safety in design: Reducing process safety hazards whilst optimising CAPEX and OPEX, ISBN: 9780852936894, Energy Institute.

EU, 28.6.2013, Directive 2013/30/EU of the European Parliament and of the Council of 12 June 2013 on safety of offshore oil and gas operations and amending Directive 2004/35/EC (Text with EEA relevance), L 178/99, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:178:0066:0106:EN:PDF (accessed November 20th 2014), Official Journal of the European Union.

Gupta, J.P. and Edwards, D.W., 2002, Inherently Safer Design – Present and Future, *Trans Instn Chem. Engrs*, **80**, B: 115-125.

HSE, March 2006, Assessment Principles for Offshore Safety Cases (APOSC), http://www.hse.gov.uk/offshore/aposc190306.pdf (accessed November 20th 2014), HSE.

HSE, 2007, Safety Report Assessment Manual (v2) (SRAM), http://www.hse.gov.uk/comah/sram/index.htm (accessed November 20th 2014), HSE.

ISA, 2 September 2004, Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, Definitions, System Hardware and Software Requirements, ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod), (American National Standard).

Kletz, T. and Amyotte, P., 2010, Process Plants: A Handbook for Inherently Safer Design, 2nd Edition, CRC Press, Taylor & Francis Group, Florida.

Lloyd's, 5th July 2013, Piper Alpha After the Fire
http://www.lloyds.com/news-and-insight/news-and-features/market-news/industry-news-2013/piper-alpha-after-the-fire (accessed15th December 2014)

NCDH (National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling), January 2011, Deep Water The Gulf Oil Disaster and the Future of Offshore Drilling - Report to the President.

SaRS (Safety and Reliability Society), February 2014, Chairman's Remarks: All at sea, *Society - The Safety and Reliability Society Newsletter*, Safety and Reliability Society.

Srinivasan, R and Natarajan, S, 2012, Developments in inherent safety: A review of the progress during 2001-2011 and opportunities ahead, *Process Safety and Environmental Protection*, **90**, 389-403.

Statoil, 01.01.2010, Guidelines for risk and emergency preparedness analysis, GL0282, Final ver. 1.

UK Government, 31st July 1974, Health and Safety at Work etc. Act 1974
http://www.legislation.gov.uk/ukpga/1974/37 (accessed 8th December 2014)