PROCESS SAFETY - WHERE DO WE DRAW THE LINE?

Eileen Blackmore, MIOSH, AIRM, RSP.
Eli Lilly and Company Limited, Speke Operations, Fleming Road, Merseyside L24 9LN

Legislation by both the Health and Safety Executive and the Environment Agency are focusing the attention of industry on ensuring that their processes are safe in terms of their employees, the public and the environment. This means that safety must be built in and not bolted on - an old but important concept for any project. However, companies are continually challenging engineers to provide cost effective solutions when designing processes - and safety reviews mean cost in both time and money.
Are the traditional methods of design reviews and HAZOP as effective as they should be or are we just 'following procedure' – and, if this is the case, where do we draw the line?

Keywords: cost effective. design reviews, HAZOP, inherent safety, procedure,

INTRODUCTION

As the Health and Safety Adviser of a bulk manufacturing pharmaceutical company I have participated in many design reviews and HAZOPS and have become increasingly uneasy about the fact that more attention appears to be paid to the detail of this process than to the inherent safety of the plant under consideration.

Safety throughout the life of the project in design, construction, operation and decommissioning will depend on the standards applied, the experience of the engineers and the budget set by the company. All these factors influence where the line is drawn on process safety. The consequences of not considering what is below the line may potentially effect people and the environment.

My paper, which gives a health and safety practitioner's view of engineers and how they manage process safety, looks at these issues and is then directed towards a model which focuses on the three key areas of process safety management; managing risk, managing change and maintaining the integrity of the system

USING A PROJECT ROADMAP - SIGNPOSTS FOR INCORPORATING PROCESS SAFETY

When any project is conceived there is a chronological order of stages which it must go through up to completion. At each of these stages the question of 'how safe will this process be if we do x, y or z?' or 'where do we draw the line?' must be answered.

This project 'roadmap' sets the direction of the project and should incorporate at each stage a review of the health, safety and environmental aspects of the project. The extent and detail of this review will depend on the stage of the project and other factors.

CONCEPTUAL AND SCHEMATIC STAGES

The first stage in the roadmap is at the conception of the project. It is here that the proposed project will be selected or rejected on the basis of business needs.

Business strategy and project requirements. A project is conceived either for a new process or when an existing process requires an upgrade or change. The driver however must be in line with the overall business strategy. If a functional unit of that business raises the project then the needs of that functional unit must also be in line with that business strategy.

To ensure that this business process works, most larger companies plan ahead. Short term (up to one year) and long-term (3 to 5 years) business plans form the basis of the company's strategy and should thereby ensure that sufficient time is available for safe, strategic decisions to be made.

It is unlikely at this conceptual stage that any formal detailed safety review will take place and 'ball park' figures for capital (in the order of +50% -30% for projects in the short to long term plan) will not be based on add-on safety measures. However, for safety to be built in to the project and to *reducing risk at source* the philosophy must be one of *inherent safety*. This meets the principles underlying The Construction (Design and Management) Regulations 1994 (CDM). It is also start of the process safety line being drawn.

Conceptual and schematic design. To further develop the business case for the project, a preliminary assessment of any environmental or health and safety issues would consist of a review of, for example;

- an outline of the process
- the other options considered and the basis for rejection
- siting of the process
- chemicals to be used, stored and transported and their by -products
- impact on utilities
- relevant statutory requirements and company standards
- waste produced and environmental effects
- the consequences of failure

Depending on the location and size of the project additional consideration should be given to the reaction of the public and non-government agencies to the plan. Getting buy-in from neighbours is almost a 'given' for any activities associated with the chemical industry.

DESIGN STAGE

When this stage is reached sufficient information should be available to perform a more detailed assessment of potential health, safety and environmental factors arising from the selected option. Here the intention is to optimise the designs in terms of ensuring that risks are reduced to as low as reasonably practicable. Unless the inherently safer option has been chosen this process may give limited reduction in risk and even prove to be a mitigation process. The process safety line has been drawn.

