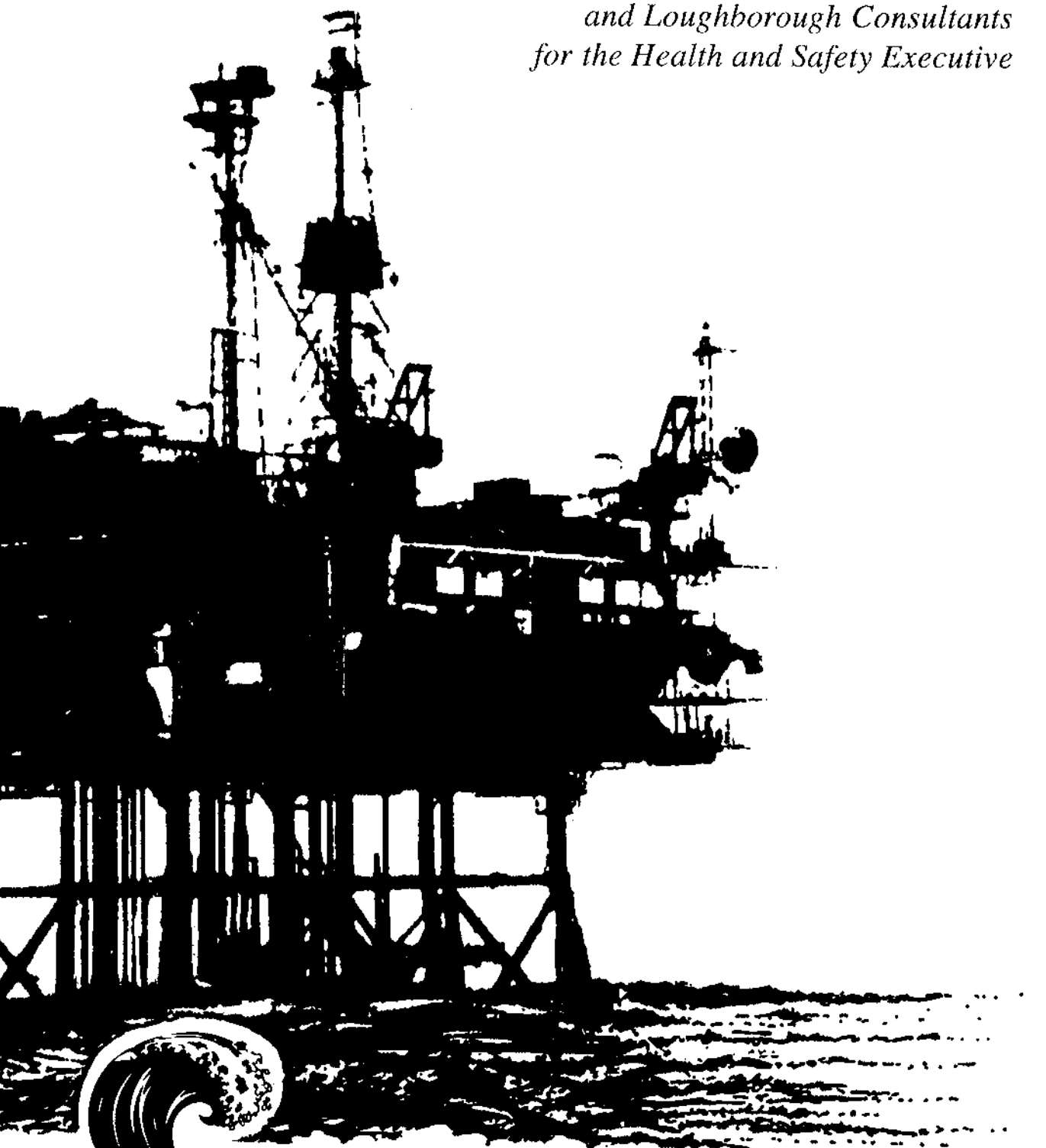
OTH 96 521

HSE
Health & Safety Executive

IMPROVING INHERENT SAFETY

Prepared by AEA Technology plc
and Loughborough Consultants
for the Health and Safety Executive



Offshore Technology Report

Health and Safety Executive

OTH 96 521

IMPROVING INHERENT SAFETY

Authors

D Mansfield
L Poulter

AEA Technology plc
Risley, Warrington
WA3 6AT

T Kletz

Loughborough Consultants Ltd
Loughborough University
Loughborough
Leicestershire
LE11 3TU

HSE BOOKS

Health and Safety Executive - Offshore Technology Report

First published 1996

ISBN 0-7176-1307-0

This report is published by the Health and Safety Executive as part of a series of reports of work which has been supported by funds provided by the Executive. Neither the Executive, or the contractors concerned assume any liability for the report nor do they necessarily reflect the views or policy of the Executive.

Results, including detailed evaluation and, where relevant, recommendations stemming from their research projects are published in the OTH series of reports.

Background information and data arising from these research projects are published in the OTI series of reports.

SUMMARY

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. Unlike these 'add-on' approaches, which add cost and can be maintenance intensive, some applications of inherent safety can lead to enhanced safety and lower capital and operating costs. Two of the key principles of inherent safety, intensification and simplification, are extremely relevant to the economics of offshore installations, and a more systematic use of these principles could further improve safety and reduce costs offshore.

This Pilot Study has been undertaken to assess the extent to which the concept and principles of 'inherent safety' are being applied in the development and design of offshore oil and gas installations on the UKCS. It included reviews of some recent literature and some of the main regulations affecting the design and operation of offshore installations. However the main element of the study was a number of interviews with representatives of some of the leading Design Contractors and Operating companies. Only a small number of people were interviewed from 5 companies, but the findings were sufficiently consistent to give confidence that they reflect the wider view of the UK offshore industry.

The findings show that the term 'inherent safety' is only just beginning to be recognised in the industry, mainly as a result of its inclusion in the Design Safety Case Guidance, and the UKOOA Fire and Explosion Hazard Management Guide. Although many safety professionals would recognise the term, few seem to have a clear view as to its meaning and principles. There appears to be a number of subtle but significant differences of opinion as to what inherent safety is, including 'hazard avoidance', 'hazard prevention', 'risk minimisation', and 'good engineering'. Whilst all of these may form part of an inherently safer strategy, they do not encompass a full understanding of the role of inherent safety. There is therefore a need to raise awareness of the principles of inherent safety, such as those presented in the many papers and books by Trevor Kletz, and perhaps to develop a more detailed definition and set of principles for use in the offshore industry.

Although few designers would be familiar with the term 'inherent safety', many do apply some of its principles such as inventory reduction and simplification, but not always in a systematic way. Further opportunities to reduce inventory, simplify plant, and apply the other inherently safer principles might be identified if these principles were made more visible, and incorporated into systematic hazard studies, design reviews and procedures.

Some of the main drivers in the offshore industry at present, to reduce manning levels and provide minimum facilities installations, encourage the use of compact and simple technology and reduce the need for operators to be present. These objectives are fully compatible with an inherently safer approach to design. Similarly, moves to more flexible and open client-contractor relationships can create the sort of environment that promotes the challenging of past practices and encourages innovation. In this type of environment the ideas of inherent safety can flourish and reap the greatest rewards for both the designer and operator.

Good hazard management depends on a clear understanding of the hazards and their interaction with the design and its operation. If the design is to be optimised to avoid or reduce the hazards of operation this needs to be done early on in the development of the design. However project programmes often do not seem to recognise that the most critical part of any project is at the very start, when all the major decisions are taken about the location and type of installation, and the processes to be adopted. By the time the concept design is finished, most of the installation's build and operational costs will have been fixed, and most of the opportunities to deal with hazards in an inherent way will also have passed.

Companies may spend some time evaluating various options from an economic point of view, but these studies may not address safety as a key parameter. If safety is treated as a simple go/nogo criteria at these early stages of design, many opportunities for an inherently safer, and perhaps cheaper, installation may be lost. Project managers should consider allocating a little more resource and time at the start of the concept design stage to challenge the basis of design and identify and evaluate alternatives that may be inherently safer (and perhaps cheaper).

Overall the design of offshore installations do reflect many applications of inherent safety, but a more systematic and visible use of these principles could lead to even more robust safety performance. Dealing with the hazards at source may also provide the most cost effective route to good safety performance, and the main principles of an inherently safer approach go hand-in-hand with cost reduction. The industry therefore stands to benefit by promoting a greater awareness and application of inherent safety and its principles.

So we would suggest that senior managers and designers in operating and engineering companies in the UK need to be made more aware of the concepts, practicalities and benefits of inherently safer approaches to hazard management. This could be achieved through the usual mechanisms such as publications, workshops, research and guidance. The regulator could also give support and encouragement to this by emphasising further the safety importance of inherently safer approaches in regulations, ACoPs and guidance.

Those who do not wish to read the full report should turn to Section 7.

"A clever man is one who finds ways out of an unpleasant situation into which a wise man would never have got himself"[1]

[1] D A Segre, 'Memoirs of a Fortunate Jew', Grafton Books (Paladin), London, 1988, p117

CONTENTS

1. INTRODUCTION

The concept of inherently safer design was developed by Kletz et al[1] in the late 1970s as a fundamental approach to hazard management which emphasised avoiding or limiting the hazard at source, rather than relying on 'add-on' safety features or management systems and procedures to control them. Although a few examples of inherently safer design can be found in both the onshore and offshore processing industries, the concept has not really been taken up in the same way as HAZOP or Risk Assessment, ideas which were developed about the same time as inherent safety.

The principles of inherent safety have a particular relevance to the offshore oil and gas industry, where hazardous materials and operations are, by necessity, in close proximity to personnel and where there has been a tendency in the past to rely on active safety systems such as emergency shutdown and deluge systems to control the hazards. Recent Regulations and practices developed following the Piper A disaster are now trying to encourage an inherently safer approach, with lower inventories and less reliance on active safety systems which can and do fail. Two of the inherent safety principles, reducing inventories and simplification, also can bring other worthwhile benefits in the offshore context, reducing topside weights and reducing operation and maintenance requirements. These fit well into current drives towards smaller 'minimum facilities' platforms and demanning. So overall, the principles of inherent safety are of increasing relevance to offshore installation design. However it is not clear to what extent the principles of inherent safety are recognised or adopted in the offshore industry, and it may be that they are not being as widely used as they could be. There is therefore a need to assess the level of awareness and use of inherent safety in the industry, and to see how these can be improved.

In 1992, the HSE initiated a study[2] to assess the status of inherent safety in the onshore chemical and process industries. The study, carried out by AEA Technology, highlighted a number of reasons why inherent safety was not being used and suggested ways in which these could be addressed. This pilot study has recently expanded into a high profile CEC co-funded joint industry programme[3] led by AEA Technology to develop tools for process selection and concept plant design. However both these have an onshore industry focus.

The aim of this pilot study was to build on the knowledge gained on the earlier HSE study to address inherent safety within the unique characteristics of the offshore oil and gas industry. The project would seek to raise awareness of the potential benefits, principles and application of inherently safer approaches, and suggest ways in which these could be further promoted.

2. OBJECTIVES AND SCOPE

The objectives of this pilot study were to assess the promotion and use of inherent safety in the offshore industry and to use its findings to raise awareness of the inherently safer concept, its benefits, principles and possible means for its practical application in the UK offshore oil and gas industry. It has concentrated on the role of inherent safety in the design of offshore installations for oil and gas production, as this is the area where it is considered that the concept can have most impact in improving safety. The study primarily addressed the role of inherent safety in process design and installation layout, but also considered aspects of structural design and integrity where a more visible recognition and application of the concepts of an inherently safer approach might be encouraged.

The project tasks included:

- A Review of Regulations and Codes of Practice

  A representative selection of current and developing UK regulations and codes for offshore design were reviewed to determine the extent to which these recognise and promote an inherently safer approach.

- A Review of Literature

  Some of the recent main literature on offshore technology was reviewed to identify advances in technology, design approaches, conflicts and issues that could influence the adoption of inherently safer designs.

- A Review of Current Design Approaches

  A number of operators and design contractors were interviewed to determine the overall industry approach to installation design, and how safety is integrated into this, with a particular emphasis on how inherent safety can or does feature in this. Current pressures or trends influencing the way safety is addressed in design were also identified.

- Assessment, Summary and Reporting

  An assessment and overview of the situation has been made, drawing conclusions on the status of inherently safer approaches offshore and suggesting ways in which such approaches can be further encouraged and implemented.

The findings of the study are to be widely disseminated through this report, and through appropriate articles and a conference paper.

This report is structured to reflect the tasks carried out. Section 3 provides a background to the subject, giving an overview of the inherently safer concept and how this relates to the offshore installation design. Sections 4 and 5 present and discuss the findings of the regulations and literature reviews respectively. These sections predominantly deal with inherently safer aspects of the processing of hydrocarbon and layout of the topsides equipment, aspects which could be considered well developed in terms of inherently safer understanding. The structures supporting these topsides are equally important for safety, and Section 6 pulls together aspects of structural design and sets these in an inherently safer context . Section 7 highlights the findings of the discussions with some key people involved in offshore installation design. Finally Section 8 summarises the findings of the study and suggests a number of ways in which inherently safer design approaches could be further promoted in the offshore industry, including the use of an inherently safer based hazard management approach such as that outlined in Appendix 1.

3. INHERENTLY SAFER DESIGN

3.1 APPROACHES TO HAZARD MANAGEMENT

Hazard management approaches are often described as being based on three main principles: prevention, control and mitigation. Prevention relates to measures taken to eliminate or reduce the hazard at source, or to reduce the likelihood of it being realised. Control measures are those taken to keep the hazard within the design envelope, either by containment or control systems, or to actively react to events that could result in an accident. Mitigation measures are those intended to deal with the hazard once the accident has occurred, either to bring the hazard back under control or to limit its effects.

Typical control and mitigation systems such as overpressure relief systems, emergency isolation systems, fire water systems and blast walls are often the most visible, and expensive, side of hazard management. These can be said to represent an 'add-on' systems approach to hazard management. The very visibility of these systems can lead to designs where the safety focus is on the control and mitigation measures, and little attention is paid to prevention or trying to reduce the hazards at source. This may mean that more subtle but very cost effective ways of eliminating or reducing hazards may be being missed. The concept of inherent safety may provide a means to turn the attention of designers towards elimination and reduction, and this in turn could lead to a better integrated combination of prevention, control and mitigation measures.

3.2 INHERENTLY SAFER CONCEPT

Inherently safer plant uses basic design measures to achieve hazard elimination, prevention and reduction. The classic definition of an inherently safe plant or activity is one that cannot under any circumstances cause harm to people or the environment. This may be because:

- it only uses materials that are harmless;
- it has such small inventories of hazardous material that these are insufficient to cause significant harm even if released;
- the hazardous materials are held in a form or under conditions that render them effectively harmless (diluted, at ambient temperatures and pressures).

The same principles could be applied to hazardous equipment, in that inherently safe equipment would not involve high energy systems such as pressure, vacuum, or high speed rotation.

