NOTHING, IS SAFETY CRITICAL

Graham Dalzell and Alan Chesterman
BP Exploration, Aberdeen

The views expressed in this paper are those of the authors. They are not necessarily the views of BP.

Do many safety systems add a nett benefit? They can result in higher manning levels and increased personnel exposure, more breaches of containment, complexity, congestion, and many other contributors to risk. Legislation and public perception have driven the offshore and chemical industries towards control and mitigation as the primary means to manage major accident hazards through the inability to quantify the contributions of good design and operation as the primary prevention measures. Are the risks on site with only the bare essential of control and mitigation systems equal to those that follow current trends? If the resources which have been previously devoted to the *purchase and upkeep of these systems were devoted to designing and* operating the plant safely and with the minimum of people and activity, would the result be a cheaper, safer plant? In other words, is it the case that Nothing, is Safety Critical? This paper examines these questions and takes a fresh look at risk management.

Key words: Inherent Safety,

INTRODUCTION

The offshore and major petrochemical industries have made major improvements in safety performance over the last 50 years. Of particular note are the following;

- a better understanding of the hazards by designers and operators
- improvements in design codes
- corrosion resistant materials
- the enhanced and more focused monitoring of technical integrity
- improvements to layout
- the use of HAZOPs to identify causes of failure
- improved arrangements for isolation
- the use of more competent personnel.

Added to these improvements in prevention measures are the much more obvious improvements to protection systems; process control and shutdown; depressurisation; fire and gas detection; deluge; passive fire protection etc. However, we have not seen a step change reduction in the quantified risks to the personnel on new installations.

Why?

One of our newer platforms gave several clues. The number of potential leak points on the process plant had doubled compared with an older design and the congestion had increased thereby exacerbating the explosion overpressures. We also

discovered that the people with the highest individual risk were the fire and gas technicians who spent most of their working time in some of the least accessible, and most hazardous locations of this plant.

Have we reached the point where our efforts to build a safer platform have simply created a better protected but more hazardous one? This paper asks the question "Is Nothing, (comma) Safety Critical?"

WHAT DO WE MEAN BY "NOTHING"

The UKOOA Guidelines on Fire and Explosion Hazard Management introduced the concept of *Interactions*. Perhaps this isn't the best term but they are defined as *"Characteristics of a system which may introduce a new hazard, increase the frequency of an existing hazardous event or reduce the effectiveness or reliability of another safety system."* It should also have included increasing the exposure of personnel to hazards. Whatever the name, it is the concept which is important; that the presence of a safety system may introduce new and significant risks. The questions are; " *what are those risks and do they outweigh the benefits?*". *If the answer to the* second half of the question is yes, then it is better to have nothing. Let's look at the attributes of having "nothing" and what we would have to do to the design so that we could live without these safety systems:

No instruments:

Process instruments; level indicators, pressure gauges, sight glasses etc. have blossomed on process plant, particularly following enhancements of design codes and the introduction of HAZOPs. Almost all are intrusive, i.e. they require direct contact with the process fluid and need regular removal for testing with consequent breaches of containment and multiple flanges or joints associated with double block and bleed. These instruments and associated tappings may be subject to inadequate reassembly and are vulnerable to damage, both from routine and non routine activities. The use of instrumented process safety systems for the protection of the plant will also lead to an increased number of shutdowns and start-ups which are themselves hazardous activities. Instruments may also be susceptible to the weather related water ingress and corrosion, so louvres may be needed to protect them and these inhibit ventilation and increase explosion overpressures.

Clearly, it will not be possible to eliminate instruments entirely but it would certainly be possible to minimise the numbers and to convert most of those that remain to a non intrusive type. This can apply to level, pressure and temperature. Many instruments have been duplicated because of their perceived unreliability and the consequences of their failure. It would be better to build a fundamentally more robust plant; one which is more tolerant of process deviations and less susceptible to failure. This may mean larger inventories which contravenes one of the principles of inherent safety but this may be one of the dilemmas which we need to resolve during design; more leaks or fewer, more prolonged leaks. A smaller inventory may not mean a smaller fire, only a shorter one. In many cases the smaller inventories may still have

almost the same potential for escalation as the fires, although of shorter duration, would still last long enough to cause failure.