Design and capital approval. The output expected at this stage would be a documented review including; a description of the process, process flow diagrams, P&ID's, mechanical, electrical, control and instrumentation systems, and any other process safety information. Importantly, all engineering controls should be identified. In other words, sufficient detail to allow informed decisions to be made so that capital can be approved and for the process safety roadmap to proceed to the next stage. The decisions made here affect how safe the process will ultimately be and some of the critical aspects of this stage are;

- the use of programmable systems
- the impact of the design on existing plant
- selection of construction materials

Use of programmable systems. Where programmable systems are to be used to control the process it is essential that the appropriate people are included at this stage of the review. Control and instrument engineers will obviously have had an input into the design but they will not be operating or maintaining the plant.

The increased use of programmable systems is the result of a number of factors; advances in technology, the conscious removal of operators from sources of risk and the trend towards 'downsizing' and 'one operator' plants. The result is operators who are no longer in tune with or even understand the actual operation of the plant. Gas detectors may not give the appropriate coverage whereas in the past the operator would have been on the plant discovering the leak himself. In other reported incidents the set up of displays on the operators control system meant that they were unable to diagnose problems.

Major causes of incidents relate to the use of inhibits. At process start up for example, inhibits are used when vessels are being filled. Plant operators quickly learn to over-ride or cancelling inhibit warnings, therefore a thorough risk assessments of the inhibit system must be carried out and appropriate control measure adopted. In addition, operators must be trained to understand the consequence of over-riding multiple alarms often for long periods of time. As a simple example, inhibiting a high level alarm in a knock out drum ca result in liquid carry over into a flare line or into the next stage of the process.

Impact of design on existing plant and equipment. The safety requirements for designing new plant in a new building will be very different to what is needed when new plant or equipment is to be introduced in an existing plant. The boundary drawn for the new project can have an impact in terms of safety as can the location of the planned project, for example, finding that the siting a new plant carrying flammable substances is in close proximity to electrical installations.

Where old and new plant are joined by a new project different hazards can be found. Significant sources of hydrocarbon leaks in chemical plant arise from small-bore pipe work fittings. This is exacerbated when the fittings on the new plant are different to the fittings on existing plant. After a time the fittings become exchanged and leaks occur. The consequences of the leak will depend on the properties of the substance e.g. flammability, toxicity, corrosiveness etc., the quantity leaking and the environment in which the leak occurs.

Materials of construction. Once construction has commenced it is too late to start assessing the suitability of materials selected. Compatibility of materials of construction and the chemicals with which the plant will be in contact is usually well considered but what if the

project involves the construction of a building or delivery access for new plant other than at ground level? The Health and Safety Executive (HSE) are currently focussing on falls through fragile rooflights however, the only absolute means of prevention is elimination of the hazard. This can be achieved through designing plants with other safer location for lighting or, if this is not possible, then by specifying the use of less fragile material for flat roofs. Designers play a key role by specifying material that ensure the inherent safety and reduction of residual risks of the new plant and building.

CONSTRUCTION STAGE

Unless well managed, the construction stage of the project is likely to be the biggest source of risk and hence potential additional cost. This can actually effect the line that has been drawn for process safety by corners being cut and though poor management of contractors.

Construction requirements. Provided that the selection of materials for the project has been satisfactory in terms of safety, the construction materials of buildings and plant are usually given adequate cost estimation at this stage in the project. However, what will add to the cost of the project and is often overlooked, is the *way* that the construction will be carried out. Direct cost *and risks* are found in the demolition, removal and safe disposal of redundant plant, the need to hire cranes and the provision of access to other parts of the site. Indirect cost can arise from delays in completion of the project if there is public reaction to the unconsidered environmental consequences of, for example, noise and dust.

The management of contractors of different disciplines at the different stages of construction whilst, in some instances continuing production in other parts of the plant, presents a challenge. Here, the introduction of CDM has proven to be both a curse and a blessing to the project engineer.

The construction industry has acknowledged these problems in their ‘Working Well Together’ campaign. This is an attempt to improve safety performance by focussing on co-operation, communication and competency to achieve best practice. This will benefit both contractors and clients through the timely and safe delivery of the project.