In practice such an ideal plant or process rarely exists, and it is often the very reactive nature of materials that makes them so useful to us for our energy and manufacturing. It is therefore more helpful to think in terms of inherently safer plant or processes, that is those that by comparison involve less inherent hazard.

It is also recognised[4] that reducing the complexity of the plant design and operation can make accidents less likely, resulting in a friendlier plant as there is less equipment to go wrong and less opportunities for human error. This is sometimes considered to be a part of a wider definition of inherently safer[2].

The main thrust behind these approaches is to help designers strike a better balance between hazard avoidance, prevention, control and mitigation, and to encourage the use of basic design features to achieve this rather than over reliance on 'add-on' active and passive systems, such as ESD systems and fire walls, that can and do fail. The relationship between these approaches can be seen in the overall framework for hazard management in design presented in Figure 1. The objective of good design should be to manage the hazards by means towards the upper left hand side of the table, rather than those in the bottom right.

Figure 1
A Framework for Hazard Management in Design

Principle	Inherent Design Measures	Add-on Passive Measures	Add-on Active Measures	Procedural Measures
Avoidance	Design to remove need for hazardous material, condition, equipment or activity (eg remove need for second separation train or avoid need for offshore separation by use of multiphase pump, or remove need for maintenance - a hazardous activity) Design the basic process so hazard cannot arise (eg design process so thermal runaway cannot occur, or design heater so it cannot overheat the process fluids)			
Prevention	Design features to make hazard less likely to occur/to be realised (eg simpler plant, fewer leak points, good ergonomics)	Measures to prevent or reduce likelihood of hazard being realised which do not require initiation (eg all welded pipework, locate pipelines away from main 'dropped object' zone)	Measures to prevent or reduce likelihood of the hazard being realised and which require initiation (eg process pressure, speed and temperature control systems)	Manual measures to prevent or reduce likelihood of the hazard being realised (eg inspection, maintenance, permit-to-work system, direct manual control of plant)

Figure 1
A Framework for Hazard Management in Design

Principle	Inherent Design Measures	Add-on Passive Measures	Add-on Active Measures	Procedural Measures
Control	Design to fully contain hazard within design envelope (eg design for maximum pressure) Design process to be self limiting (eg limit heat transfer capacity or temperature of heating medium to slow down thermal runaway) Design process so deviations/errors are obvious/easy to detect and remedy	Measures to control the severity of the hazard or stop the chain of events before it becomes an accident which do not require initiation (eg flow restriction orifices, good natural ventilation, use of non-sparking electrical equipment)	Measures to control the severity of the hazard or stop the chain of events before it becomes an accident which require initiation (eg feed isolation systems; high pressure, temperature and level trips, pressure relief valves)	Manual measures to control the severity of the hazard or stop the chain of events before it becomes an accident, (eg manually initiated blowdown or isolation)
Mitigation	Design to limit or reduce magnitude of hazard if realised (eg reduce inventory, reduce pressure, use a less hazardous material) Design to limit/reduce effects of hazard if realised (eg good layout, segregation, natural ventilation)	Measures to limit the magnitude or effects of a hazard once realised (ie as an accident) which do not require initiation (eg fire and blast walls, structural fire protective coatings)	Measures to limit the magnitude or effects of a hazard once realised (ie as an accident) which require initiation (eg fire water deluge, water mists for explosion suppression)	Manual measures to limit the magnitude or effects of a hazard once realised (ie as an accident) (eg manual fire fighting)

3.3 POTENTIAL APPLICATION OFFSHORE

The main hazards on Offshore installations are the process fluids and processing operations, the sea environment and the process links between the reservoir and other installations. A recent study by the HSE[5] shows that process and structural failure incidents account for almost 70 % of the risk to personnel offshore. The contributions to risk found in the study are presented in Figure 2.

Figure 2
% Predicted Fatality Rate by Major Hazards - by Hazard Source

Process	38.8
Blowout	2.0
Riser/Pipeline	1.6
Structural - Mobile Installation	23.0
Structural - Fixed Installation	1.7
Collision	11.2
Helicopters	21.8

There is little that can be done to eliminate or reduce the environmental hazards, except building the installation onshore or on an artificial island and using horizontal drilling to reach the reservoir. However some structural designs may be inherently more stable or resistant to environmental conditions or more able to withstand damage, and could therefore be seen as inherently safer.

Connections to the reservoir and pipelines are also fundamental requirements, but perhaps these can use transport systems that allow better isolation or flow control (eg multiphase pumps, simpler subsea/downhole isolation and flow restriction systems).

Good opportunities for applying inherently safer design exist in the processing of the reservoir fluids. In the extreme it may be possible in the future to avoid processing offshore completely, using subsea multiphase pumping systems to bring the fluids to the beach where they can be processed at a terminal. Onshore processing and gas compression should be far more inherently safer that offshore processing, since separation distances can be used to keep people well away from the effects of hazards, and the main offshore structural risks are eliminated. In the meantime advances in technology and careful specification of equipment and layout can help reduce the inventories of hazardous materials on the installation and protect people from the effects of the hazards.

The main sources of major hazard in offshore processing are the inventories of flammable materials in the risers (and in associated pipelines or the reservoir), slug catchers, separators, contactors, and heat exchangers, and the high pressures and inertia in high speed rotating equipment such as turbines, compressors, export pumps, and reinjection pumps. These then should be the main targets for inherently safer approaches.

Figure 3 Typical Main Sources of Platform Hydrocarbon Inventories - % of total inventory	
Oil and Gas Production Platform	
Separation	45
Oil Coalescer	38
Oil Export	6
Compression	5
Gas Production Platform	
Slug Catcher	37
Separation	26
Compression	18
Other Sources of Inventory	
Risers	Varies - but could be as high as 'on platform' inventory. Gas risers usually in tonne quantities, oil risers in 100 tonne quantities.
Glycol for gas drying	In tonne to 10 tonne quantities
Methanol for hydrate control	In tonne to 10 tonne quantities
Diesel fuel	In 10 to 100 tonne quantities
Note - Above data taken from various confidential sources and is for illustrative purposes only.	

With many safety improvements, there is some trade off required between the costs of the improvement and the risk benefit it brings. This is often because the safety improvement is an 'add-on' measure which only serves a safety function, and adds little, if anything, to the effectiveness of the process or strength of the structure. The cost of such a system can therefore only be justified if it brings about a worthwhile improvement in safety.

However if the safety function can be achieved by some integral part of the process or structure, then the cost of this is 'shared', and any improvement could bring other benefits as well as those for safety. This idea of integrating the safety function into the basic plant design is what inherent safety is all about.

Some inherent safety approaches can bring a win-win situation where safety enhancements are achieved as well as cost savings or improvements in process/structural performance. For example the elimination of, or reduction in size of, equipment, can lead to the use of simpler, smaller, more compact equipment which offers the promise of reduced hazard and risks, reduced weight and space requirements and less maintenance. In this way an inherently safer approach to design can provide the most cost-effective route to safety.

Given the cost implications of weight, space, and maintenance offshore, inherently safer designs may be of more value to the offshore industry than to the onshore chemical and process sectors.

Also, there are often conflicting requirements of the design, so an improvement in one aspect may be at the expense of performance in another. This applies to different aspects of safety eg containment vs. natural ventilation for gas leak and explosion overpressure relief, as well as between safety and production for example.

Adopting an inherent approach to safety perhaps offers the best chance to eliminate or find the best compromises to these conflicts, by addressing the problems in the fundamental design.

4. REVIEW OF REGULATIONS AND OTHER CODES AND GUIDANCE

4.1 ROLE OF REGULATION AND GUIDANCE

UK regulation and guidance, together with industry developed codes and guidance has always played a key role in the way safety is managed in the offshore industry. The principles and implementation of these has often shaped the approach to safety in design, as designers strive to meet he requirements set down.

Following the Cullen Report into the Piper Alpha disaster[6] industry and the regulator have made fundamental changes to the approaches to managing safety. The older prescriptive safety regime is being replaced by a 'goal-setting' regime with clearer attention on dealing effectively with the specific hazards on any installation. These changes are being reflected in the new regulations and guidance being issued or developed.

As part of this study a review was carried out of some of the key regulations, codes and guidance in place or being developed, to assess the extent to which these acknowledge, promote or hinder the search for and adoption of inherently safer designs.

4.2 MAIN UK OFFSHORE REGULATIONS

The main regulations put in place following the Cullen Report are the Offshore Installations Safety Case Regulations[7]. These set out a risk based goal setting regime for safety which uses hazard identification and assessment to set reasonable practicable means of prevention, control and mitigation. Inherent safety approaches can fit in well with such risk based regimes, providing a key means of hazard management.

These regulations include a specific requirement to prepare a design safety case at the early stages of the design (so any comments, or substantial changes can be incorporated without undue cost/programme penalties). The **guidance** with this emphasises the role of inherent safety and asks for a demonstration of how the concepts of inherent safety have been applied including:

> *...From [7], p29, section 5..*
>
> *a) substitution of hazardous materials for less hazardous ones;*
>
> *b) avoiding undue complexity in the design;*
>
> *c) allowance for human factors, for example fail-safe designs, or control systems that reduce the risk of human error;*
>
> *d) minimising risks from hydrocarbon inventories, by keeping inventories as low as possible, and by segregating inventories, and by fitting fire protection and isolation valves;*
>
> *e) selection of construction materials; and*
>
> *f) the design of vessels and pipelines to minimise the effects of sources of deterioration (eg erosion), to reduce stress concentrations, and to facilitate inspection after construction and during operation.*
>
> Note - the last part of d) is 'add-on' safety and not 'inherent' safety

The role of inherent safety is also stressed in the UKOOA Guidelines on Fire and Explosion Hazard Management[8] which devotes an entire chapter to inherent safety and hazard prevention. The guide explicitly states a preference for prevention rather than control and mitigation, but recognises that in practice an integrated approach combining prevention, control and mitigation is needed to give defence in depth against hazards which cannot be avoided. It also notes that inherent safety aspects needs to be considered early in the design process when major changes can be made without compromising construction schedules and cost commitments. The document gives some good practical advice on the application of inherently safer approaches to offshore installation design hazard management including the themes of hazard avoidance, inventory reduction, substitution, use of lower pressures and temperatures, simplification and segregation.

The PFEER Regulation and ACoP[9] also stress the role of prevention in managing risks. 'Inherent safety' is mentioned briefly, as are the principles of hazard avoidance, combating at source and adapting work to suit the individual, all of which could be considered as part of an inherently safer approach. However the regulations and ACoP could have given inherent safety a higher profile and supporting information could have included references to the concept, its principles or how it could be applied in practice.

Drafts of the proposed new ISO standards on HSE Management Systems[10], Evaluation and Risk Management[11] and Control and Mitigation of fires and Explosions on Offshore Installations[12] also refer to inherent safety in the context of a risk based, goal setting approach to hazard management. The Evaluation and Risk Management draft in particular is likely to contain a detailed section on inherent safety and its application to offshore installation design.

4.3 STRUCTURAL REGULATIONS

Structural design and the role of existing regulations and codes are discussed in Section 6. This short section simply offers some comments on more recent developments. The recently issued consultative document on the Draft Offshore Installations and Wells (Design and Construction, etc) Regulations[13] is primarily concerned with structural design and integrity and the verification of safety critical elements of installations and wells, but places an emphasis on ensuring integrity at all times and in having an adequate design which is operated within set design limits. Inherent safety is briefly mentioned in the Guidance (p98) as part of an overall risk management strategy, but there is no attempt to explain what is meant by 'inherent safety' or how it could be applied to structural design. There may be some difficulty in applying the process based 'inherently safer' principles to structural/mechanical issues. It is also worth noting that both the Machinery Directive[14] and CDM Regulations[15] refer to avoiding, eliminating and combating risks at source by good (structural/mechanical) design as the preferred strategy for hazard management.

4.4 OLDER CODES AND GUIDANCE

Perhaps not surprisingly some of the older codes and guidance take a more prescriptive approach to hazard management. API RP 14 C[16] is still widely used to specify instrumentation and safety system requirements for pressure vessels etc, and although the safety assessment principles it sets out do ensure the hazards are identified, it can lead designers to rely entirely on add-on safety systems to control and mitigate these, rather than look for inherently safer alternatives.

It is also interesting to note that API RP 500 on Electrical Area Classification[17] uses a risk based approach for assessing the likelihood of flammable mixtures being present. However this is based on fugitive emissions only, and the code clearly states that it is not intended to address accidental releases. This therefore needs to be considered in the installation design, and the assessment of accidental releases may mean that more stringent requirements or extended areas over and above that for RP 500 may need to be specified where large accidental releases are likely.

4.5 CONCLUSIONS

Recently issued regulations, ACoPs and guidance from both industry and the regulator promote a risk based approach to managing safety which facilitates the use of inherently safer designs as part of hazard management, even though they may make only limited mention of inherent safety or its principles. While some of the regulations and guidance do mention the term 'inherent safety', few attempt to outline the principles of inherent safety or its potential benefits, or say how it can be applied in practice. This is essential if readers are to have a clear understanding of what inherent safety is and how to implement it. The regulations and guidance also need to recognise that the best time to consider inherent safety is at the very early stages of concept design when widely different options can be considered and major changes introduced with minimal schedule and cost implications.

Some of the older design codes are more prescriptive in nature and may hinder the designer in identifying and adopting inherently safer alternatives as part of an overall integrated approach to hazard management.

Whilst 'inherent safety' is widely promoted for process safety, this terminology is not generally applied to issues of structural integrity and design. It is not clear how the principles of inherent safety used for process system could relate to structural design integrity, or what other principles could be defined as structural inherent safety.

5. REVIEW OF LITERATURE

5.1 SCOPE OF REVIEW

A review of a recent published literature and a selected number of journals for the offshore industry has been carried out as part of the study to identify any trends in technology or other economic developments and initiatives that could be relevant to inherent safety.

The review included a selection of recent copies of Oil and Gas Technology[19], the Oil and Gas Journal[20], The Chemical Engineer[21] and Offshore Engineering[22]. A keyword search was also carried out on a large international literature databank.

The databank review was not particularly useful, bringing up many abstracts that were of little or no use, and few that were of any real use. This reflects the difficulty is selecting suitable keywords when searching for offshore inherent design examples and issues, a problem found in other studies on inherent safety[18]. A manual search of the magazines was far more fruitful and identified a number of relevant and interesting articles. These tended to fall into a number of discrete topic areas: compact separation; compact heat transfer; multiphase metering and pumping and subsea/satellite installations. These are discussed in more detail in the following sections.

5.2 COMPACT SEPARATION

In recent years static hydrocyclones have become an accepted technology for the treatment of oily water[21a]. These devices can reduce inventories, and space and weight requirements by an order of magnitude compared to conventional technologies. They are also very simple devices, more like a length of pipe than a separator, they need little maintenance and are also far less prone to leaks than older style flotation units.

