SAFER DESIGN — AN ATTITUDE

G.A. Dalzell and P.R. Willing*
Upstream Technology Group, BP Amoco Exploration, Dyce, Aberdeen AB21 7PB
*WoS-Clair, BP Amoco Exploration, Dyce, Aberdeen AB21 7PB

This paper is dedicated to the memory of Ken Paterson MIChemE who practised what we preach.

The paper examines how the design process can to be improved so that as many opportunities to reduce risk as possible are identified and implemented. It argues that the formal risk assessment approach and "making a case for safety" can result in an over-complex and retrospective approach to risk management in design. This may miss many opportunities for optimising the inherent safety. The time lag between design and analysis may leave protection against the effects of hazards as the only practical option. The formality may also divorce "safety" from the core design process. As an alternative, the paper suggests that the correct attitude within the design team will lead to a risk reduction culture where everyone asks "What's the hazard and what can we do to minimise the risks?" It questions whether we are doing enough to engender this attitude both in the design process and in our education system. It suggests that this questioning attitude should be applied both to major accident hazards and to operational activities such as pump removal which may be hazardous in themselves and the cause of a bigger incident. In the case of major accidents, this will lead to the hazard analysis becoming a fundamental design input. It shows that the participation of the designers in the analysis reveals many more opportunities to reduce the likelihood, severity and consequence. The paper concludes with a discussion on the barriers to this concept and a discussion on how its value may be measured.

Keywords: inherent safety; attitude; design; project management; safety case.

INTRODUCTION

A few years ago, a poster appeared in our offices and offshore installations. It said:

Safety is an Attitude

Safety is not something you can take or leave. Safety is not an activity in which a person participates only when being watched or supervised.

Safety is not posters, slogans or rules; nor is it movies, meetings, investigations or inspections.

Safety is an attitude, a frame of mind. It is the awareness of ones actions and how they relate to different surroundings and situations, all day, every day.

Safety is knowing what is going on; knowing what can cause injury or cause damage. It is knowing how to prevent such injury and then acting accordingly. To do this does not require genius or rank. All it requires is intelligence and understanding, coupled with the ability to use ones natural senses.

To ignore safety does not indicate bravery; only foolishness. To do things safely and correctly is the mark of a wise man, not a timid one.

It was aimed at the people who can make a difference; the plant operators, supervisors and managers. The message is clear; safety is not just compliance with rules but an underlying desire in everyone to identify hazards and to make them safe. Is the creation of a similar attitude amongst designers the key to realising the full potential of inherent safety?

BACKGROUND

The search for safer design has been ongoing since the first industrial accident which could be attributed to mechanical failure. Our codes and standards contain the history of our mistakes, oversights and ignorance. As such, they are the building blocks of safe design. Unfortunately many tell us what to do, but not why. This does not encourage designers to examine the reasons behind the requirements or to question the applicability of the code to their particular circumstances. Their unthinking application can create a culture in which compliance equals safety, and designers do not consider the hazards which the codes are intending to prevent or control. However, it does provide the perfect defence; I obeyed the rules.

Accidents such as Flixborough and Piper Alpha[(1)] showed that this approach on its own was flawed. They led to fundamental changes in legislation and the introduction of formal safety assessments. When these were first applied to new designs, safety was assured by examining the hazards, carrying out a quantitative risk assessment, and improving the prevention, control and mitigation measures which had been specified using these default codes and standards. This was performed as a retrospective process. The safety studies underlying the overall assessment were discrete activities performed by specialists after the majority of the design was fixed. The timing was such that there was little scope for minimising hazards at source. There was a danger that "proving the design was safe" and "demonstrating ALARP", would become the new compliance. Both the HSE and industry recognised the dangers and realised that there was scope for improvement. Subsequent regulations, both on and offshore[(2)] together with supporting guidance[(3)], advocated an integrated hazard management process based on an understanding of the dangers. This began to change the approach to design from a retrospective assessment culture to one in which information from the hazard analysis was used both to optimise the layout to minimise the impact on the temporary refuge, and as the basis of design for protection systems[(4).]

Although this was a significant improvement, hazards were still being managed by limiting their severity or impact, and protecting the people and plant. It was widely recognised that prevention was better than cure but the emphasis and investment still remained on control and mitigation as the benefits were numerically quantifiable. The question remained; how could a design and hazard management process be established where good design and quality equipment would be valued as the primary means of reducing risk by eliminating or preventing incidents?

The UKOOA Guidelines[(3)] had mentioned inherent safety and offered a hierarchical approach to hazard management with their 22 step life-cycle flow chart putting elimination and prevention of hazards first. Other documents[(5)(6)] had defined or categorised inherent safety and had offered examples for the offshore or process industry. There have been other initiatives to promote inherent safety such as the INSIDE project[(7)] and the Institution of Chemical Engineers CD Rom training package[(8)]. Despite all of these efforts and internal initiatives within operating companies and design contractors[(9)], inherent safety only seems to be applied in a piecemeal fashion rather than being a core activity. The question still

remains; how do we create a culture where the reduction of hazards at source is fundamental to everything that we do?