PROJECT COMPLETION AND BEYOND

The final stages of the project roadmap i.e. commissioning, validation and the ‘in house’ requirements of documentation, training and asset care are equally important to the project. If the previous stages have delivered a product that meets the client’s requirements and includes the principles of inherent safety, then the project will have been successful. A further consideration however, is that one day the plant will reach the end of its life or usefulness to the company.

Decommissioning should entail as safe a procedure as building the plant if the fundamental differences between putting a plant together and taking it apart have been considered in the design. The decommissioning project should mainly be concerned with the residues of substances, intermediates and by-product resulting from the process that may be left in pipe work and vents rather than the removal operations of a crane.

Fast track projects. Before leaving the project roadmap, a word of caution! The value of a roadmap approach to projects can clearly be seen, but sometimes, in an attempt to get ahead of the market and regardless of the size of the project, time scales can become compressed. These so called 'fast track projects' can result in ordering equipment at conceptual stage without knowing detailed design and then making modifications when it doesn't quite meet the needs of the process. An example would include reactor vessels being ordered before the process dynamics are fully understood. With fast track projects the chances are that process safety will always fall below the line.

DESIGN REVIEWS AND HAZOPS - HOW TO AVOID THEM BECOMING A PAPER EXERCISE

There has been no mention made thus far of the HAZOP. This would take place ahead of the detailed design and implementation stage with the intent of designing out any hazard. Chemical engineers are trained to carry out a HAZOP and sometimes familiarity does breed contempt. The exercise becomes a mechanistic ticking the box exercise forgetting that the purpose behind the 'guide word' approach to HAZOP requires certain questions to be borne in mind;

1. Have all hazards inherent in the process or activity been identified?
2. Have those credible failures, both human and /or equipment that could lead to accident scenarios been identified?
3. What are the risks in terms of likelihood and consequence of those scenarios?
4. Can changes be made to the design and/or operation of process conditions to mitigate those risks?

Operability. The result of a HAZOP should be a plant that is capable of being operated without latent risk. The problem is that the project designer sometimes forgets to include the operator in the HAZOP process resulting in tasks that are often an ergonomical challenge. Then, changes or modifications have to be made to make the plant easier to operate, the original design requirements and basis of safety being forgotten.

It is of little value ensuring that a HAZOP is carried out if the initial design budget has not allowed for operators to be released from their work to provide their valuable input HAZOP. As stated earlier, budget is a major factor in where the process safety line is drawn, but so also is the quality of the HAZOP.

THE HUMAN FACTOR AND ITS EFFECT ON THE DESIGN PROCESS

Engineers usually have their own preferred way of designing plant reflecting either training or their experience in another industry or place of work. This can exhibit itself in plant that;

- has an excess of safety devices, or
- a deficit of safety devices

Some engineers, and even safety professionals, are of the opinion that the more safety devices the better. However, apart from increasing the overall cost of a project and increasing risks from maintenance intervention, plants with an excess of safety devices can prove difficult to operate. This belt and braces approach often leads to many of the safety controls being bypassed or over-ridden once the operator has worked out that the job can run quicker

without them. The problem then is if the particular device bypassed is the one that is critical to the safety of the operation the consequences could be serious as seen in the Paddington Rail disaster with the use of the Train Protection Warning System.

At the other end of the scale, as the result of either budget constraints, lack of experience or to prevent having to make too many changes to the original design, process engineers design plants that using procedures rather than hardware as means of control. This works well until a distracted operated turns the two-way valve from chilled water and acid lines the wrong way, again with potentially serious consequences. The HAZOP intended to remove hazards then potentially introduces a different hazard - human error of judgement. The answer must lie in designing inherently safe plant and including operators at the earliest possible stage in the project.

ACTIONS ARISING FROM HAZOP - PROCEDURAL *V* HARDWARE SOLUTIONS

The HAZOP process forces the HAZOP team to challenge the safety of the design. This challenge requires that certain questions are answered and that the solution ensures safety of operations and does not compromise the inherent safety in design.