Hydrocyclone technology and the power fluidics science it is based on is also finding other applications for separation. BP[21b] has carried out trials successfully using hydrocyclones for well fluid dewatering. This included the use of rotary as well as static hydrocyclones, giving even higher separation and effective 'g'. The technology was said to cut residence times from minutes to seconds. The article notes that centrifuges potentially offer the best separation performance per unit volume, but that concerns over the maintenance requirements of the seal and high speed rotating equipment are drawbacks. Alfa Laval are reported to have developed a disk stacked centrifuge that can be use to separate oil from water or vice versa, it is intended to replace existing coalescers for oily water treatment and recovery[22a].

Power fluidics is also been used to develop a vortex choke valve[22b] for flow control, that should reduce erosion and corrosion problems at chokes, and reduce maintenance requirements. The design, which requires no seal or gland for the main well stream flow, is said to last 5 times longer than a conventional choke valve.

Although power fluidics are currently being used mainly for oily water treatment it is possible that the technology could find wider application offshore for main stream separation, sand and solids separation, and glycol contacting, offering size and inventory reductions to about 1/5 that of conventional equipment[21c]. The technology has already been used to develop a 'static centrifuge' for sand separation from well streams[22c].

Power fluidic technology may in the future provide simple and compact equipment for most separation and contacting duties including slug handling, primary separation and glycol contacting.

It may also be possible to achieve further intensification by combining unit operations. Many fluidic devices can generate intense mixing, providing the basis for good heat transfer. Perhaps in the future heat exchangers could be located within or around separators or contactors. In fact the combining of unit operations / functions is a classic route to intensification, and one that should be given serious consideration in process development design.

5.3 COMPACT HEAT TRANSFER

In recent years compact heat exchangers, especially Plate-Fin heat exchangers (PFHEs), have been specified for offshore duty[21d][21e]. These are an order of magnitude smaller and lighter that conventional shell and tube designs, and hence have lower process inventories, however they are prone to fouling and are not as robust. 'Printed Circuit' heat exchangers (PCHEs) are an alternative compact design that has been used for compressor after-cooling, and is said to offer a five fold reduction in size and weight[22d]. The space and weight saving of the PCHE also led to a cost saving of £0.75 M compared to a conventional upgrade.

Other developments have tried to improve the design of conventional shell and tube units, and a Norwegian company claims to have developed a spiral baffle system which can enhance shell side performance leading to 25% weight and size savings[22e].

5.4 MULTIPHASE METERING AND PUMPING

Multiphase metering and pumping are two developing technologies that in combination could significantly change the way oil and gas reserves are developed. Multiphase pumping and metering offer the prospect of being able to transfer well fluids from a satellite or subsea completion to a central complex some distance away, or even to an onshore facility[21f][21g]. This could eliminate or greatly reduce the need for offshore processing. Multiphase metering would allow fiscal requirements for metering to be met without having to have segregated separation trains for each reservoir. In practice this would allow produced fluids to be metered locally, so they could then be combined with flows from other wells to share pipelines and processing infrastructure.

The technological challenges of multiphase pumping and metering[21h] are considerable, but the potential advantages from a safety and economic point of view are substantial. Several companies have developed small remote multiphase pumping stations which are capable of transferring some fluids short distances, say between a subsea completion and a nearby central complex[19a][21f][21g], and a number of multiphase metering systems are under development[20a][21i].

One approach that has been proposed to ease the problems of dealing with multiphase pumping is to use stabilised oil from the central complex to act as a stabiliser for well fluids, and to provide some extra motive power by introducing this oil at pressure via an ejector at the subsea wellhead. The stabilised oil mixes with and dilutes the live well stream condensing any volatiles[21j].

All these subsea technologies make use of simple pumping systems and non intrusive metering equipment due to the need for high reliability and minimal maintenance requirements. The equipment used is often very compact and such technology could also be used on unmanned surface installations, so called 'subsea technology on a stick'[20b].

5.5 SUBSEA AND SATELLITE INSTALLATIONS

One of the most significant safety advances in recent times has been that of remote operated underwater vehicles (ROVs). These have eliminated the need for diving for many inspection and maintenance tasks. The complexity and capability of these vehicles continues to increase[19b], and one day may eliminate the need for diving completely. ROVs are also being developed to carry out the hazardous tasks of platform and subsea facility decommissioning[19c], reducing or eliminating the need to expose personnel to these hazards.

Structural integrity is a key issue for installation design and operation, and is particularly important for floating installations. Confidence in the structures is achieved by a combination of design and in-service inspection. A recent study of a semi-submersible showed that designing the structure for easy inspection can result in lower lifetime costs, with the design enhancements costing around one tenth the predicted savings in inspection costs[19d]. Designing for easy inspection could be considered as an inherently safer approach in terms of simplicity and ease of operation, making faults easier to detect and making the inspection activity itself safer. Inspectability is discussed further in Section 6.

The current trends for marginal offshore developments are for simpler concepts, re-usable equipment and less maintenance: unmanned installations; subsea installations/satellites; floating production systems. AMOCO are developing a simple monotower structure for some of their new smaller developments, these will use wind turbines to cut diesel fuel costs and reduce the visits to the installation to maintain the diesel generators. Kvaerner are also developing a monotower satellite which uses subsea technology to reduce the need for maintenance - so called 'subsea technology on a stick'[20b]. These approaches aim to minimise operation and maintenance requirements and reduce risks by removing people from the installations. The use of wind turbines for electricity generation is also an example of inherently environmentally friendly technology and should lead to less frequent visits to the platform to replenish diesel stocks or maintain the diesel generators, especially as the technology becomes more reliable. Perhaps wave powered generators could be developed in the future, eliminating the need for diesel generators.

There are also several moves to standardise/ modularise equipment to reduce design costs, enable quicker lead times, make it cheaper to buy and make it reusable. Even the idea of 'off the shelf' platforms has been suggested[20b]. This could have a negative impact on inherent safety if it slowed down technology advances or led to plant being used that was not ideally suited to its duty (eg. separator larger than actually needed). In practice the benefits mean that technology will still push ahead, and the use of standard equipment may have some ergonomic safety advantages. The need for the 'standard' equipment to work in a wide range of operating conditions may also mean some element of overdesign may be present or a better safety margin has been provided in many applications.

5.6 OTHER EXAMPLES

One region of the US EPA has adopted a radically different approach to setting discharge consents which can lead to significant reductions in the toxic wastes from drilling mud operations[20c]. The discharge consent is based on an assessment of the proposed drill programme so that effluents are minimised. The drill programme is reviewed to see if safer alternative muds/additives can be used, or lower amounts used. The discharge consent is then based on the quantity and type of materials to be used and the measures to manage these.

This contrasts with the conventional approach where the EPA only look at discharges that could exceed the 30,000 ppm permissible limit, typifying an 'end of pipe' control-based regime rather than 'effluent minimisation'. This is a good example of how an inherently safer approach to reducing the hazards at source can minimise the risks far more effectively than the simple application of 'limit' controls, which can divert attention away from other areas where improvements can be cost effectively achieved.

Careful consideration of process design options can also help identify inherently safer alternatives which also offer production and cost benefits. A study of a compressor system for offshore gas re-injection compared several alternative options using a simulation programme[20d]. This showed that how a simpler system gave the best safety and process performance. The optimum design combined the interstage cooler and recycle coolers for stages 1 and 2 in the same unit, and also led to a reduction in the number of valves needed for recycle and surge control. This provides an example of how careful consideration of design alternatives can lead to inherently simpler and safer plant. The design eliminated the need for several valves and reduced the number of coolers from 3 to 1, and probably reduced capital and operating costs accordingly.

5.7 CONCLUSIONS

Some of the main trends in offshore production are towards greater use of subsea and remote operated unmanned facilities. These may be considered inherently safer by virtue that people are not exposed to the hazards they present. Much of the equipment being developed for these minimum facilities is based on power fluidics technology, which offers the prospect of lower inventories and reduced maintenance as well as space and weight savings and this type of equipment is perhaps the best example of classic inherent safety. In the future subsea multiphase metering and pumping may eliminate the need for any significant processes offshore. This, together with ROV inspection, maintenance and repair of subsea systems (practically eliminating the need for diving), could lead to an era where the risks to personnel are negligible.

In the meantime advances in heat exchangers and separation technology should allow the reduction of inventories of hazardous materials, and offer more choices for optimised layouts to make the installations inherently safer. There are also opportunities to optimise the processes themselves, removing the need for some unit operations and reducing the number of flanges, valves, instruments and other items which are potential leak sites and which require maintenance.

Further inherent safety improvements may also be achieved simply by careful setting of safety goals, standards and philosophies so that designers are urged to seek way of minimising hazards at source wherever reasonably practicable, rather than stopping at some arbitrary level of design safety judged to be adequate.

6. STRUCTURAL CONSIDERATIONS

6.1 INTRODUCTION

The principles of inherent safety are most widely used in the context of chemical plant design e.g. by using processes that minimise the inventory of flammable materials. In this section we comment on the applicability of inherent safety principles to the design of structures, but note that much of what is said is relevant to other mechanical systems where continued integrity is important, such as pressure circuits, vessels and pipelines.

Failures of structures are at the very least conceivable events; an oil platform can collapse, such as the Alexander Keilland did through fatigue, and pressure vessels have failed when under load. In many cases the ultimate inherently safe feature is impractical, eg the building of structures that cannot collapse. To consider applications of inherent safety principles it may be necessary to identify aspects where either failure can be prevented, or where serious consequences of that failure can be avoided or reduced by the fundamental design of the structure. For example the overall structure can be designed to retain its function and integrity even if some local elements of the structure fail. Such an approach is commonly used in the design of offshore structures.

A well as highlighting the ways in which inherent safety can affect design, this section includes a review of relevant parts of SI 289[23] and the fourth edition of the DEn notes 'Offshore Installations: Guidance on design, construction and certification'[24]. However a consultative document has been issued[13] containing proposals for new regulations and guidance on the integrity of offshore installations that will replace SI 289[2]. The consultative document states that the management of risk involves a hierarchy of control measures. For design these could be considered to be, in order of preference:-

(i) inherently safe design
(ii) control of hazards
(iii) mitigation of hazards
(iv) management controls

The role of inherent safety concepts in design is discussed below.

6.2 INHERENT SAFETY AND STRUCTURAL DESIGN

Design often involves compromise between conflicting requirements. To produce a design that encompasses safety requirements there is a need for a clear assessment and understanding of the risks that the structure could be exposed to, and the risks it could present. This then allows the most effective risk management strategy to be developed. We would argue that design should be performed with the explicit consideration of a set of principles that recognise the need for inherent safety. As an example, for an offshore platform, there is usually a requirement to have a structure able to resist both wave loading and the weakening effects of fire. The use of high strength, low melting point materials is not a desirable solution to the problem of wave action where there is a substantial risk from fire and should be recognised as such.

Other compromises may be needed if risks of different undesirable events acting in combination are possible. For example, choice of surface coatings may affect corrosion rates, but the ability to use the best coating may be determined by the need to minimise the risk of environmental pollution.

---

[2] Note - These new regulations and guidance have now been issued as the Offshore Installations and Wells (Design and Construction, etc) Regulations 1996 (SI 1996/913), HMSO 1996, and guidance published in three parts: L83, L84 and L85 by HSE Books, 1996.

It is necessary to recognise that there may be overriding economic considerations that prevent the applicability of inherent safety principles in all cases. For example, it may sometimes be possible to avoid the use of offshore structures by drilling from onshore using horizontal drilling technology so that hydrocarbons under the sea, but close to land, can be reached. Thus the risk of structural collapse is avoided by not having an offshore structure at all. Other examples of this type of risk avoidance may be possible, such as the construction of artificial islands rather than the erection of structures supported on the sea floor. However such methods are not suitable for applications far from shore in deep waters and are never likely to be economic on the UKCS. Thus fixed or floating structures are used, with potential risks of collapse or sinking.

In some cases the risk of failure for different types of structure can be quantified and used as part of the decision process. Craig[25], for example, discusses the value of higher risk minimum 'structures' as used in marginal fields where the need to adopt more expensive construction methods would mean that the fields were not worth developing.

A robust approach to managing hazards is to ensure that there are several different engineered barriers against that hazard. This concept is sometimes termed 'Defence in Depth'[26]. This is an important aspect of inherent safety for cases where the risk is conceivable, ie a structure can in principle fall down, as opposed to when the risk is inconceivable, ie an explosion can not occur in the absence of certain materials.

6.3 DESIGN CRITERIA

Design, whether it is for a structure, such as an installation jacket, or a pressure circuit, such as a separation vessel, is carried out to ensure that there is sufficient reserve against possible degradation or damage mechanisms. Thus for an offshore structure, where there is likely to be substantial fatigue loading, it is necessary to design an adequate reserve against fatigue. To do this requires knowledge of the likely loading pattern, the material properties and other factors. Depending on how well these parameters are understood it is necessary to build in a degree of conservatism, ie to design the structure to be stronger and longer lasting than it strictly needs be.

Different criteria can be used as part of this design process. Materials properties vary, thus the terms used in fatigue crack growth laws are not known with certainty. It is possible to distinguish between deterministic and probabilistic analysis. In the former case, conservative assumptions are made about properties and loadings; typically material properties two standard deviations away from the mean value are used. By designing with such conservatisms at every stage, it is in effect a demonstration that failure is highly unlikely.

Probabilistic analysis, perhaps making use of the techniques of probabilistic fracture mechanics, does not use lower bound materials properties. Instead, the properties are characterised by a distribution of values intended to represent the real variation. In a full analysis there may be many parameters represented by distributions, such as the materials property fracture toughness, the applied stress, fatigue crack growth law constants etc. It is then possible to perform calculations that will provide a probability of failure for the system. Probabilistic design tools are built into most recent offshore design codes, using techniques such as load and resistance factor design. Thus notional target reliability levels can be achieved. Although such quantitative analysis is most widely used for mechanical fatigue, it can be used where other damage mechanisms exist, such as corrosion.

Whether deterministic or probabilistic methods are used, there is a general imperative to minimise cost by using the available tools to design a structure down to the minimum necessary to ensure that the failure probability is kept below the required level. This could almost be taken as being the opposite of the principle of inherent safety - a principle of 'minimum tolerable safety' might seem to be in place. To avoid this false dichotomy it is necessary to view aspects of inherent safety differently. Instead of regarding inherent safety as in conflict with cost minimisation, it should instead be seen as a desirable set of underlying principles to be used during design.

To incorporate these inherent safety principles it is necessary to consider the design and operation process as a whole, together with the environment in which the structure is expected to operate. Thus although design features that mitigate against the effects of seismic events, such as reinforcement or asymmetric bracing to prevent resonances, might be termed as contributing to inherent safety, they are less relevant if the rig is to be sited in an area that has low seismic activity.