No Pressure Relief Systems

Heresy! We can't live without pressure relief systems: Or can we? At least one major catastrophe has been attributed to the failure to correctly install a blank flange while a relief valve was undergoing routine testing. As with instruments, the presence of these valves leads to regular breaches of containment and potential large bore releases. By their nature, they must be installed at the highest point of the plant. They invariably require permanently installed access ladders, walkways and hoists which increase congestion and explosion overpressures. The valves, associated piping and the walkways also inhibit optical fire and gas detection systems. Relief valves are not lightweight and are a classic dropped object which has sufficient kinetic energy to shear instrument tappings. The operation to change out relief valves invariably requires people to ascend to the highest and least accessible parts of the plant. People in these locations take longer to escape and would be more vulnerable to an incident in the area. Clearly those personnel changing a relief valve may be at particular risk if an incident were to occur on the plant, especially if the incident was related to this particular activity.

Pressure relief is installed for three reasons; the inherent weakness of the plant to withstand pressure deviations, thermal relief due to increased temperatures caused by the processing, and fire relief. It may be possible to use instrumented control in place of relief systems but this may bring as many problems as it solves. It should be possible to build a robust plant that can withstand all the pressures associated with the processing. It would be expensive. However, the increased cost might be justified. The potential savings which are often excluded from the equation are those for the relief systems themselves and the other safety systems to deal with fires or explosions if these regular breaches of containment are not carried out effectively.

In the case of fire relief, passive fire protection could eliminate the need, but again, it can have drawbacks such as increased corrosion and restrictions on inspection and non destructive testing. It takes some time before the temperature will rise to cause a problem. Stronger plant will take longer to fail and this time can be further increased by the choice of materials. This could reduce the chance of rupture and allow personnel to reach a safe place. Is it better to minimise the chance of leakage and resultant fires than to add relief systems which are, in themselves, one of the primary reasons for breaches of containment and causes of leaks? After all, if the plant doesn't leak, then there is no need for fire relief.

No Emergency Shutdown (ESD) Systems.

Emergency shutdown systems cause two major hazardous activities; shutdowns and, indirectly, startups. They also require increased numbers of flanges and these need to be of a type which will allow valve removal and these are inherently more prone to leaks. The valves require additional piping and space. This results in additional inventory, longer pipe lengths, congestion in the plant and larger modules. These give

longer fires and bigger explosions. ESD valves ought to be tested both by observing the full travel of the valve and by checking the leak tightness. Both require people to be out on the plant and the testing requires instruments and possible breaches of containment. One of the more hazardous activities offshore is the leak testing of the riser ESD valves in compliance with SI 1029. The operator is required either to determine a maximum acceptable leak rate through the valve or to accept a default value and to measure these rates at regular intervals. In some cases this has required the connection of devices to collect and measure the liquid in some of the more inaccessible, hazardous and awkward areas of the platform such as the splash zone.

Of course we need to be able to shut down the plant quickly and effectively but do we need a specific system with its own control panel and dedicated valves? The purpose of the ESD is twofold; to stop a hazardous process deviation and to limit the severity of a hazardous event such as a fire. In the first case, the more robust type of plant described above will be more tolerant of process deviation and the standard process control valves may have both adequate reliability and performance such as leak tightness. Where the standard choice of valve may not be adequate, better ones may be available or could be developed. It should also be possible to specify fail safe process control valves.

Shutdown for gas leaks or fire is intended to minimise the quantity which is released. However, it only makes a significant contribution if it limits the inventory to that which would be unlikely to cause escalation. It does not reduce the initial rate of release, the scale or intensity of the fire or explosion. Examination of typical Safety Cases showed that only a proportion of the ESD valves made a significant contribution to reducing the risks. Typically, the critical ESD valves are the wellheads, riser ESD valves and separator outlets. Clearly, the first two are essential but the separator and other process isolation is already duplicated by level control or other process valves. These normally have adequate leak tightness to act as ESD valves in this duty. Many process valves are pneumatically operated and close on loss of supply pressure so the use of pneumatic tubing on each valve or fusible plugs throughout the supply could cause them to close during a fire.

No Emergency Depressurisation

Emergency depressurisation requires additional valving and leak sources on the live operating plant. It also needs extensive piping , knockout vessels and liquid return pumps; all potential sources of secondary failure during an incident. Rapid depressurisation causes rapid cooling with the associated hazards of embrittlement, liquid dropout, slug flow and hydrates. As with other systems, the additional plant increases the congestion and the size of the modules giving higher explosion overpressures. Depressurising the plant significantly increases the difficulty of the restart following an emergency shutdown and the associated hazards.