The problem is found when the design is not inherently safe. The future safety of both the plant and those operating it depends on the decision made by the HAZOP team. Their choice may be to;

- suggest a change to the design
- offer a procedural solution

A well chosen, trained HAZOP team should capture the issue of procedural versus hardware solutions in plant design provided that the team does have the appropriate skills, a good leader and sufficient time to carry out the HAZOP. Any actions, particularly those that identify a procedure as the solution for an operation, must be talked through and agreed with the plant owner and operators.

Procedures should never be used as a solution for activities where the risk of failure could forseeably result in serious injury to person, plant or the environment. If the plant cannot be designed in any safer way then the provision of operator-proof safety devices (if they exist!) are the only solution.

There are many examples demonstrating the fatal consequences of relying on procedures as a means of controlling risk. Hand-over procedures in the case of Piper Alpha, Permits to Work in the Hickson Welch fire and dependence upon train drivers to follow procedure when approaching warning lights in both the Southall and the Paddington rail disasters all show the appalling consequences of use of procedures in high risk situations.

Many organisations use as a primary statement in their health and safety policies ‘no harm to people’ but it is really a question of how much a company wants or is prepared to pay to satisfy this policy statement. The government has an accepted figure of £2 million per statistical life saved, and when an organisation carries out its own cost benefit analysis for each project, the cost of lives saved should have a significant bearing on the option chosen and hence, where the process safety line is drawn.

MANAGING CHANGE - WHAT ABOUT THE HAZOP?

A company with well-developed systems that ensure design reviews and HAZOP take place should never encounter new or unforeseen hazards. They will be dealt with prior to the introduction of the new equipment or process..... or will they? The answer will depend on how the company manages change.

MANAGING NEW PROCESSES

A new process can be the source of new or perpetuated hazards. The new substance being introduced may be toxic or a sensitiser and the existing local exhaust ventilation equipment may not be capable of removing it from the air to make it safe. And what if the substance is flammable - is the process in the plant generating sufficient heat to cause a fire or explosion and equipment is the equipment designed to the appropriate standard of electrical safety?

What about like for like replacement - surely there is no hazard there? Quite possibly not provided that the original equipment presented no hazard, that it was right for the job and that no new or different demands are to be made on it. However, there is still a duty to reduce risk and continual improvements in technology may mean that a safer, less noisy, low maintenance replacement is now available.

Procedures which require a systematic assessment of the effects of change and a purchasing policy which restricts purchases to authorised people make for a sound basis in the prevention of the introduction of new hazards.

MANAGING MODIFICATIONS TO PROCESSES

The development of new products or the refinement of production processes is often brought about by modifying processes, plant or equipment. The changes that are made are carried out with the best of intentions. What is often forgotten though is the original HAZOP and the initial basis of safety in design or construction. For example, a process engineer in a local chemical company was recently surprised to find a maintenance engineer’s caustic burns was the direct result of a leak caused by pipe work of large diameter being coupled with existing pipe work of smaller diameter. The root cause lay in making a change or modification without referring to the design review or the original HAZOP. The position where the process safety line had been drawn had been changed. Making any modifications without examining the reason for the initial design criteria is a recipe for disaster as demonstrated by the fire at Texaco refinery in Milford Haven.

The management of new hazards is encompassed in the management of change. The philosophy is simple:

Nothing new should be brought into the workplace unless it is proven not to be introducing a hazard. Nothing should be changed until it is proven to be safe.

LEARNING FROM HISTORY - SYSTEMS FOR FEEDING BACK INFORMATION WHEN THINGS GO WRONG

LEARNING FROM EXPERIENCE

Auguste Detoeuf wrote " The only sure thing in this world is the past, but all we have to work with is the future"[1]. Any process, and this includes process safety management systems, must incorporate a feedback loop at each stage so that new information can be assimilated. Otherwise important information is lost despite root causes being identified and acted upon.