6.4 STRUCTURAL REDUNDANCY

There are several features of structural engineering design that could be said to contribute to inherent safety. The first of these is the provision of a measure of redundancy in a structure. For an offshore steel structure, there may be many elements that could in principle fail. Although in the limit, each of these elements may have had detailed calculations performed on them, there remains the possibility that the calculations were in error or did not represent reality to the extent that a failure does occur. If adequate structural redundancy is present, limited failures of individual elements will not lead to say the collapse of a fixed structure, or cause unacceptable resistance to overturning for mobile installations.

Assessment of structural redundancy is not a trivial issue, it is not simple to calculate whether a structure can survive with missing or damaged elements. So called 'Push over Trials' have been performed on small models to demonstrate strength of structures as calculated by computer codes. These codes are then used to calculate the response of real offshore structures. However validation of the computer codes in this way is both expensive and in some cases has not been totally convincing.

There may be questions to do with the remaining strength of the structure in a severely damaged state and the point at which other safety aspects are compromised. As an example of the latter effect, performance of active safety systems such as fire protection systems may deteriorate as a structure begins to lean. Nevertheless a structure that is redundant in the sense that it can survive with a degree of damage to the individual elements can fairly be termed inherently safer than one which cannot. Similarly, some structures may collapse more slowly than others that are susceptible to sudden failure of tensile loaded elements that have poor fracture properties. The former retain integrity better than others in a given incident situation, and could therefore be considered as inherently safer.

The principle of inherent safety could thus be contained within the rule that if a form of damage could reasonably be foreseen, then a measure of resistance (redundancy) should be provided. This is to ensure a high level of survivability of the overall structure against total failure. Such damage may be progressive, as in the case of fatigue or sudden in the case of fire or explosion. The redundancy should provide an ability to withstand minor failures without overall collapse, and/or to result in a slower or more progressive collapse that gives more scope for evacuation.

6.5 DESIGN FOR INSPECTABILITY

Inspection is a key mechanism to identify possible problems of structural integrity and allow these to be remedied before they pose a serious risk. Although inspection itself is a monitoring activity, and not an 'inherently safe' approach, the way it is carried out and its effectiveness can be improved by designing for inspection. Remote monitoring, eg the use of impact accelerometers, acoustic emission devices or fixed NDT transducers can be used to allow continuous monitoring, where that monitoring could otherwise only be performed on a periodic or incomplete basis. Adoption of techniques such as Flooded Member Detection (FMD) and devices such as remote operated vehicles (ROVs) can reduce or eliminate the need for divers. Designing for inspection could therefore be considered as an example of inherently safer design.

The detectability of damage when it has occurred is very important, particularly for fatigue damage when there is a possibility of unrevealed damage up to a point shortly before failure occurs. In an environment where degradation is a possibility, inherent safety may include the concepts of 'design for inspectability'. Differences in inspectability may exist between structures which have the same overall strength or defence against damage. In some cases, comparatively small changes in dimensions, with limited effect on the strength, make great differences to the ease of inspection. An example here would be provision of easy access to welded joints for inspection.

In an offshore installation, the sub-sea elements are difficult to inspect, requiring possibly divers or ROVs and the application of complex and error-prone NDT procedures to detect cracks. Inspection may only be performed on a periodic basis, perhaps limited in any case by considerations of diver safety, to periods of calm weather. However, the emergence of new techniques may allow either continuous or much more frequent assessment of integrity. Examples of this include:-

1 The use of permanently attached transducers. Recent advances in both transducers and instrumentation mean that it is possible to set up monitoring arrangements that can operate continuously. Although it may be difficult to cover more than small volumes of the structure this way, the technique has advantages when the degradation is expected in certain areas. Examples of this include both highly stressed points, such as nodes, and areas where defects have been found in earlier inspections and which require monitoring.

2 The use of 'smart' materials. In some cases it may be possible to incorporate transducers into a material to allow detection of cracking. One commonly cited example is the incorporation of optical glass fibres into composite materials. The detection of reflected light indicates breaks in the fibres associated with damage to the structure. In some cases it may also be possible to measure other parameters such as applied strain by determining the effect on the propagation of light in the fibre.

3 The use of methods such as Flooded Member Detection (FMD). Here cracks are detected by determining whether the relevant member has filled with water. Although the damage that can be detected is comparatively gross, the technique is quick and easily applied, making more frequent inspection a possibility. Use of FMD is not in itself an inherently safer approach. In fact it demands a different approach to damage assessment as cracking is only detectable at a comparatively gross level. However that approach may offer greater safety, depending on the inspection periods and the reliability with which the different techniques can be used to detect defects.

6.6 THE ROLE OF DESIGN GUIDANCE AND CODES

Documents, such as the 4th edition guidelines[24] and other design codes such as the ASME codes for pressure vessel design, detail the results of calculations or measurements performed on real systems. As such they should incorporate the principles of deterministic or probabilistic design as appropriate.

There is a widely made assumption that codes are conservative, ie. that design in accordance with them will result in a structure that is safe. However the use of codes allows a simplification of the design process, ie. by removing the necessity to perform individual calculations. To do this it is a reasonable assumption that limits within the codes have been set such that there is a wide safety margin. There remains the possibility, however, that in some cases code requirements are not conservative[27]. A further possibility is that ambiguity of the codes, which can be highly complex, becomes the source of a mistake in their interpretation.

Shortcomings in codes may be further exposed by the use of risk-based approaches, for example, for fatigue analysis, to trim 'conservatism' from a code to reduce the cost of the structure. Eroding the margins of safety in the codes in this way may in some cases be justified where these are grossly conservative. But this does require a detailed understanding of the code, its basis, and how these relate to the specific hazards and their interactions in the design. If the nature and degree of conservatism is not well understood there is a danger that margins will be eroded too far.

Although there is no reason to suppose that any of the details contained in the 4th edition guidelines[24] or other major design codes are incorrect, we caution against the assumption that codes are necessarily conservative or lead to conservative designs. As an example, a fatigue curve may be present in the codes, the adequacy of which is well demonstrated within a set of standard parameters such as stress range and environmental conditions. However, the process of showing that the actual stress range is within the region of confidence of the curve is an area where misjudgments can conceivably be made. Such an event should, however, be prevented if the code is written properly. There are also situations where limited test data are available to derive specific equations, perhaps necessitating the scaling up of data from small scale experiments. In such cases there remains a level of doubt about the appropriateness of the equation to the actual application.

The principles of inherent safety are perhaps not immediately obvious within a design process in which a structure is designed to a notional failure probability. For example, wave height data are provided for various locations around the UK. These are normally formulated in terms of the likely '50-year return wave', ie the wave of such an amplitude that it will only be seen on a 50 year timescale. Although there is a requirement to consider the effect of the 50 year wave, considering less frequent events may result in rapidly escalating construction costs. However it would be reasonable to say that a design which is also able to withstand say a '100 or 1000-year return wave' without significant damage would be inherently safer than one whose design can withstand the '50-year return wave', but which would undergo rapid collapse with larger waves. This is therefore an area where the balance between cost and safety is apparent.

There may be a role for inherent safety in the sensitivity studies that should be performed to test the response of structures to various external and internal hazards. The design should be able to withstand the basic design hazards, but would also benefit from being well away from any 'cliff-edge' areas where a slightly greater hazard, or under-design due to uncertainty in the assessment could result in collapse. Clearly a structure that meets design requirements, but for which a calculated failure probability is very sensitive to, say, assumptions about the 50 year wave height, is less inherently safe than one where there is less sensitivity.

In other cases there is a clearer role for inherently safe design principles to be applied. For example, both snow and ice accumulation and marine growth can present problems of structural integrity, by adding to the load caused by wind and currents respectively. An application of inherently safe design principles might be to find methods that minimised the accumulation. In the former case, this could be achieved by: selecting a subsea design (hazard avoided); minimising horizontal elements (passive measure); or providing the ability to heat them (active add-on measure) such as is done for aircraft wings. In the case of marine growth, there may be the possibility to apply an anti-fouling coating. However in this particular case there may well be a trade-off between the structural integrity of the installation and the effect of the anti-foulant on the environment.

6.7 CONCLUSIONS

In the above discussion certain points have been developed. There is a general imperative to minimise cost by reducing what amounts to unnecessary added strength. Inherent safety should not be seen as the process purely of 'making things stronger' as it then contradicts the economic reality. It is also ultimately unnecessary according to the ALARP principle. A compromise is called for between safety and cost in cases where the risk is not extreme and where the point of 'diminishing returns' has not been reached.

Aspects of the design need to be considered to determine if the risk can be avoided (by horizontal drilling from shore/island), mitigated (by limiting marine growth), made more easy to detect when latent (by improved inspectability), or made less important (by improved structural redundancy).

Some aspects of what could be considered as the main principles of inherent safety are covered in part by the leading design codes (basic strength, redundancy, safety margins) but not usually as a central, visible, requirement. They may therefore be benefit in developing inherently safer principles for structures, that bring these important aspects more into the open. An overall approach based on inherently safer principles could be set out as follows:

- explicit treatment at the earliest stages of concept design of all hazard loadings and relevant combinations of these.

- select processes which minimise threats to structural integrity by, eg avoiding materials which can attack or degrade structural components because of phenomena such as chemical incompatibility. Also avoid the need for passive or active engineered safeguards to maintain integrity, especially those that can impede inspection and maintenance.

- select locations, configurations and orientations which minimise threats to the structure by, eg avoiding shipping lanes, orientating to take the predominant wind/waves, avoiding areas subject to scouring or foundation weaknesses. These options will increase as horizontal drilling and multiphase pumping technology develops, allowing more flexible location of installations.

- design primary structure to have higher reliability and resistance to failure, eg lower stress ratios, longer fatigue life, fracture resistant materials.

- design to survive local / component failure by maximising redundancy through alternative load paths, and by identifying and addressing 'weak links' in the structure.

- design to minimise overall structural integrity risks caused by local failures by ensuring the gross effects of failures are progressive, eg gradual collapse of installation, compartments arranged to maintain stability on flooding on floaters.

- design to minimise the potential for damage to safety critical systems and elements, eg reduced vibration and deflection, and limiting deformation under hazard conditions such as fire attack.

- design to allow more reliable and effective pre-service and in-service inspection and maintenance.

- design the structures so that early defect detection probability is high - to allow incipient failures to be detected early eg by inspection and to give enough warning to take remedial action, eg 'leak before break' design of containment, and the use of defect tolerant materials.

- design to reduce the task of end-of-life decommissioning.

This list provides an attempt to turn the concepts of inherently safer design into structural design principles. Many of these principles are already recognised by designers as being good engineering practice. However, consideration is not always given to them in a visible and recognisable manner. The process of ensuring safety during design could benefit if the need to consider the principles of inherent safety existed explicitly.

7. REVIEW OF CURRENT DESIGN APPROACHES

7.1 INTERVIEWS WITH SELECTED INDUSTRY REPRESENTATIVES

A small number of key people in UK operating companies and engineering contractors were interviewed to assess the level of awareness and use of inherent safety in the design of offshore installations, and to seek their views on the value of such an approach and how it could be promoted better. The people selected were those considered to be at the forefront of offshore installation design and design safety, and included corporate design safety specialists, safety specialists in design teams and engineering / design managers. Overall 14 people from 5 organisations were involved in the interviews.

These interviews were very informal, and were structured around a simple set of questions:

1 Introduction - about your own organisation, and about this Project
2 About you and your role in design/safety
3 The design process you follow
4 How Safety is addressed in the design process
- technical aspects of addressing safety
- inherent safety awareness
5 Obstructions / hurdles / stimuli to the use of inherent safety
6 Your views on inherent safety (and health / environment)
- what benefits, where and when to use it
- how to improve the use of inherent safety generally and in design specifically
7 Use of tools, aids, training packages
- what could be developed to help you in adopting/applying inherent safety

The interviews were very successful in drawing out some of the key issues in design safety and the role of inherently safer approaches. The findings were also remarkably consistent, with similar approaches, views and problems being raised. This gives some confidence that the findings may be representative of the industry as a whole. It was also interesting to note that the findings of these discussions were very much in-line with the findings of other recent surveys[2][3] of the UK and European onshore chemical and process industries.

The following sections summarise the main findings of the interviews.

7.2 AWARENESS OF INHERENTLY SAFER APPROACHES

7.2.1 Awareness of individuals

The interviews showed that some of the leading safety specialists are familiar with the term 'inherent safety' and have some understanding of its principles and benefits. A few of those interviewed clearly had a good grasp of the concept and its application (perhaps those that had read one or more of the books by Trevor Kletz), but others only seemed to have a superficial understanding of the principles and how to apply them.

As a result there were several views as to what constituted inherent safety, including the classic principles of 'intensification, substitution, attenuation and simplification', 'avoiding hazards', 'risk minimisation' , 'hazard prevention' and 'good engineering'. This shows there is a need to further educate the safety specialists in the concepts and application of inherently safer approaches, and show how this fits in with hazard avoidance, prevention, control and mitigation and the use of 'inherent' and 'add-on' safety measures to minimise risks.

A clear understanding of inherent safety by the safety specialists (be they in the design contractors, operators' asset groups or corporate functions, or consultants which these use) is vital since these people provide the best means of educating the designers and project engineers and persuading them to use inherently safer approaches to the design.

Most companies are putting safety specialists into projects at the very start, so they can use their powers of persuasion to ensure safety integrated with design. These safety people have little real power so they have to rely on leading by example/persuasion to ensure safety is considered by all in the design/project teams. The safety specialist also needs to be competent and respected, and have a good grasp of the hazards, design issues and inherent safety issues if they are to make any significant effect. The safety specialists or other 'champions' of inherent safety must have the backing and support of senior management if they are to successfully persuade designers, etc to use inherent safety (IS). Without this active, visible, or even simply acknowledged, support the champion will find it very difficult.

A positive effort is therefore needed to bring inherent safety in to an organisation and change the culture; just adding it to the regulations or procedures will not be sufficient.

Unfortunately, from the views of those we interviewed, it would seem that few senior managers, project / engineering managers or designers would recognise the term 'inherent safety'. They therefore are unable to provide the leadership, encouragement and support needed to foster an 'inherently safer approach' to design, or any other hazardous management situation. They may however recognise, support and apply some of its principles such as 'keep it simple - keep it safe', 'minimise inventories of hazardous materials', and 'try to keep hazards away from people'. Perhaps these could be emphasised as a part of an inherently safe approach to make managers more aware of inherent safety and its benefits.

Despite the slightly different views as to what is inherent safety is, all those we interviewed believed that avoiding or combating hazards at source provides the best means of hazard management, and in most cases also should provide the most cost-effective means of hazard management.

7.2.2 Training

The level of safety training given to safety specialists and the design teams varied from organisation to organisation, but inherent safety rarely featured in any of this training. One of the companies interviewed has recently embarked on a training programme for all team leaders and specialists which specifically includes the hazard management principle and the role of inherent safety. This should go so way to ensuring that all those managing or advising projects have a basic understanding and competency in inherent safety.