Emergency depressurisation should not be necessary to control a process upset condition providing that the plant is sufficiently robust. Depressurisation reduces the duration, but not the initial size of a gas cloud. Arguably, it may reduce the probability of a severe explosion but only those which might have ignited after a significant time

delay. It also reduces the release rate and intensity of liquid releases and this can give a significant reduction in the severity and escalation potential of such an event. Again, this is a case of prevention or cure, and if the plant doesn't leak or deviate into unacceptable process conditions, emergency depressurisation isn't needed.

No Fire and Gas Detection

Fire and gas systems have seen the greatest development in technology and in the extent and sensitivity of the systems. What started as simple systems which, in the case of fire, were reliable but relatively insensitive have blossomed into highly complex arrangements with numerous detector heads festooned throughout every corner of the plant. Arguably, this complexity has brought sensitivity but not necessarily reliability. However, it has also brought extremely onerous requirement for cleaning, maintenance, inspection and testing. Again, this brings permanent ladders, or of more concern scaffolding, to gain access. Ironically, this reduces the detector coverage but it also hinders good ventilation, increases congestion and, in the case of scaffolding, provides excellent missiles for explosions. However, the most severe drawback is the exposure of the maintenance personnel for these systems. As mentioned in the introduction, these people spend most of their working time offshore within the hazardous modules, often at high level where it is difficult to escape rapidly if an oil or gas release should occur. They are at greater risk from the smaller, more frequent, events than almost any other person on an installation.

The Fire and Gas detection performs two roles; the warning of a gas release or fire so that personnel can respond and muster, and the initiation of emergency systems such as ESD, depressurisation and firefighting. If these systems are eliminated from the design, so is the need for their actuation by the detectors. This leaves the need to have systems to alert personnel about gas releases or incipient fire conditions. This is critical with a normally manned installation during those times when personnel would not be out on the plant but in enclosed control rooms or asleep. It is less critical on a not normally manned installation when the only personnel on the installation are those operating and maintaining the process plant. In reality, it would be unreasonable to do without some form of fire or gas detection as personnel must always take a break. Access to an unmanned installation must always be confirmed as safe before arrival. However, the current complexity could be significantly reduced and the level of sensitivity limited to that indicative of a severe incident which will require evacuation; i.e. perimeter detection. In the case of fire, it might be integrated with the pneumatic supplies to the control valves. As with other systems, it is only needed if the plant leaks.

No FireFighting Systems

Few of the Safety Cases have taken much credit for the deluge systems for several reasons; its behaviour in module fires with pressurised fluids is only just becoming understood; it is highly susceptible to explosion damage, attempts to provide redundancy have increased that vulnerability, and finally, it is not considered to be reliable with a history of nozzle blockage. To be reliable, the systems require frequent maintenance and, again, this leads to extra manning on the installations, particularly in

the modules. The systems also add to the congestion particularly where scaffolding is needed for maintenance. Deluge systems require function testing to ensure that they are effective. The systems use salt water and in the past, this has lead to corrosion under insulation with near catastrophic results. The water also enters flameproof instrumentation causing corrosion which may lead to a failure to detect hazardous process deviations.

Deluge systems have three roles; the prevention of escalation, the reduction of fire severity to allow evacuation, and the protection of the asset. If the personnel are physically protected from the immediate effects and can evacuate before escalation takes place then deluge only contributes to asset protection. Deluge systems are very expensive, particularly when multiple firepumps, ringmains and the associated platform space is taken into account. Could the funds not be better spent ensuring the technical integrity of the plant thereby giving more effective asset protection?

Other firefighting systems such as gaseous extinguishing systems in switch and control rooms have been shown to offer negligible contribution to saving life when critically examined as part of a halons reduction programme. Even in gas turbines, isolation of the fuel and arrangements to stop the build-up of oil in insulation and on the floor should be sufficient to minimise the fire load so that we may be able to do without the fixed systems.

No Unnecessary Processing

We normally accept the requirements for process design without question, particularly requirements for accurate fiscal metering, oil, water and gas quality. However, these all require more elaborate processing resulting in additional inventory, instrumentation, joints, congestion and maintenance requirements. They may also require particularly hazardous operations such as sampling. We also accept duplicated processing, standby pumps and compressors, recycle loops and manifolding for flexibility. Many of the earlier designs did not have these features yet they managed to produce oil safely and reliably. This increased process complexity has made plants more susceptible to unwanted shutdowns and more hazardous startups. Again, this adds to increased operator requirements, maintenance, congestion and personnel exposure.