How to capture and use information from incidents. When a major incident has occurred resulting in either injuries or fatalities or even damage to plant, the environment or the image of the company, considerable effort goes into ensuring it cannot happen again. If the management system is working properly the lessons learned will be disseminated and recorded in such a way that the information is retrieval and easily used. Often, case studies of disasters are published by the HSE so that everyone can learn from them. A finding in the recommendations made by the HSE in response to the Texaco fire was:

> **"Safety Management systems should include means of storing, retrieving and reviewing incident information from the history of similar plants"[2].**

However, less serious accidents tend to be forgotten and they are repeated more often despite the personal injury and ill health that result. The vogue for trending of accidents is only useful if the root causes are understood and acted upon. These low consequence/high frequency events are often true indicators of more serious potential incidents the majority of which arise from acts or conditions resulting from human error or unsafe behaviour. Active employee participation is the key to addressing these hazards through a properly implemented behavioural safety programme and through participation in the investigation, review and root cause analysis of the event.

But how can sites capture such information and use it in a way that when incidents occur action can be taken to ensure that there is no repetition? Most large companies use electronic databases for maintenance and these can be used to capture learning. These systems record the frequency and type of maintenance and can also define the tools and procedures to be used, and also the specification for replacement parts.

Such databases are key to providing information that can be translated into safe systems of work. If, for example, breakdown maintenance needs to be carried out on a pump handling a hazardous substance that has a programme of annual maintenance, then this information can be used to re-evaluate the situation and to record improvements. The outcome may be to use a different type of pump or to carry out maintenance every six months. Similar types of databases for say operational procedures can be used for recording learning from risk assessments, incident and accident investigations and audits.

One of this centuries' greatest advocate for process safety is quoted as saying that 'organisations have no memory'[3] yet we are in an era where downsizing allows the more experienced people to leave. The organisation then continues to operate and make changes to plants and processes without the benefit of a huge, historical knowledge base. Means must be found of recording and debriefing such valuable 'databases' before the inevitable occurs.

A MODEL FOR MANAGING PROCESS SAFETY

This paper has been devoted to addressing how far we should go to ensure plants are designed safely thus preventing incidents that may pose a threat both on and off site. An off site release has the potential to injure people and the environment and, in addition, it may also result in adverse publicity which could ultimately damage the company's name. Litigation faced when a process fails in this way can result in huge or even complete loss of business. Figure 1 illustrates a model[4] for ensuring that process safety is managed so that risks are understood, changes are planned and support systems are in place to prevent this occurring.

Managing risks. Risks can be removed or reduced and controlled by ensuring that up-to-date information relating to processes and substances are available and used to assess potential accident scenarios. For this to happen, the root cause of incidents, accidents, and emergency situation must be analysed. If the result for example indicate deficiencies in operator training or the requirement for refresher training then, to maintain the integrity of the system, training must be carried out. Other indicators might be the increased frequency of leaks showing the need to reassess maintenance activities.

The management of change. When new products or equipment (or even people) are introduced or changes made to processes or procedures the picture changes. The known and controlled risks potentially become unknown and uncontrolled. A system must be in place to manage these changes before an accident occurs.

The effective management of change depends on robust procedures that call for the assessment of their impact on the process and on the health and safety of employees and the public before changes are introduced. For example, the rush to bring in a new, faster computer controlled piece of equipment to increase production is no excuse for cutting corners in commissioning equipment or for not delivering training before the equipment is used.

Significant risk often arises from those changes that are rapid, diverse and outside the control of the plant for example,

- a major fire at an adjacent business can have a serious impact if the manufacturing plant needs to be evacuated for long periods of time
- the sudden loss of a key employee through accident or resignation

Business continuity and succession planning must identify key processes, equipment and personnel so that effective contingency plans can be put into place in the event of change and thus reduce potential for injury.

Maintaining system integrity. Some of the key activities for supporting and maintaining business are also a feature of good process safety management. These include procedures, training and an appropriate system for 'maintenance'. Here the term 'maintenance' covers both the document control maintenance that is essential to ensure that procedures and training are up-to-date and also the traditional maintenance of plant and equipment.