7.2.3 Regulations and the HSE

Everyone we spoke to said that the requirements and ideas in the regulations and industry guidance were the main influence on how safety was addressed in design. However, although the more recent of these do mention inherent safety, few emphasise it. As a result they do not appear to have led to a widespread understanding and implementation of inherent safety. It may take some time before the ideas mentioned in the regulations and industry guidance permeate into the design teams. This process could be helped by a more visible recognition of the role of inherent safety in regulations, and a clear understanding of the meaning of inherent safety and its application in guidance and other supporting documentation.

7.2.4 The learning process

All the organisations we talked recognise that good design safety, including inherent safety, requires an ongoing learning process, where issues, lessons and experience are gained and then passed on to the next project. They all thought that the best way of achieving this is to ensure a stable project team, and to provide a working environment where people stay with the company and go on to work on other projects. The use of joint client-contractor teams provides an even better environment for sharing ideas and learning from each other. This way of working in an alliance is finding favour with a number of operators and contractors.

Although people provide the main means of 'learning', there are a number of organisational activities which can enhance this process by providing a more formal means of recording information and disseminating this more widely. Some good examples mentioned in the interviews were:

project 'close-out' reviews to record what went well and what did not, and why;

'post project' reviews one or two years into operation where the designers and operators discuss what has worked well and what has not, and why;

the appointment of 'technology collators' in the project team who have the responsibility to record any new ideas, lessons or issues that arise during the project, especially those that for one reason or another could not be adopted on the current project. This information is then fed into the research programme and the next project teams.

These activities could include a specific requirement to record inherently safer ideas and options and to suggest inherently safer alternatives to some of the problems encountered.

The ideas above fall under what has been described as the 'plant after next' philosophy. Good ideas and novel technology may be rejected during a design project simply because they came to the attention of the team too late on, or because they were seen as in need of development or testing. If these ideas are not captured, or developed, then the same thing could occur on the next project. The 'plant after next' philosophy is that those in the current design team should record any good ideas and feed them in to the start of the next project. Ideas or new technology in need of development should be pursued outside the project team (eg by R&D team) so they can be made ready for a later project, 'the project after next'.

7.3 THE DESIGN PROCESS

7.3.1 Feasibility stage

Most of the companies we spoke to follow a staged approach to design, starting with a feasibility study to determine the best economic option for exploiting the field, then conceptual design of the installations and infrastructure this requires, and finally detailed engineering once the project has been sanctioned.

The feasibility study is usually carried out by the lead operator, although it is becoming more common for the design contractors to also be involved at this stage. The selection of the best option is usually made on economic and practical feasibility criteria. Safety may be addressed by a simple hazard or risk study on the preferred option to ensure that it likely to be acceptable in terms of its safety performance - a sort of safety go/nogo check. Some operators have started to bring safety performance more directly into this selection process, by assessing the risks of each option, and using this as one of the selection criteria. This allows judgements to be made between practicable options to see which offers the best combination of safety and economic performance. The safety performance includes looking at the full lifecycle of the field and installation to ensure, for example, that a safer installation is not achieved at the expense of higher drilling or diving risks. The economic assessment also usually takes a lifecycle view. This may be important for inherent safety, since some options (eg thicker vessels, structures designed to ease inspection) may be more expensive to buy but offer cost savings during operation.

BP inconjunction with W S Atkins and others have developed a rapid ranking tool[28] to evaluate the risks from many different options to help in this feasibility / selection process. Although the tool does not assess the 'inherent safetyness' of the option, it does take broad account of the equipment, inventories, pressures and the layout of the installations. In the future such tools could be adapted to distinguish between the risks addressed by 'inherent' and 'add-on' safety measures.

Taking a more detailed look at safety, health and environmental matters at the feasibility stage ought to be a priority for all in the industry, as this is the stage when the main problems can be 'ironed out' by changing the basic design. Once the basic concept has been selected, the flexibility to improve safety by tackling the hazards at source diminishes rapidly, and this can result in a greater dependence on 'add-on' and procedural controls which can be costly to install and operate, and which can and do fail.

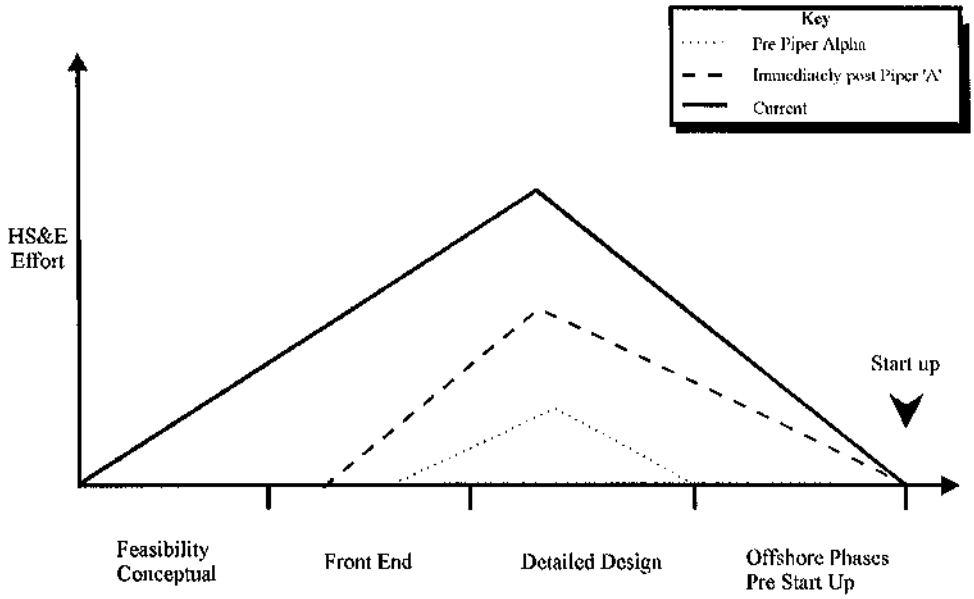
All the people we spoke to believed that the best opportunities for using inherent safety were at the very early stages of design, and that time and effort put in at this stages would more than pay for itself later on since the main problems would have been sorted out at the start. One company recalled how such an approach had been tried on an onshore project, and the overall result had been very successful, with the detailed design progressing very smoothly and the project overall coming in on time and budget despite a large investment at the concept design stage (about 1/3 of design time spent in concept design and associated safety studies).

In fact the industry is moving in this direction already with more effort now being directed at safety than before (See Figure 4, next page) and, significantly, the effort is coming in at the start of projects rather than later on. This reflects the move from the old regime where safety studies were mainly aimed at proving that the detailed design met the prescriptive requirements of regulations to the current regime where the design has to be developed so that risks are minimised.

The safety case approach has been fundamental in bringing about this change, but appears to be resulting in a more effective use of 'add-on' safety measures, with less attention to inherently safer alternatives. Inherently safer issues ought to be given more attention in the next round of design safety cases.

Several operators commented that few of their 'new' projects were actually 'green field' projects. Most involved using past designs to cut down on design costs, or were constrained by other requirements such as other facilities they need to tie in to. In these cases the opportunities for inherent safety were limited since the design was essentially fixed.

Figure 4
Phasing and Growth in HS&E Activities for New Developments



• Reproduced Courtesy of BP Exploration

7.3.2 Conceptual and detailed design

At the end of the feasibility stage, the basic design and manning arrangements for the installation will have been decided. In the next stage, concept/front end design, a lot of effort goes into optimising the layout and position of the various modules to minimise risks to personnel.

Inventory reduction and simplification can also be sought, although some of the basic choices about the process may have been made during the feasibility stage, eg. number of process trains and stages, need for compression. Combining units or eliminating process stages provides a good example of inherent safety which can also cuts costs and make space/weight savings eg. eliminating the need for a third separation stage, or combining intercooler duties between compression stages.

We were surprised to find that different installation sizes and shapes were not apparently being considered at the concept design stage. The design team seem to be given flexibility regarding the layout of any equipment, but cannot or do not change the structure it is to rest on. Perhaps alternative designs are considered during the feasibility stage, eg. long thin vs. short squat platform, 'Y' shaped vs rectangle vs triangle. It was not clear to what extent different installation types were considered, when this might be done, or how safety was factored into this.

Structural design codes have provided the basis for safe design for many years. Recently risk based approaches have been proposed to identify areas where conservatism in the codes could be trimmed, with the aim of reducing capital, inspection and maintenance costs. Such trimming may reduce the robustness of the design, especially in areas where the hazards and failure mechanisms are not well understood, making it less inherently safe.

7.3.3 Influence of safety case regime

The requirements of the safety case regime have typically been implemented as a number of hazard and risk studies throughout the project. The HSE place a reliance on such studies as the means of demonstrating safety and as the regime develops and matures it may be that more emphasis will be placed on demonstrating and assuring the quality of the design teams and the decisions they make.

The detailed descriptions of the studies required and the issues to consider found in the large volumes of recent offshore regulations, ACoPs and guidance may also tempt some into believing that if all the requirements of these are met (ie they have done all the required safety studies), then they will have a safe operation and design. This may not be true, and operators must always be able to judge for themselves what is safe or not, even if this means doing things beyond that specified in the regulations, or by doing things in some other way. It should be noted that the general duties under the Health and Safety at Work, etc Act 1974 require all owner/operators to have safe plant and safe systems of work 'so far as is reasonably practicable'.

7.3.4 Attitudes and timing

It was noted that safer design options may be rejected because of some past experience or judgement based on the belief that they are too expensive, without asking how they could be made economic. If, for example, designers were asked if they could provide a 50 m gap between the process and the accommodation they would probably say this was uneconomic in all but shallow water. If on the other hand a senior manager stipulated that all installations should have such a feature, it would probably not be long before someone came up with an economic way of achieving this. This may not be a particularly good example, but I hope it illustrates the point that it may be better to ask **how** we could achieve something rather than **if** it can be achieved.

The rapid programmes for new installations combined with the natural tendency to 'do what you know will work' means that there is often not enough time and commitment to test out or investigate novel technology or new ideas on layout or process design. Some companies are trying to use 'technology custodians' to capture any ideas and to try to keep abreast of developments and research so new ideas can be evaluated ready for future projects (ie 'Plant after next' philosophy).

It is not clear whether the message that 'extra effort and time spent at the early stages of a project, and the use of inherently safer approaches can reduce costs and may even shorten the overall programme' is getting through to the senior managers and project engineers. They seem to be reluctant to put in extra effort at the early stages, or allow extra time at the early stages of the project to sort out the main issues and problems, and explore alternatives, before getting into details that essentially 'fix' the design.

Certainly the industry now seems to consider all projects as 'fast track', and are making extensive efforts to shorten programmes. Whilst it is understandable that revenue should start to flow as soon after capital expenditure as possible, this is mainly down to the time between procurement and start up. The feasibility studies and early concept design involve relatively little expenditure, yet the decisions made at these stages essentially set the cost of the project. It would therefore seem logical that more time should be allowed at these early stages to identify and assess design options to optimise cost and safety performance.

There is no approval regime for the 'Design Safety Case', outstanding problems or disagreements could result in having to make significant changes late in the design or run the risk that the main operational safety case may be rejected. Some operators now see the Design Safety Case 'rejection' as the main risk to the viability of the project, and some are not sanctioning projects until this stage has been reached.

The underlying problem is that the level of detail required by the Design Safety Case may not be available until well into concept design. By this time the major long lead time components will have been ordered, so the design is already 'fixed'. Comments need to be made at a sufficiently early stage to allow these to be incorporated into the design without the need to do expensive major rework which could cripple the project. This implies an ongoing process of comment and 'acceptance / agreement', rather than a single milestone submission of the safety case.

Such an approach is essential if inherent safety is to be encouraged, since this relies on the ability to influence the basic design at an early stage. Making late comments on the design is likely to leave the designer with no practical choice other than to back fit some 'add-on' safety measures to address the hazard.

A further hurdle to inherent safety is the way in which some project teams have, in the past, waited for the results of the hazard studies before seeing how the design can be improved. In some cases these studies have taken so long, that the design has moved on such that major changes cannot be introduced. More rapid and targeted studies are required at the onset of the project if basic improvements are to be incorporated into the design. In fact many contractors and operators are finding that the best approach is to use a very experienced safety and engineering team to 'blitz' the design at the start to identify the main problems and do some quick studies so that the these problems can be sorted out in good time. The experience of those who have tried this is very positive, but it was noted that a 'quality' team is needed to do this quickly and to ensure major problems are not missed or poor solutions implemented.

The design team should also be trained/encouraged to identify or pre-empt problems and solve these as they go along, and use the main studies as a cross-check to ensure nothing is missed.

Overall, it appeared that the industry seems to have too short a horizon, or insufficient confidence in its future, to carry out assessments of possible options in advance of definite projects. There seems to be no resources to plan for the future in terms of safe design and operation.

7.3.5 Application of Inherent safety

The main application of 'inherently safe design' at present is to avoid or reduce the consequences of hazards such as fire, blast, ship collision and dropped objects by careful orientation and optimisation of the topsides layout. Living quarters are typically placed away from the effects of fire and explosion by the use of bridged linked installation, or by placing less hazardous modules between the process area and the accommodation to act as a buffer zone. Whilst this 'segregation' approach can help prevent escalation or protect evacuation routes it does little to reduce the severity of the initial hazard, or any fatalities this may cause. Measures such as reducing inventory or eliminating leak points can be more effective, reducing both the initial hazard, and the chance of escalation.

Demanning or the use of not normally manned installations (NNMIs) is another 'inherently safer' approach based on segregating people from the hazards which is being widely adopted. This introduces some issues regarding level of maintenance and the need to provide safety systems when people are on board. Simplification and inventory reduction can again help here by reducing the maintenance load and limiting the magnitude and likelihood of an incident when people are on board. An exception to this may be diesel storage, where a larger inventory may be 'inherently safer' since it reduces the need to visit the installation, yet not significantly increase the hazard (diesel is a low hazard compared to oil and gas).

In the future, technology, such as multiphase pumping and metering and subsea separation may eliminate the need for surface installations, and with high reliability systems and advanced ROVs the need for diving to maintain these subsea systems may also be minimal.

Some compact new technology such as hydrocyclones for oil/water separation are already being used a provide classic examples of inherent safety - being both compact and simple. Compact heat exchangers are also being used. Although these have smaller inventories then conventional shell and tube designs they can be more prone to leaks and may not be as robust.

Significant further inventory reduction within unit operations is unlikely until technology moves on another step, although designers should try to minimise inventory wherever possible, since this adds hazard and weight/space. However, sometimes it is possible to reduce inventories by combining unit operations, equipment or functions.

Simplification is another effective way of reducing risk, especially if the size and number of leak sources can be reduced by the use of welded pipework, high integrity seals and fittings, reduced instrumentation etc. Reducing the number of leak points often has a pro-rata affect on the risk levels. Several of those we interviewed claim to carry out systematic reviews during the design to try to eliminate leak points, although in one case this was normally only done for high pressure gas lines.

Other means of simplification by the use of good ergonomics, clear plant status, etc to ease operation and maintenance may not be reflected in the risk assessments, but should bring substantial benefits during operation, as well as reducing the likelihood of an accident due to human error.