LEADERSHIP AND EXPECTATIONS

Most major organisations have an HSE management system with between 10 and 16 elements each with specific expectations. In almost all cases, the first element is leadership. We get what we ask for; from our staff, design contractors and our suppliers. If senior management takes a direct interest in safety and it is obviously considered in every one of their activities and decisions, then everyone who works with them will follow by example. As DuPont so clearly demonstrate[10], it works, and it is good business. But what about design? Leadership by project managers can be as effective in delivering safer designs as it is in ensuring safe operations. A clear statement of expectations relating to design safety, a continuous interest in the hazards, and a demonstrable commitment to reducing risks, by allocating time and resources, will set an example which will spread through the entire design and supply process. But how often does this take place and, when we do address safety, are we seen to be more interested in accidents in the design office than the product? On an offshore installation, new starts routinely meet the platform manager when they arrive in order to hear the expectations for safe operation from the top. How often does that occur in a design office, and, if it does occur, do the discussions relate to design or office safety? If the project manager asks about the hazards and seeks to find safer solutions, then everyone else will too.

It should not just be the responsibility of design managers to engender this active culture of risk reduction. As professional engineers, this should be part of our work ethic and it should be instilled into us on the first day of our studies and continuously reinforced throughout university and the remainder of our working lives. It should be an absolute expectation for Institution Membership. Arguably this is in place with the lecture series such as Safety in Design[11] produced by the Hazards Forum and the minimum membership requirements, particularly for the Institution of Chemical Engineers. However, there is still a danger that this will still be a discrete activity; the safety module. We may learn the processes such as Failure Modes and Effects Analysis (FMEA), Hazard and Operability Studies (HAZOP) and Quantified Risk Assessment (QRA) but they do not create the attitude. Again this comes down to leadership; in this case from the professors, lecturers and tutors.

WHAT IS SAFER DESIGN?

It is all very well telling people to be aware of hazards and to create safer designs but peoples perceptions of safety and the means to reduce risks are varied and judgmental. As well as creating the desire, we must give it direction. An earlier controversial paper[12] challenged the trends of increasing complexity and dependence on protection systems as the means to reduce risk offshore. It argued that this could lead to more frequent incidents and increased exposure of people to the immediate effects. Instead, it offered the vision of a safer design in which the inherent simplicity, strength and reliability of the plant minimised the both chance of a leak and the need for people to work in close proximity to the hazards. Taken to its ultimate conclusion, it suggested that protection systems could be unnecessary.

There is a current emphasis on achieving inherent safety through intensification and substitution; i.e. reducing the potential severity of an incident. This is questioned. It is an important aspect of inherent safety but surely it is better to have a plant with a larger inventory which is fundamentally less likely to leak, than one with smaller process vessels where the consequences are reduced. A plant with reduced inventories may be less tolerant of process deviation, more prone to hazardous shutdowns and start-ups, and have more instruments,

rotating machinery or other leak sites. Less than 500 kg of hydrocarbons can cause a major explosion and 1 - 2000kg may cause fire escalation. In an intensified plant, a small inventory could still lead to a major accident if the leak is not detected or the shutdown fails to be initiated. There is a hierarchy in Inherent Safety; eliminate the hazard and the cause, and thereafter, reduce the severity.

The question remains; what does the design industry have to do to if the inherently safer goal of less processing, no leaks and minimal hazardous activities is to be realised? Other papers[13][4] suggested that the maximum potential for inherent safety could only be achieved if the whole design team proactively managed the hazards. They advocated that designers should seek ways to eliminate hazards altogether and thereafter should address each cause by optimising the design so that the likelihood would be minimised. In short, they would all take ownership of the hazards during design in the same way as plant operators and managers do during operation. With every decision they make, they would ask the question***; "What's the hazard and what can we do to reduce the risks".*** This is the attitude which will deliver safer designs. It might be argued that responsible designers ask this question as a matter of course. Unfortunately there are too many incidents where there was failure to think about the hazards and identify simple changes which could have made a fundamental difference. In the Port of Ramsgate Walkway Collapse Disaster[14], there was a catalogue of design and commissioning errors but the simple addition of a ledge under the end of the walkway would have made the design fail safe at minimal cost. The real design error was that the designer didn't think about the hazards and consequences.