Perhaps we should question the need for these high specifications. It may be acceptable to tolerate a lower quality product and to have additional processing onshore. There will be economic arguments for maintaining the status quo but these should be balanced against the safety impact on the platform.

No Maintenance or Inspection Requirements.

Maintenance requires people. People can make mistakes and they, and others, could be involved in fatal accidents. A good example is road maintenance. A poorly specified road requires continual attention with consequent hazards to the maintenance personnel. If they are killed or injured, perhaps the designer should share some of the blame.

While it will not be possible to totally eliminate maintenance, by ensuring that inherently robust and reliable plant and fittings are chosen, it can be reduced significantly. Whether a paint system or a pump; you get what you pay for. With the experience of the conditions in the North Sea, it should be possible to purchase plant which does not need regular attention. It may be better to do without some of the ancillary features and to concentrate the investment on the basic design and materials. Some installations are using materials for the fabric which are inherently corrosion resistant such as stainless steels and glass reinforced epoxy resins. Paints with a 20 year life are available but are rarely used. The reason; the capital cost. Only when the real benefits of a maintenance free system are realised will sufficient capital be invested. These benefits include fewer people, reduced support facilities and simpler systems to protect them with the consequent lower risks to life. It may be the maintenance philosophy which makes the difference between a manned and an unmanned installation. Once an installation is permanently manned, then there is a need for accommodation, fire resistant temporary refuges and the usual extensive provision of the safety systems listed above.

No Activity

Activity leads to three things; occupation of hazardous areas with consequent exposure to these hazards; activities which could cause or exacerbate incidents; and high workloads. The first two have been covered in detail above. In the third case, it should be recognised that a high level of activity means that supervisors may have to monitor a number of activities and different groups of people at the same time. If there is so much going on that one individual cannot supervise everything or there are concurrent activities, then there may be an increased risk of mistakes. The same applies to the design and construction process. With simper designs and fewer systems, it becomes much easier to focus on the control of activities and the technical integrity of the plant. Again, any reduction in the provision of the systems and activities listed above will have a beneficial effect.

No Visits

Visits to the installation by operators, maintenance personnel, auditors, visitors etc. involve helicopter flights. This is recognised as one of the primary risks to life. It has been recognised that personnel who visit number of not normally manned installations and have a high number of flights are some of the most exposed in the industry. The other risk is that of the helicopter crash onto the platform leading to a fire or other incident on the installation.

While it is impractical to have an installation which could function without any visits, their minimisation could be addressed in the conceptual design. Again, a robust design which needs little maintenance and is less susceptible to unwanted shutdowns will minimise both planned and additional visits.

No Modifications

Major modifications are obviously one of the greatest sources of hazards on an operating installation. They can include all of the activities listed above such as heavy lifts and scaffolding and it also exposes large numbers of people to the increased chance of a hydrocarbon release. Modifications will often increase risk by adding additional processing. They also usually undermine any initial attempts at creating an inherently safe installation; for example, increasing the congestion. There can be design compromises with higher dependence on instrumentation and requirements for installation with flanges rather than welded joints if hot work is to be avoided.

Why are modifications needed? There are a number of possible reasons; a poor statement of requirements by the future operator; a lack of foresight by the design team; an overeagerness to reduce initial capital expenditure; a lack of flexibility in the design to absorb the unpredictability of the reservoir conditions; and a desire for change or improvement. A thorough assessment of the lifecycle of the operating plant during design would provide one which is less likely to require change. Input from operational personnel will identify future requirements and design inadequacies. If both the capital cost and the long term operational expenditure are given equal consideration during the preparation of the plant specifications, then the potential for failure and subsequent modification can be minimised.

No People

All of the above focus onto this concept. If no one is on the installation, they cannot make mistakes which cause incidents and they cannot be harmed if things go wrong. This is the aspect of inherent safety which has been overlooked. Is in not fundamentally wrong to design or operate a hazardous plant which requires unnecessary personnel to work or live on it? As well as direct exposure to an initial hazardous event, larger numbers are more at risk from an escalating event as it takes longer to muster and evacuate. More safety systems are needed to control this escalation and in turn, these systems need even more people. This is how we enter into an increasing spiral of manning and increased risk.

IS "NOTHING" POSSIBLE ?