7.3.6 Procedures and methods for inherent safety in design

Few of the companies we spoke to had safety policies or design safety procedures that specifically mentioned inherent safety. However some of the safety reviews in the design procedures did include mention of reducing inventory, reducing the number and size of leak points, simplifying operations etc.

Various hazard identification studies, specific safety studies and risk assessments are used to develop the safety case for the design, but it was not clear to what extent these studies addressed inherent safety. We did not see any systematic methods or tools to question or challenge the design from an inherent safety point of view. Such tools are being developed and used in the onshore chemical industry[3][29]. For example, Figure 5 shows a general guideword list developed on the INSIDE Project[3] aimed mainly at the onshore chemical industry which could be used in a study of the process flowsheet to challenge the design and seek out inherently safer options. 'Function challenging' methods are also being developed.

The overall view from our interviews with offshore designers and safety specialists appeared to be that the degree to which these studies attempted to avoid or reduce the hazards at source (ie apply inherently safer approaches) was dependant on the awareness and 'way of thinking' of the persons leading or in the study team. Little or nothing in the study methodology or the 'checklists' used would prompt an inherently safer approach.

This suggests that opportunities to apply inherent safety may be being missed due to a lack of any systematic consideration of inherently safer approaches. This could be overcome by raising awareness of the concepts and by providing some structured methods or tools to prompt consideration of inherent safety during hazard studies.

One company said that it had found that systematically questioning the function of equipment was a good way to gain an understanding of its real purpose, and hence identify alternatives or changes that could achieve the same function, but in a safer or better way. The INSIDE Project[3] is already developing the idea of a function identification and challenging tool to promote the identification and evaluation of inherently safer alternatives in process development and design.

Several of the people interviewed stressed the need for designers to understand the strategic approach of prevention, control and mitigation for hazard management often quoted in regulations and other safety publications. However it was also recognised that this representation of hazard management did not necessarily encourage inherent safety. Perhaps a simple strategy that encouraged hazard avoidance/elimination, reduction at source and segregation might provide a more effective prompt for inherently safer hazard management.

Another important issue that was raised several times was that the use of inherent safety relies on a good understanding of the range of hazards and how these interact with the design. What may be 'inherently safer' for one hazard could cause problems in another area, so it is vital to have a good overview of the situation. Also an inherently safer design may not have such visible safety as an add-on safety design. For instance an ESD valve or pressure relief valve is clearly identifiable as being critical to safety, and any modifications to these would be controlled accordingly. However in an inherently safer design it may be the pressure rating of a separator, or the inventory of an heat exchanger that is critical to safety. These are not so visible as 'safety' and so a more careful recording of the basis of design safety may be required for an inherently safer plant so that future operations or modification do not inadvertently breech the safety envelope.

Figure 5
Process Flowsheet Assessment Parameters / Guidewords

Parameter	*Guideword*	Deviation
Process Stage **(Apply to unit operation or process feed / junction)**	*Avoid* *Change*	Eliminate / Avoid Elsewhere Combine Split Segregate
Processing Method	*Change*	Batch / Continuous Processing method (see functionality assessment keywords)
Equipment	*Change*	Size Geometry Type
Timing	*Change*	Sequence Duration Timing Feed profile
Physical Conditions	*Change*	Pressure Temperature State (solid,liquid,vapour) Level
Chemical Conditions	*Change*	Material Concentration Composition Catalyst Solvent Mixing

7.4 WIDER ISSUES

7.4.1 Client - contractor relationship

The relationship, both at the working level and contractually, between a client and contractor(s) can affect the degree to which innovation and inherently safer alternatives are sought and used.

There still appears to be a wide range of relationships in use in the offshore industry, from rigid fixed price/detailed specification contracts to more open and flexible alliancing arrangements where the responsibility for the design is shared between the various partners. The more flexible and open arrangements probably provide the best environment for the constructive exchange of views and experience hopefully leading to a better balance between inherent and add-on safety.

It was noted that some contractors are aiming to offer 'lifecycle' services to operators in the future, where the contract includes design, construction, operation and abandonment of the installation. These type of arrangement should mean that operability issues are given more thought at the design stage, and perhaps provide an additional incentive to simplify the plant and its operation and maintenance.

It was also recognised that fixed price contracts may not provide an environment to encourage consideration of alternative design options and novel ideas or technology because of the extra time and risks this may involve. There may be case for having a more flexible 'reimbursable' or 'alliance' arrangement for feasibility and concept design work to allow alternative options to be followed up. Once the concept design has been firmed up, then the remaining detailed design, procurement and installation could still be let as a firm price EPIC contract.

7.4.2 CRINE

The CRINE initiative (Cost Reduction In the New Era) appears to be supported by most operators and contractors. Both the operators and contractors we spoke to welcomed the drive to have more open and 'objective' contractual arrangements to give a more 'fit for purpose' deliverable and fairer share of margins. Such arrangements should provide a good incentive to identify and use inherently safer approaches to design.

The drive for standardisation was more problematic. This may go against the current trend to provide bespoke designs that are fit or purpose, tailoring cost and specification to meet the specific requirements. There is also a concern that standardisation may hinder technology development. To what extent standardisation hindered or helped inherent safety would depend on how inherently safe the standard specifications and equipment are.

7.4.3 Fiscal metering

A significant proportion of offshore processing is carried out solely to meet fiscal metering requirements. This may include having to provide extra separation and metering trains on installations serving more than one field, or having to provide extra risers and pipelines to keep fluids from different fields segregated. It may also mean that a separate installation is required to with a separation train and possibly compression instead of a simple pipeline to an adjacent installation.

If the requirement for separate metering for each field could be relaxed or achieved in some other way, this could simplify many offshore installations, allowing co-processing and shared pipelines/risers, or even avoid the need to provide some platforms or separation facilities completely. This could allow many offshore designs and operation to be made far more 'inherently safer'. 'Metering' could be achieved instead by the use of non-intrusive multiphase meters, or by allocations based on calculations/analysis of the co-processed fluids. Fiscal meters also require a lot of maintenance and testing which adds to the manning burden on NNMIs, so less fiscal metering would also cut operator exposure.

7.5 CONCLUSIONS

The limited number of interviews, with representatives from the UK offshore industry, undertaken for this project have nevertheless provided a good insight into the way safety is addressed in design, and the role inherent safety can play in this. There was good agreement between the findings of the different interviews, and this gives some confidence that the findings may be representative of the industry as a whole.

The term 'inherent safety' has only recently come into the mainstream language of offshore design safety, mainly through its appearance in the Offshore Installation Design Safety Case Guidance[7], and the UKOOA Fire and Explosion Management Guide[8]. This has started a process of education in inherent safety, that as yet seems to be confined to some of the safety specialists. Even within these circles there are subtle, but significant differences in what people consider as 'inherent safety', from hazard avoidance, to risk minimisation.

The industry has made some significant advances in safety practices over recent years, and the 'Safety Case' regime has led to designs being developed with close attention to the likely hazards it could present. This has encouraged designers to avoid or reduce some hazards at source, and especially to look to demanning or segregation as a means of protecting personnel from the effects of hazards. Many of these approaches have led to inherently safer designs, however there does not appear to be many systematic attempts to consider inherent safety throughout the development of the design.

The greatest opportunities for identifying and considering inherently safer design options are at the feasibility stage, but it is not clear to what extent safety is factored into these studies. In some cases safety may simply be a go/nogo criterion applied to the most favourable economic options, rather than an integral parameter in the decision making process.

Inherently safer applications can also bring longer term benefits such as greater reliability, reduced operating costs in later years, or easier decommissioning. These benefits may be overlooked unless some form of life-cycle cost-benefit assessment is carried out at the design stage. Some companies are using lifecyle-cost techniques to optimise maintenance and repair strategies.

The fast track nature of projects is also leading to a number of problems which may be hindering the adoption of inherently safer alternatives, and diluting the influence of the design safety case liaison from both the point of view of the project team and the HSE.

Finally contractual and working arrangements between clients and contractors can greatly influence the ability to encourage designers to challenge the basis of design and to seek out and adopt inherently safer alternatives. Alliance contracting arrangements and other forms of collaborative team design may provide the sort of environment required to encourage the use of inherent safety.

8. CONCLUSIONS

This Pilot Study has been undertaken to assess the extent to which the concept and principles of 'inherent safety' are being applied in the development and design of offshore oil and gas installations in the UKCS.

It has reviewed some recent literature and some of the main regulations affecting the design and operation of offshore installations. However the main element of the study was a number of interviews with representatives of some of the leading Design Contractors and Operating companies. Only a small number of people were interviewed from 5 companies, but the findings were sufficiently consistent to give confidence that they perhaps reflect the wider view of the UK offshore industry.

The study has shown that the concept of Inherent safety is an effective means of hazard management, and one that fits in well with the way the UK offshore oil and gas industry is developing. The concept encourages demanning, simplification and intensification and hence goes hand in hand with subsea technology, minimum facilities and unmanned installations. It may offer the most cost effective way to achieve safety for new designs. The main hurdles to adopting inherent safety are: the lack of awareness of the concept, especially by designers and project leaders; a lack of understanding of the principles of inherent safety and how these can be applied in those who have heard of the concept; the difficulty in securing time at the early stages of projects to consider safety aspects; the way safety may be addressed in feasibility studies; the limited attention to inherent safety in regulations and the way the design safety case does not appear to align well with the project decision timetable.

The findings of the study show that the term 'inherent safety' is only just beginning to be recognised in the industry, mainly as a result of its inclusion in the Design Safety Case Guidance, and the UKOOA Fire and Explosion hazard Management Guide. Although many safety professionals would claim knowledge of the concept, not all seem to have a clear view as to its meaning and principles. There appears to be a number of subtle but significant differences of opinion as to what inherent safety is, including 'hazard avoidance', 'hazard prevention', 'risk minimisation', and 'good engineering'. Whilst all of these may form part of an inherently safer strategy, they do not encompass a full understanding of the role of inherent safety. There is therefore a need to raise awareness of the principles of inherent safety and perhaps to develop a more detailed definition and set of principles for use in the offshore industry.

Many companies seem to be placing safety specialists in to the project teams at the early stages to help ensure safety is addressed integrally with the design, and to educate designers about safety issues and possible solutions. If this approach is to be effective, the safety specialists must have sufficient experience and knowledge to appear credible in the eyes of the project team. They must also have a clear understanding of inherent safety and its practical application if it is to be taken on board by the project team.

Although few designers would be familiar with the term 'inherent safety', many do apply some of its principles such as inventory reduction and simplification, but not always in a systematic way. Further opportunities to reduce inventory, simplify plant, and apply the other inherently safer principles might be identified if these principles were made more visible, and incorporated into systematic hazard studies, design reviews and procedures. Designers should also be encouraged to challenge and question the basis of the design and the need for equipment and features. This can help clarify the requirements of the design and lead to better and more streamlined alternatives being considered which could be inherently safer and cheaper.

New technology is also providing opportunities for inherently safer oil and gas extraction and processing. Compact heat exchangers and hydrocyclones are now widely used, and the development of multiphase pumps and metering devices is well advanced. In the future these technologies may negate the need for conventional offshore installations, by utilising subsea completions, pumping and metering to bring the fluids to landfall. In the meantime work should be carried out to investigate compact forms of main stream separation, gas drying and slug handling - areas currently with the largest inventories of hazardous materials.

The recent expansion into the deep water West of Shetland means that new generation floating production, storage and off-loading installations are required. These will present new challenges for designers, and may require practices/rules of thumb developed for hazard management on more conventional installations to be re-evaluated.

This study has focused on installation design, but the design of wells, drilling programmes and practices is an area where it could be worth developing the ideas of inherent safety. The process based 'inherently safer' concept and principles may need to be adapted to aid its application in this specialist area.

Some of the main drivers in the offshore industry at present, to reduce manning levels and provide minimum facilities installations, encourage the use of compact and simple technology and reduce operator. These objectives are fully compatible with an inherently safer approach to design. Similarly, moves to more flexible and open client-contractor relationships can create the sort of environment that promotes the challenging of past practices and encourages innovation. It is in this type of environment that the ideas of inherent safety can flourish and reap the greatest rewards for both the designer and operator.

Good hazard management depends on a clear understanding of the hazards and their interaction with the design. If the design is to be optimised to avoid or reduce the hazards this needs to be done early on in the development of the design. However project programmes often do not seem to recognise that the most critical part of any project is at the very start, when all the major decisions are taken about the location and type of installation, and the processes to be adopted. By the time the concept design is finished, most of the installation's build and operational costs will have been fixed. Also most of the opportunities to deal with hazards in an inherent way will also have passed. Companies may spend some time evaluating various options from an economic point of view, but these studies may not address safety as a key parameter. If safety is treated as a simple go/nogo criteria at these early stages of design, many opportunities for an inherently safer, and perhaps cheaper, installation may be lost. Project managers should consider allocating a little more resource and time at the start of the concept design stage to challenge the basis of design and identify and evaluate alternatives that may be inherently safer (and perhaps cheaper).

There also appears to be a desire to use segregation, either by demanning, bridge linking or layout of the topsides as the primary means of 'inherent safety'. Although this approach to design may be 'inherently safer' than older designs by limiting escalation, it does little to reduce the likelihood or severity of the initial hazard itself. It therefore does little to protect those normally out on the plant. Reducing the hazardous inventories and simplifying the plant can reduce the risks from the initial hazards as well as limiting escalation, and more attention might be given to this in future designs. It is however accepted that the order of magnitude reductions in inventory needed to significantly reduce the size and duration of fire and explosion hazards may not be achievable without some step change advances in separation technology.

Current Regulations and Guidance do mention inherent safety but could do more to promote its use and understanding. More could be done to explain what 'inherent safety' is and how it can be applied as part of an overall approach to hazard management. The way the Design Safety Case is implemented could also be modified to provide a better and more timely opportunity to encourage the investigation of inherently safer alternatives and inherently safer design objectives. The underlying problem is that the level of detail required by the design safety case may not be available until well into concept design. By this time the major long lead time components will have been ordered, so the design is already 'fixed'. Comments need to be made at a sufficiently early stage to allow these to be incorporated into the design without the need to do expensive major rework which could cripple the project. This implies an ongoing process of comment and 'acceptance / agreement', rather than a single milestone submission of the safety case, giving the designers more confidence to move the design forward on the basis of agreement at key stages.

Fiscal metering requirements also hinder the application of inherent safety. They place a duty on many designs to undertake additional processing which could be eliminated if alternative measurement arrangements were allowed. Eliminating the need for separate processing trains, or eliminating the need for separation completely in some cases would make installations more inherently safe and cut build and operating costs.

The overview at present suggests that the principles of inherent safety suit the offshore situation very well both in terms of safety and economic performance. All those we talked to believed that 'inherently safer' approaches to design are worthwhile perusing and often offer capital or operating costs savings as well as more robust safety performance. Many installation designs incorporate some examples of inherent safety, but these tend to have arisen from 'good ideas' or specific initiatives rather than a deliberate application of inherent safety and its principles during the design process. This suggests that a more visible and systematic application of the principles could lead to a more widespread adoption of 'inherently safer' design.