These steady state activities should never be diminished regardless of the status of the organisation. Very often when business is either brisk or slow there is a tendency for the need to revise procedures, provide training or the carrying out of essential maintenance to go by the

board. The impact can be equipment breakdown or employees being injured. Either situation can result in lost business but injured employees can also lead to prosecution or publicity and the reputation of an uncaring company- all very damaging to business.

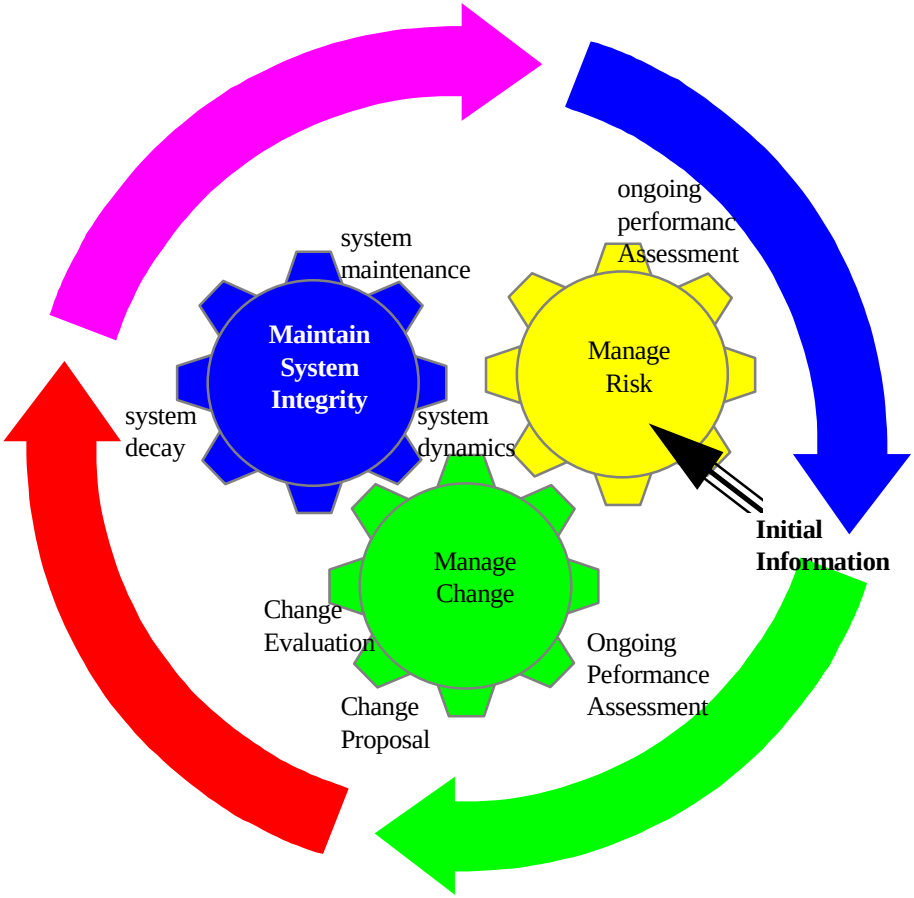

Figure 1. Model for managing process safety

The feedback loop. No management system can be effective without being updated with new information. Continuous learning provides this feedback loop. Information arising reactively from accidents, incidents, emergency situations, breakdowns and other failures in the system together with strategic data from performance measures and the marketplace is essential.

If managed correctly this information can be used to improve knowledge about all process risks and, more importantly, their means of control to show where the line can be drawn on process safety.

1. PG Moore and H Thomas 1988, *The anatomy of decisions*, Penguin Books
2. Texaco Fire July 1994, *HSE Incident Report*, HSE Books
3. Kletz TA 1980, Organisations have no memory, *Loss Prevention*, 13:1
4. Blackmore E 1999, How to improved Hazard Identification and Risk Prioritisation to manage risk and prevent loss, *IIR Conference, Practicalities of risk assessment and safety management July 1999.*