HUMAN ERROR

All designs have implicit requirements for operators to carry out of hazardous activities correctly or to continuously maintain and monitor the plant for critical deterioration. How much thought is given during design to the number of these activities and the ease with which they may be carried out. On the morning after a recent major accident, one commentator said, ***"It looks like human error"***. But how often did the operator have to carry out this critical action, how much time did he have to think, what else did he have to do and what were his working conditions like? How much thought was given to this when the whole operating infrastructure was developed, or did it simply evolve and did the operators have to live with what they inherited from the design? Perhaps we can expect too much from operators and maintenance staff, particularly on complex plant or perhaps we don't think about them at all and take their actions for granted. No-one is perfect and an excessive dependence on people will eventually lead to mistakes even with checks and double checks. Is the minimisation of the potential for human error one of the keys to safer design?

It is not practical to identify and examine every potential for human error during design, construction or operation as the range is almost infinite. However, it should be possible to identify and examine both critical and hazardous activities in more detail. This can be done as a whole plant overview but it will also be beneficial if individual designers undertake it for the equipment or structure for which they are responsible. It should cover not only critical activities in operation but construction, inspection, maintenance, repair and even design; anything where a mistake or omission could cause an accident or leave a hidden critical weakness. The first challenge would be the elimination of some of these activities followed by the reduction in the frequency and criticality of those that remain. This may be achieved through simplification, increasing the inherent strength of the plant and structure, corrosion resistance or taking a radical approach which might eliminate the need for the equipment altogether. The second challenge would be optimisation of the operating conditions so that the

chance of error is reduced. It may be appropriate to carry out a formal ergonomics study, but in most cases, the designer simply needs to visualise the task, conditions and workload, ideally with the help of an operator. The value of such operator input has been highlighted many times but it should be proactive; i.e. assisting the design process, rather than retrospectively reviewing the operability. Operators can be the designers greatest allies when eliminating unnecessary equipment and avoiding complexity.

ORIGINAL THINKING

Part of Safer Design is the search for a different or unconventional solution to a hazard. In many cases, these will be obvious such as the use of a stronger structure to avoid or reduce the need for inspection and repair which may require hazardous access. In other cases, the answer will require considerable original thought. Trevor Kletz identified a critical similarity between innovation and inherent safety[15]. Everyone knows that they are both critical to making radical improvements in business growth and safety respectively. Despite this acknowledgement, even at the highest levels in companies, only a small fraction of the potential is realised in practice. Where innovation has been successfully applied, as in companies such as 3M and Microsoft, there is a culture which encourages everyone to look for new ideas. They also provide a working environment with time, freedom and resources to develop and apply them. In short, they harness and apply the original thinking of everyone in the organisation, not just the specialists. They do not appear to try to measure the process, having enough faith to "just do it". Are there a lessons here for inherent safety?

BARRIERS

This all sounds like good common sense so why is it so difficult to make it happen? There may be four main reasons; the momentum of the preceding design safety cultures, time and resource pressures, safety overload within projects and the difficulty of measuring the benefit. Some of these were also identified as barriers to innovation[15]. Contrary to the views in that paper, the individual designers are not seen as a barrier and, in the cases where they have been given the challenge, resources, freedom and a little encouragement, they have found numerous ways to improve conventional designs.

Both the prescriptive or compliance culture and the Safety Case regime created large infrastructure with expectations from the clients, regulators, certifying authorities and independent verifiers. These expectations cover both the need for these monitoring and assessment processes and also for safety systems such as fire protection, or pressure relief. There is a wide range of suppliers, consultants, internal departments and service companies supporting these activities. Safety is an industry. Each particular activity has its own momentum and its practitioners have strong views about its importance and contribution. Much of what is done will continue to be needed but is it all essential if risks are reduced at source? It manages the hazards that remain after the inherent safety of the design has been optimised. However, most projects see these current safety requirements as essential, with inherent safety seen as an option or an initiative; something that is "nice to have" or something extra to achieve corporate or regulatory kudos. If inherent safety, and the attitudes required to deliver it, do not have primacy, both in importance and timing, it will deliver very little and will be overwhelmed by the "safety steamroller".

The pressure to reduce the cost and schedule of projects is increasing. Operator involvement in design is reducing and many slimmer organisations cannot spare experienced operations personnel to join a project. Safer Design cannot be achieved unless there is time to think and review the ideas. Current project schedules do not allow this time, particularly

during the front end design. The pressure on capital expenditure, when applied at system and component level may not allow investment in the stronger and more reliable plant which needs less inspection and maintenance. The process plant and structure are being designed closer to the limit so there is less tolerance of unforeseen circumstances or deterioration. As such, both the process and condition monitoring have increased criticality. Breakdown and repair will also be more frequent. However, if a holistic view of capital expenditure is taken, the potential reduction in the safety systems infrastructure, both procedural and hardware, could more than pay or the improvements in the primary plant. The main obstacle here is the public and regulatory perception that that everything that has gone before is still necessary in an inherently safer world. The benefits for future operational expenditure speak for themselves. A more reliable plant requiring less inspection, maintenance and people has to be cheaper and safer. Safer Design is good business.