The following suggestions are offered as ways in which inherently safer approaches to design could be further promoted and encouraged in the UK offshore industry.

1 The findings of this report should be widely disseminated throughout industry and the HSE to raise awareness of inherently safer approaches to design and to promote a wider discussion of the role of inherent safety and how its use can be encouraged.

2 Articles or papers based on the findings of this report should be offered to conferences or journals read by senior managers as well as designers so that senior and 'non-safety' people become aware of the concepts and the potential economic and operability benefits it can bring.

3 The HSE could consider how inherently safer approaches can be given a more visible position in Regulations, ACoPs, Guidance and its other publications, and how these can be used to show the important role inherent safety can play in an overall hazard management strategy.

4 Representatives from the HSE Offshore Safety Division and the industry could consider working together to produce an authoritative document providing an agreed definition of 'inherently safer approaches' and how these can fit into an overall hazard management strategy. It should also offer practical advice on how these principles can be applied in practice to installation structural and topsides design, well design, and drilling programmes and practices. This could be based on the ideas presented in Section 6.7 and Appendix 1 of this report, and those from the UKOOA Fire and Explosion Hazard Management Guide[8].

5 Consideration could be given to producing a simple booklet based on the above document, aimed at providing an aide-memoir to designers and project engineers. This could use simple illustrations to get the main points across effectively.

6 The HSE and industry could encourage the inclusion of inherent safety principles and their application in training programmes for safety specialists and designers, and for senior managers and project managers so they are also made aware of the principles and benefits of the approach.

7 Research and development programmes could be reviewed to see the extent to which these are addressing or encouraging inherently safer technology, design and operation. Perhaps greater priority could be given to joint programmes to develop and test new technology which could provide inherently safer alternatives in high hazard areas such as structural integrity, separation, dehydration, slug handling, gas compression, risers and pipelines, multiphase pumping and metering and subsea technology.

8 The implementation of the Design Safety Case should be reviewed to see if a more 'step by step' regime of 'design submission' and 'broad acceptance' can be adopted. This should allow a more timely consideration of issues and alternatives such that suggestions and changes can be considered and implemented without unduly compromising the project programme.

9 Consideration should be given to practical ways of encouraging innovation and the search for inherently safer design solution in projects. This might include providing more time or resources at the early stages of projects for these activities and by having more open and flexible contractual and working relationships. Perhaps one or two projects could be used as case studies to try out such an approach, and see how this extra attention at the early stages affects the overall programme, costs and safety performance.

10 Academic institutions providing graduate or similar qualifications for engineers should seek to include more emphasis on safety in general, and inherently safer design of processes and plant in particular, as part of the curriculum.

9. OTHER WORK IN THE FIELD OF INHERENT SAFETY

A number of other researchers and organisations are active in the field of inherent safety. Where applicable it may be worth coordinating any UK Offshore initiatives with other initiatives aimed at promoting the use of inherently safer approaches to design, such as:

The recently launched IPSG/I Chem E Training package on inherent safety, including a short video on the principles of inherent safety;

The CEC co-sponsored *INSIDE* Project developing tools and methods to help designers address inherent safety during the early stages of process design;

The CCPS in the USA who are intending to produce a Guide to Inherent Safety in Design and Operation.

Loughborough University of Technology who are developing an index for inherent safety.

ACKNOWLEDGEMENTS

We would like to express our thanks to the following companies for agreeing to be interviewed as part of this project, and for their support and suggestions on improving the use of inherently safer approaches offshore.

AMEC Process and Energy Limited

BP Exploration

Brown and Root *Energy Services* Limited

Mobil North Sea Limited

Shell UK Exploration and Production

REFERENCES

1 Kletz TA, 1978, "What you don't have, can't leak", Jubilee Lecture, Chemistry and Industry

2 Mansfield DP, 1994, "HSE/AEA Pilot Study: Inherently Safer Approaches to Plant Design", HMSO, ISBN 0 85356415 9.

3 The *INSIDE* Project, Phase 1, Summary Report, A review of the current status of inherent safety in the process industries, *INSIDE*/PHASE1/01/ISSUE 1, Issue 1, March 1995, David Mansfield, AEA Technology, Yngve Malmen, VTT Manufacturing Technology, Miep Verwoerd, TNO, Robin Turney, Eutech Engineering Solutions, Richard Rogers, Inburex.

4 Kletz TA, 1991, "Plant Design for Safety, A User-Friendly Approach", Hemisphere New York.

5 OTH 94 458, Update of the UKCS Risk Overview, DNV Technica Ltd, HSE Books 1995

6 The Hon Lord Cullen, "The Public Inquiry into the Piper Alpha Disaster", Department of Energy, HMSO, London, November 1990 (Two volumes)

7 A Guide to the Offshore Installations (Safety Case) Regulations 1992, UK Health and Safety Executive, HMSO, 1992

8 Guidelines for Fire and Explosion Hazard Management, UKOOA, Issue 1, May 1995

9 SI 1995 No. 743 The Offshore Installations (Prevention of Fire and Explosion, and Emergency Response) Regulations 1995, and Approved Code of practice and Guidance, L65, HSE Books, June 1995, HMSO

10 ISO Standard ISO/CD 14 690 (Draft), Petroleum and natural gas industries - HEALTH, SAFETY AND ENVIRONMENTAL MANAGEMENT SYSTEMS, The International Standards Organisation, Technical Committee ISO/TC 67, Sub Committee SC 6, July 1995

11 ISO Standard ISO/NWI 14 140 (Early Working Document Draft), Petroleum and natural gas industries - EVALUATION AND RISK MANAGEMENT, The International Standards Organisation, Technical Committee ISO/TC 67, Sub Committee SC 6, June 1995

12 ISO Standard ISO/CD 13 702 (Draft), Petroleum and natural gas industries - CONTROL AND MITIGATION OF FIRES AND EXPLOSIONS ON OFFSHORE INSTALLATIONS - Requirements and Guidelines, The International Standards Organisation, Technical Committee ISO/TC 67, Sub Committee SC 6, July 1995

13 Draft Offshore Installations and Wells (Design and Construction, etc) Regulations 199-, Consultative Document, CD89, HSE, July 1995

14 Machinery - Guidance Notes on UK Regulations (The Supply of Machinery (Safety) (Amendment) Regulations 1994) URN 95/650, May 1995, Dept. of Trade and Industry.

15 Construction (Design and Management) Regulations 1994, Managing construction for health and safety, Approved Code of Practice, HSC L54, HSE Books 1995

16 American Petroleum Institute, Recommended Practice for Analysis, Design, Installation and Testing of Basic Surface Safety Systems for offshore Production Platforms, API Recommended Practice 14C (RP 14C), 4th Edition, September 1, 1986

17 American Petroleum Institute, Recommended Practice for Classification of Locations for Electrical Installations at Petroleum Facilities, API RP 500, First Edition, 1 June 1991

18 'Titles can mislead', Trevor Kletz, J. Loss Prev. Process Ind., 1992, Vol 5, No 5, p259

19 Oil and Gas Technology, THERMIE Programme, European Commission, Directorate General for Energy, DGXVII

19a No.15 December 1994 Enhanced hydrocarbon recovery improves profitability

19b No.14 October 1994 MARS: Diver Assistance Vehicle - ROV for IRM work

19c No.11 January 1994 Decommissioning - French technology at the cutting edge

19d No.13 July 1994 Life-cycle design of semi-submersible platforms design compromise between initial cost of system and its in-service running costs

20 Oil and Gas Journal, PennWell Publications, USA

20a April 17, 95 Multiphase meter to undergo North Sea trials

20b January 9, 95 North sea operators target cost cutting in field development

20c April 10, 95 Influent/effluent approach to mud formulation reduces toxicity; CJ Burke

20d January 16, 95 Design, simulation create low surge, low cost gas-injection compressor; A Zeckendorf, JW Altena

21 The Chemical Engineer, Institution of Chemical Engineers, UK

21a April 20, 95 BP, ICI and Vortoil win environmental awards

21b March 11, 93 BP proves compact oil dewatering

21c December 9, 93 Solvent Recovery: Try power fluidics: Nick Hanigan

21d April 26, 90 Plate-fin exchangers offshore - the background: Mike Taylor

21e Sept 1989 Compact future for heat exchangers

21f July 25, 91 Innovative Technology: multiphase pumping

21g December 1988 Multiphase pumping

21h October 1988 Measuring multiphase flow

21i May 1989 First subsea 3-phase meter on test

21j May 1989 Subsea high-lights from Oslo

22 Offshore Engineer, Thomas Telford Ltd, I Civil E, UK

22a May 1991 Revolutionary LEO prepares to clean up in oily water stakes

22b August 1992 Vortex choke cut erosion

22c May 1991 Sand spinner arrives offshore

22d May 1991 High tech exchanger has it all on a plate

22e May 1991 Spiral flow boosts shell and tube exchanger

23 1974 No 289 Offshore Installations - The Offshore Installations (Construction and Survey) Regulations 1974.

24 Offshore Installations: Guidance on design construction and certification 4th Edition (Consolidated Edition) March 1993 London:HMSO ISBN 0 11 882116 4

25 Minimum Offshore Structures Cost Less, Pose Higher Risk, M.J.K.Craig, OGJ Special, July 17 1995, Oil & Gas Journal p33-36.

26 Basic Safety Principles for Nuclear Power Plants No 75-INSAG-3, International Atomic Energy Agency Vienna 1988, ISBN 92-0-123188-1.

27 'Fatigue vulnerability of jack-up platforms', E C Hambly, Proc. Instn Civ. Engrs, Part 1, 1985, **77/78**, Feb, p161-178 and discussion Proc. Instn Civ. Engrs, Part 1, 1986, **80**, Feb, p291-296

28 'Offshore Loss Prevention', F Crawley, The Chemical Engineer, 13 July 1995, p 24-25, Institution of Chemical Engineers, Rugby, UK

29 ICI Corporate Guidance 'Process Safety, Health & Environmental Guide No. 13 - Hazard Study Methodology', Eutech Engineering Solutions Ltd, 1994

APPENDIX 1 - AN INHERENTLY SAFER APPROACH TO HAZARD MANAGEMENT

A1.1 HAZARD MANAGEMENT AND INHERENT SAFETY

The main elements of a management regime for the control of risk are widely quoted as:

- *hazard identification*
- *hazard assessment*
- *hazard management by:*

  prevention,
  control, and
  mitigation

The measures used to prevent, control or mitigate the hazards, and hence reduce risk, can be inherent in the fundamental design, added to it in the form of specific engineered systems (which can be active or passive), be provided by operator/management actions, or by some combination of these.

The concept of 'inherent safety' has been used to describe those aspects of the fundamental design which can be used to prevent, control or mitigate the hazards. Such measures have the advantage that they address the source of the hazard, and make use of existing equipment and systems thus avoiding the need for expensive 'add-on' safety measures which can fail or be neglected. Techniques such as process intensification and simplification not only offer inherently safer performance, but can also reduce weight and space requirements, reduce the need for maintenance and operator supervision, and hence reduce capital and operating costs.

The following sections set out a detailed strategy for hazard management that makes best use of the principles of inherent safety, and provides a framework for designers to identify the optimal combination of safeguards to manage hazards.

The approach follows a logical sequence (See Figure A1.1) in which attempts are first made to avoid the hazard altogether. This is followed by means to reduce the severity of the hazard at source and means to reduce its likelihood of occurrence at source. If these measures prove insufficient by themselves, then segregation is offered as a means of limiting the effects and range of the hazards. Finally 'add-on' safeguards are considered, with an order of preference of: passive safeguards, active safeguards, procedural controls. The aim is to provide an effective 'defence in depth' approach to managing the hazard built in to the fundamental design.

This stepwise approach also means that designers are encouraged to deal with the hazards as close to the source as possible, and minimise the need for, or reliance on, 'add-on' safeguards that can be costly and unreliable. Similarly, segregation is used after attempts have been made to avoid or reduce the risks from the hazard at source. A reduced hazard may mean that segregation is not required, or that less segregation is needed, resulting in a more compact or flexible layout which should be cheaper to provide or easier to live with.

Another advantage of this approach is that reducing the hazards at source can reduce the risks to personnel in the vicinity of the hazard, as well as those in the more distant/protected control rooms or living areas. Purely relying on segregation and fire walls/ blast walls may reduce risks to the majority on the installation, but do nothing to limit the likelihood and consequences of the initial hazard, and the potential for injury and fatality for those on the plant.

Before the approach is described some definitions are offered to ensure a common understanding of terms and to clarify the role and meaning of inherent safety and some common hazard management principles.

A1.2 SOME DEFINITIONS

A clear and consistent basis of understanding is required if inherently safer approaches are to be integrated effectively into the hazard management process. The following definitions are offered in a attempt to clarify the role of inherent safety in hazard management, and show how various approaches to safeguards relate to the classic prevention, control and mitigation principles.

A Hazard: a chemical or physical condition that has the potential for causing damage to people, property or the environment.

Inherent safety design: an approach to plant and process design whereby the hazards are avoided or reduced to such trivial levels that the plant and process pose no threat of harm to people, property or the environment on or off-site, and as a result there is no need for additional engineered or procedural safeguards.

Inherently safer design: an approach to design that recognises that hazards cannot always be avoided or reduced to trivial levels, but which avoids or reduces the hazards at source, or simplifies the process or plant to minimise the likelihood of the hazards being realised so far as is reasonably practicable. The residual risks are then dealt with, so far as is reasonably practicable, by an appropriate combination of engineered and procedural safeguards, but with a preference for those measure that are simpler and more likely to be effective eg passive safety systems rather than active ones.

Hazard avoidance: measures taken in the design of the process or plant to eliminate or avoid the hazardous material, condition or action ie by removing it completely.

> eg. locating a crane so lifts cannot be made over the process area, avoiding the need for a second process train by the use of multiphase metering, selecting materials that do not corrode, or avoiding the need for offshore topsides separation and compression by multiphase pumping.

Hazard prevention: measures taken to prevent, or reduce the likelihood of the hazardous situation or action arising, or to reduce the chance of a hazard being realised. In practice the only way of totally preventing the hazard is to avoid/eliminate it, prevention is therefore to do with reducing the chance/likelihood of the hazard arising or being realised.

> eg. reducing the number of flanges and other leak sites in the design, pressure control systems on vessels, placing risers inside the jacket, monitoring of vessels for corrosion/erosion and acting where needed.

Hazard control: measures taken to limit the severity of a hazard before it is realised (reduce consequences) or recover the situation before the hazard is realised (reduce likelihood), especially actions or measures to interfere with the chain of events leading to the realisation of the hazard which would limit the effects of the hazard or enhance/enable recovery.

> eg. use of smaller pipework or higher integrity fittings to reduce the leak rate in the event of a loss of containment, pressure relief venting, emergency shutdown and blowdown systems, hot work controls.