Probably not, but a minimum provision might be achievable. The biggest problem is the mindset amongst designers, operators, and the authorities that the only way to make a plant safer is to add systems to it. The Safety Case regime promotes the risk based approach but, unfortunately, it is easier to quantify the contribution of control and mitigation systems rather than prevention. As a result, it has perpetuated the over concentration on them as the primary means to reduce risk.

To an extent, the minimalist approach has been promoted through the use of Not Normally Manned Installations (NMMIs) and some of the smaller gas platforms have achieved the goal of minimum manning through minimum facilities. However, there is a presumption that the extensive provision of safety systems is necessary once a platform reaches a certain size and there is a step change in complexity and manning.

Recent attempts to build platforms with lower numbers of people have failed with the accommodation proving to be too small to allow maintenance and modifications to be carried out. This, in part, is due to inadequate specification in the design and over complexity. In other cases, it has proved to be impossible to operate and maintain the platform within the tight manning the criteria for an NMMI. As a result, extensive systems have been perceived as necessary to reduce the risks to those on board, further increasing the numbers.

However, the first major oilfield in the North Sea, with peak production in excess of 500,000 barrels per day was originally designed to be unmanned with the main control room in Aberdeen. The original process equipment is characterised by its simplicity. It was based on the approach in the Gulf of Mexico. Examination of their current generation of platforms shows that they have managed to retain their simplicity and, if they are manned at all, there are at most 10 personnel excluding the drilling crews. They have managed to resist the drive for increased complexity and extensive protection systems but, in doing so they have not put their personnel at undue risk. They do have the advantage that escape to the sea is a much more realistic option and, with only 10 people to rescue, a single helicopter, can evacuate them all. Perhaps, this is the way forward for the North Sea; minimise manning, invest in plant integrity rather than in detection, control and mitigation systems and ensure their survival through an effective mustering and evacuation system.

This should be achievable at the same cost as a current design. Arguably, it may be cheaper but it is not the aim of this paper to reduce cost; rather to redistribute it in order to reduce the likelihood and severity of hazardous events and to minimise the number of people exposed to them. If savings are redistributed first into the quality, training and competence of personnel designing and operating the plant, secondly into the design standards, simplicity, robustness, reliability and longevity of the process plant and structure, and thirdly into the assurance of its initial build quality, then the chance of any incident occurring in the first place must be significantly reduced.

Arguably further expenditure to preserve the plant and assure the safety of personnel might not be cost beneficial. However, given that the industry has chosen to invest extensively in control and mitigation, it should continue to invest in the preservation of life and, in doing so, to further raise our standards. This may be through a step change in our thinking on evacuation systems or the provision of even safer refuges. It may turn out to be economic to use twin jackets on a marginal field but only if the minimalist approach on other safety systems is adopted. Alternatively the conventional approach of lifeboat evacuation has dictated the investment levels for such systems and this has limited their potential effectiveness. A step change in investment could encourage the development of systems which could be usable, safe and effective in the severe weather conditions of the North Sea. If only 10 to 15 people rather than 150 need to be evacuated, then there should be no reason why practical options could not be developed.

The switch to this inherently safer design with minimum manning will not be achieved if there is an initial presumption that traditional systems are needed. It must start with a design which only has a robust and simple process plant. Other safety

systems should only be added if the analysis of risks shows that they are absolutely necessary and that there is no other way of safeguarding the personnel on the installation. Even when they are added, they should only have the minimum of features necessary to deliver the essential performance and, as far as possible, they should be maintenance free.

CONCLUSIONS

It is possible that the petrochemical industry, in particular the offshore sector, has been taking the wrong approach to safety. In adding safety systems it may have reduced the risks from specific hazards but has created an infrastructure which has a higher chance of an accident and exposes more people to its effects. This infrastructure is so expensive that it may jeopardise the development of many marginal fields in the UK. In comparing different development options as required by offshore legislation, one than must be considered is that with minimal facilities, few people and a high integrity robust plant; i.e. the option where all the safety investment is directed towards *prevention*.

Should not every designer or operations manager ask the question "Does what I have asked for, or added to the installation increase the number of people offshore?" If the answer is yes, as it will almost invariably be, then they should ask; "Is it essential to production or safety and could it be achieved in another way which does not involve sending people offshore?". If it is a safety system, does the hidden increase in risk outweigh the direct benefits? If so, Nothing, is Safety Critical.