Can projects take yet another requirement for safety? In the offshore industry, an immense amount of effort is needed to fulfil current expectations, particularly the delivery of the Safety Cases, supporting hazard studies, schemes of verification and performance standards. Every month or so, yet another requirement arises; a new or better type of study, further requirements for performance measurement etc. If Inherent Safety is seen as yet another requirement or imposition, it will be rejected or only lip service will be paid to it. These other expectations must be amended so that it takes primacy and replaces or reduces some of the other requirements. If the chance of a leak and its effects have been minimised, why carry out the ultimate fire or explosion analysis?

Safer Design is the search for opportunities; innovative ways to reduce risks. How can it be measured, and if the benefits cannot easily be quantified, what is the incentive to invest the time and effort? Why bother, if there is no tangible return to the deign contractor or the project? Attempts are being made[16] to measure safety in design but these can tend to focus on the hazard management process rather than hazard elimination. There are indicators such as the number of people required to operate and maintain the plant safely (also an indicator of the number of people at risk), the number of hazardous or critical activities, and the reserves of strength or capacity in the plant and structure. However, the real indicator is the attitude, knowledge and delivery of the individuals on the design team. If they can talk knowledgeably about the hazards and show how they have reduced the risks, this is the best indicator that the process is working. As operational safety in discovering, its the attitudes that count just as much as the numbers.

CONCLUSION

- Inherent Safety, and the attitude required to deliver it, needs primacy over “traditional” safety requirements if it is to deliver.
- It is an attitude which should be instilled during our engineering training, possibly even in school and it needs to be reinforced by leadership and example throughout our working lives.
- To be able to create and deliver inherently safer designs, we must effectively challenge our own, the public and regulatory perceptions that all safety features and processes which have gone before are still necessary in an inherently safer world.
- Design safety is analogous to operational safety. Every designer has as much responsibility for plant safety as the operators.
- The full potential for Safer Design can only be achieved if every member of the design team actively seeks to understand the hazards and to improve the design to reduce the risks.

- It will only deliver results if there are the time and resources to think of safer options and implement them.

Looking back to the original poster, here's an offering as applied to design:

Safer Design is an Attitude

Safe Design is not something you can take or leave. Safer Design is not a separate task, nor is it restricted to those activities which are checked or reviewed.

Safer Design is not only codes and standards, compliance, studies or formal risk assessment,

Safer Design is not someone else's responsibility.

Safer Design is an attitude, a frame of mind. It is the awareness of ones decisions and how they relate to different surroundings and situations on the plant for every day of its life.

Safer Design is knowing what will go on; knowing what could cause injury or damage. It is knowing why accidents happen and changing the design accordingly. To do this does not require genius or rank. All it requires is intelligence and understanding, coupled with the ability to use ones common sense.

To ignore safety during design is to pass by on the other side. Finding a safer way is a mark of a creative and caring man, not a selfish one.

REFERENCES

1: The Public Inquiry into the Piper Alpha Disaster; HMSO publications
2: The Prevention of Fire and Explosion, and Emergency Response Regulations; SI 743, 1995
3; Guidelines for Fire and Explosion Hazard Management; published by the United Kingdom Offshore Operators Association (UKOOA)
4: Fire and Explosion Hazard Management in the Chemical and Hydrocarbon Processing Industry; Safety '98, I Chem. E Interactive Conference; Crawley, F.K.
5: Improving Inherent Safety; Mansfield D.P., Poulter L., Kletz T.A.; UK Health and Safety Executive Offshore Technology Report OTH 96 521
6: Inherently Safer Design; The Growth of an Idea; Kletz T.A.; IBC Inherent SHE Conference; London 1997
7: The Inside Project - Inherent SHE in Design; Mansfield D.P., IBC Inherent SHE conference, London 1997
8: Inherent Safety CD Rom Training Package; I. Chem. E.
9: Guide to Inherent Safety; Brown and Root AOC internal publication
10: Du Pont Safety Management System and STOP programmes
11: Safety in Design, an Engineers Responsibility for Safety published by the Hazards Forum
12: Nothing is Safety Critical; Dalzell G. A., Chesterman A., Hazards XIII Conference; I. Chem. E.; 1997

13: What Makes an Inherently Safe Platform; Dalzell G. A., OMAE Conference, Lisbon, 1998
14: Port Ramsgate Walkway Collapse Disaster;; Crossland B., Joel S.J, Norton G., Underwood J.; the 71st Thomas Lowe Gray Lecture; Institution of Mechanical Engineers
15: The Constraints on Inherently Safer Design and Other Innovations; Kletz T. A., Process Safety Progress Vol. 18. No1, Spring '99
16: Development of Indicators for the Effective Management of Health and Safety during Offshore Design; SPE 56984