Note - Active control (and mitigation) measures need to be initiated before they can start to have an effect and so rely on timely detection of the developing chain of events. Detection therefore plays key role in hazard management. See 'Detection System' definition later on.

> eg. process instrumentation and alarms and trips, fire and gas detection systems, vessel collision alarms

Hazard mitigation: measures taken to limit the effects or spread (consequences) of the hazard once it has been realised. These can include emergency escape and evacuation arrangements.

> eg. segregated layout to limit escalation, fire walls, water deluge, manual fire fighting, stand-by vessel, lifeboats.

Inherent safeguard: the design or adaption of a process, engineered system, plant or provision to avoid, prevent, control or mitigate a hazard or hazards. The safeguard is achieved by the basic functionality or attributes of the process, plant or system.

> eg. minimisation of hazardous inventory by reducing size of a vessel, designing the plant to take maximum well pressure, redesigning the process so some stages are avoided, optimising the layout in a module to reduce the severity of an explosion, minimising the number of potential leak sites by eliminating the need for some flanges, instrument connections etc.

Add-on safeguard: an engineered safeguard which is only there to ensure safety and has no function in the normal operation of the plant or process.

> eg. emergency shutdown systems, protective fire coatings, pressure relief valves, shutdown isolation valves.

Passive safeguard: an 'add-on' engineered system or provision to prevent, control or mitigate a hazard or hazards which does not need to be activated or has no moving parts. Such systems should have a high availability since they do not rely on timely hazard detection to operate.

> eg. fire walls, protective fire coatings, drains, bunds.

Active safeguard: an 'add-on' engineered system or provision to prevent, control or mitigate a hazard or hazards which needs to be activated to come into effect. Such systems rely on timely hazard detection and regular testing to ensure they operate.

> eg. emergency shutdown system, deluge system.

Procedural safeguard: a system, procedure or action undertaken by personnel to prevent (proactive), control or mitigate (reactive) a hazard or hazards.

> eg. leak testing before start-up, permit-to-work system, vessel corrosion/erosion inspections, manual fire fighting, manually initiated vessel contents dumping.

Detection system: a system or provision to enable a hazard or hazard initiation sequence, or the realisation of a hazard to be identified. These systems do not prevent, control or mitigate the hazards themselves, but are vital to the initiation of active and procedural safeguards, and so form an integral part of these safeguards.

eg. process pressure instrumentation and trips, fire and gas detection system, manual fire-watching.

A1.3 EFFECTIVE HAZARD MANAGEMENT

An approach is set out that attempts to integrate the principles of inherent safety into an hazard management strategy, and does this in a way that gives these the visibility and status they deserve. The overall approach is set out in Figure A1.1, and the various stages are described in more detail below.

The overall aim is to be able to reduce risks to a tolerable level, or as far as is reasonably practicable, by avoiding or reducing the hazards at source. If after this the risks still lie in the 'unacceptable' or 'ALARP', then segregation and 'add-on' measures should be used to further reduce risks.

A1.3.1 Identify the hazards

Effective hazard management relies on the identification/recognition of all the hazards that could arise during the lifetime of the process, plant or activity. This is just as important whether 'inherent' or conventional 'add-on' means of hazard management are to be applied. Since inherently safer means of hazard management affect the basic design and layout of the plant and process, these need to be considered at the earliest stages of feasibility/concept design. This requires that some form of preliminary hazard identification study(ies) is(are) carried out at this stage to identify the main hazards which will be addressed in the design.

The identification of the hazards should include all foreseeable operational modes, including start-up, maintenance, inspection, and shutdown, where the nature of the hazards may be very different, and where different safeguards may be required.

A1.3.2 Assess the hazards

The attributes, severity and likely causes of the hazards need to be assessed to estimate the risks they present and, where these risk are not tolerable, to enable designers to consider how best to avoid or reduce these hazards, or segregate vulnerable people and plant from their effects. This would typically require some scoping consequence analysis, frequency analysis and risk assessment in addition to the hazard identification studies noted above.

The assessment should also try to identify the main interactions between the design and the hazard so that this can be used to target inherent safety application.

In practice an inherent safety approach to hazard management does require a good understanding of the hazards and their causes and effects, otherwise there is a danger that the design will not be as effective at managing the hazards as was thought.

A1.3.3 Avoid the hazards

The first objective must be to try to avoid or eliminate the hazard altogether by changing the process, design, layout or activity. This then avoids the need to manage the hazard, with all its associated costs and risks. This can be achieved by avoiding the hazard itself or by designing the basic process to withstand the hazard, eg design for maximum foreseeable pressure.

A1.3.4 Reduce the hazard severity at source

The principles of inherent safety (substitution, intensification, attenuation) should be applied to reduce the size or severity of the hazard, so that its effects are limited. In some cases the basic plant layout may also provide some means of hazard mitigation eg for reducing blast overpressure.

A1.3.5 Reduce the likelihood of the hazard at source

The principles of simplification and good ergonomic design can be used to design the process or plant and its layout such that it is less prone to failures, errors or deviations. This can be achieved by reducing the frequency of the activities which could lead to failure, reducing the number of items/initiators of failure, designing the activities and items of equipment such that a failure is less likely, or designing activities and equipment so that failings are easier to detect and recover/remedy before they become an incident.

A1.3.6 Segregate

If the hazards cannot be successfully managed at source, then the next step is to try to segregate the hazards from people and other plant and equipment essential to safety. Segregation can be achieved by simple physical distance, or by the use of other less hazardous/escalation resistant equipment being used as a barrier to protect the people etc. from the hazard. A strategy could be employed where the most hazardous equipment is at one end of the plant, and the control room and living areas at the other, with plant of decreasing hazard set in-between these.

The use of fire walls or other such add-on barriers is not included in the above category. This may be a fine distinction, but the use of the basic plant layout and existing structural features of the plant is a more inherent approach than adding passive safeguards such as specific blast or fire walls which do not serve any other useful function. In some cases it may be possible to upgrade or enhance basic plant structures or walls so they can also offer some fire and blast protection..a half way house between an 'inherent' and 'add-on' approach.

A1.3.7 Passive safeguards

If the hazards cannot be successfully managed by inherent means or segregation, then some additional safeguards will need to be provided. Where practicable these should be passive systems which offer the advantages of high availability, since they should normally be present and do not rely on detection and actuation to make them work. They may still require maintenance and inspection to keep them effective, but this is generally much less onerous that for active systems.

A1.3.8 Active safeguards

These will only be effective if they can be kept in good condition, are reliable, and can be linked to an effective, reliable and timely means of detection. Such systems therefore tend to require a lot of testing and maintenance.

A1.3.9 Procedural safeguards

Procedural systems are prone to a number of failings and generally should not be used as the sole means of hazard management. Procedural systems can however usefully supplement other measures especially in hazard prevention. People are also very good at detecting hazards, but this should not be relied upon in the hazard management strategy.

Procedural safeguards should not, as a general rule, be used as the sole or main means to control and mitigate hazards, since there is a high chance of human error, or injury/hazards preventing action in such circumstances. It may be helpful in some cases to provide the means to override some engineered systems or provide means for human intervention and recovery. There may also be some cases where a combination of engineered and procedural safeguards does offer the best chance of success, especially where the operator needs to maintain a close monitoring of the system.

Procedural systems will be needed to ensure the effectiveness of any passive or active safeguards.

Procedural systems can be more effectively used to aid prevention, by inspection, testing and maintenance activities to ensure the system status is at it should be and to carry our remedial work as required.

A1.3.10 The design process and record keeping

Having noted that procedural systems are prone to failings, it is worth highlighting that the design process itself is carried out by people and requires management control. Careful attention to experience, skills, procedures and team working is needed to ensure the design is effective and meets the various performance objectives set.

The basis of the safety justification for the process and plant also needs to be recorded so that any changes in the future can be assessed to ensure they do not compromise the design and its safety. This is especially relevant where inherently safer measures have been used, as these are not so obviously visible as 'safety'. For example a proposal to remove an emergency shutdown valve would easily be recognised as having an effect on safety, whereas increasing the size of one of the heat exchangers to allow a higher throughput may not be seen as an immediate threat to safety, even though that inventory may be critical to an inherently safe strategy.

The safety case provides the obvious vehicle for such through-life record keeping.

A1.4 CONCLUSIONS

The principles of prevention, control and mitigation are often used to describe the risk based approach to hazard management. Sometimes a preference for prevention rather then 'cure' is expressed in association with these principles.

Although these ideas are sound, they can be difficult to relate to real situations where there is often a combination of these principles in use, and where some safeguards blur the categories between prevention, control and mitigation. As an example 'inherent safety' is sometimes thought of as a means of prevention, when in practice is describes an approach to prevention, control and mitigation. In fact the main inherent safety principles of intensification and attenuation rarely prevent the hazard. What they do is to reduce its severity, applying the principle of mitigation at the source of the hazard.

In the future perhaps we should be accentuating the difference between inherent safeguards and those that rely on 'add-on' systems or procedural controls. These are 'systems based' definitions, more easily related to equipment by a designer than the 'prevent/control/mitigate' classifications.

Also in principle, if the hazard cannot be avoided, it is probably better to reduce its severity first, rather than its likelihood. This implies a preference for control and mitigation rather then prevention. The advantage of such an approach is that we can generally assess the consequences of hazards with some confidence, and hence design to reduce or accommodate these, whereas identifying and preventing the causes of incidents is far more complex, involving aspects of human error and organisational failings as well as technical failings. Although much can be done to reduce the likelihood of an incident, it would be a foolish person who claims to be able to eliminate all causes. This is especially so as the plant is likely to operate for many years during which changes to plant or management regimes may occur perhaps in a way that compromises the design, or leads to falling standards of maintenance. So where a hazard cannot be eliminated, we should design to reduce the severity of the hazard to a manageable level, accepting that it could occur at some stage (even if this is remote).

This does not mean that we should not try to reduce the likelihood of the hazard. There will still be many useful and cost-effective things that can be done to simplify the design and reduce the chance of a hazard being realised, making the plant easier to operate and well as inherently safer. But we should try to limit the severity of the hazard as a first step. We might be able to make the consequence so small that we no longer have to worry about it. If we cannot do this, then we will need a combination of (preferably inherent) consequence and frequency reduction measures to manage the risks.

The approach outlined above could lead to a new way of expressing the principles of hazard management which better fits the plant situation and which highlights the role of inherently safer approaches, ie.

> replace 'prevent, control and mitigate' with;
>
> avoid/eliminate, reduce inherent severity, reduce inherent likelihood, segregate, apply add-on safeguards, apply procedural safeguards
>
> ....perhaps **'eliminate, reduce, isolate and safeguard'** for short.

The industry and regulators should consider whether this alternative statement of the principles of hazard management is worth including in their regulations and guidance either to replace or supplement the existing 'prevent, control, mitigate' principles.

Figure A1.1
Overall Approach to Hazard Management

Identify all hazards and causes of these - materials, actions, conditions		*IDENTIFY HAZARDS* ↓
Assess hazards*, their causes and effects and how these interact with the design		*UNDERSTAND HAZARDS* ↓
APPLY INHERENT SAFETY PRINCIPLES	Avoid or eliminate hazard by design	*AVOID HAZARD* ↓
	Intensify, attenuate or substitute to reduce the severity of the hazard	*REDUCE SEVERITY* ↓
	Simplify the process or plant to reduce the likelihood of the hazard occurring	*REDUCE LIKELIHOOD* ↓
Use distance, or use sections of the plant itself as barriers, to segregate/protect people and emergency systems from effects of hazards		*SEGREGATE* ↓
APPLY 'ADD-ON' SAFETY	Use safeguards that do not need initiation, and hence have high availability	*APPLY PASSIVE SAFEGUARDS* ↓
	Use active systems, but note these depend on timely hazard detection and initiation	*APPLY ACTIVE SAFEGUARDS* ↓
Operator and maintenance procedures should be the last resort, especially for control and mitigation, where the chance of error or failure is high.		*APPLY PROCEDURAL SAFEGUARDS* ↓
*Use the findings of the Hazard Assessment to estimate the risks, and target and implement inherent→segregation→add-on safeguards until risks are tolerable or ALARP		*RISKS TOLERABLE/ALARP*

RECENTLY PUBLISHED OTH/OTI REPORTS

Available from HSE Books (see back cover)

OTI 95/626	Maintenance related incidents in topside systems	ISBN 0 7176 1125 6	£7.50
OTH 94/431	Pipeline leak detection study	ISBN 0 7176 1167 1	£15.00
OTH 94/437	Extreme residual current speeds upon the UK continental shelf	ISBN 0 7176 1188 4	£10.00
OTH 94/443	Drill floor design - a consideration of human factors	ISBN 0 7176 1203 1	£35.00
OTI 95/635	A test method to determine the susceptibility to cracking of linepipe steels in sour service	ISBN 0 7176 1216 3	£15.00
OTH 94/454	Risk perception and safety in the offshore oil and gas industry	ISBN 0 7176 1239 2	£30.00
OTH 95/498	Evaluation study of models used in predicting smoke and gas ingress on offshore structures	ISBN 0 7176 1229 5	£15.00
OTI 94/623	Some calculations of fluid loading using computational fluid dynamics	ISBN 0 7176 1126 4	£25.00
OTH 95/477	Assessment of the uniformity of the interim jet fire test procedure	ISBN 0 7176 1215 5	£75.00
OTH 94/441	Isle of Grain pipeline depressurisation tests report	ISBN 0 7176 1228 7	£15.00
OTH 94/450	Kuwait scientific mission. Volume 1: Mission overview, July 1992	ISBN 0 7176 1242 2	£40.00
OTI 96/641	Kuwait scientific mission. Volume 2: Technical report, July 1992	ISBN 0 7176 1243 0	£55.00
OTH 94/460	Topside Emergency Shutdown Valve (ESV) Survivability	ISBN 0 7176 1244 9	£20.00
OTH 95/499	Review of emergency lighting and way-guidance systems for offshore structures	ISBN 0 7176 1269 4	£25.00
OTI 96/636	Offshore safety research and development programme. Project handbook 1996	ISBN 0 7176 1283 X	£25.00
OTH 94/442	A fibre optic sensor for flexible pipeline and riser integrity monitoring	ISBN 0 7176 1304 6	£35.00
OTH 96/521	Improving inherent safety	ISBN 0 7176 1307 0	£20.00
OTI 96/642	Strategy for offshore research - 1996/7 Summaries and objectives	ISBN 0 7176 1299 6	£10.00

Printed and published by the Health and Safety Executive

C2 11/96

HSE
BOOKS

MAIL ORDER
HSE priced and free
publications are
available from:
HSE Books
PO Box 1999
Sudbury
Suffolk CO10 6FS
Tel: 01787 881165
Fax: 01787 313995

RETAIL
HSE priced publications
are available from
good booksellers

HEALTH AND SAFETY ENQUIRIES
HSE InfoLine
Tel: 0541 545500
or write to:
HSE Information Centre
Broad Lane
Sheffield S3 7HQ

ISBN 0-7176-1307-0

£20.00 net