

SELECTING RISK CONTROL MEASURES – WHY ORGANISATIONS OFTEN DEMONSTRATE POOR RISK MANAGEMENT

Christopher J. Beale (FIChemE)
Ciba Expert Services, Charter Way, Macclesfield, Cheshire, SK10 2NX, UK

The selection of risk reduction measures is a fundamental aspect of risk management. Many different approaches are used for selecting measures including legal compliance, insurance/engineering code compliance, qualitative and quantitative risk analysis. Project experience in different countries involving chemicals with major accident hazard potential has been used to identify the range of methodologies which are used for specifying risk reduction measures and making judgements about the acceptability of process safety risks.

The different techniques are described, supported by examples. A range of large and small accidents, including Buncefield and Texas City, are then reviewed to identify why deficiencies in risk control measures occurred. The paper concludes by assessing the methods which are used for costing risk reduction measures and how these are combined with risk reduction engineering to specify risk reduction measures.

KEYWORDS: ALARP, COMAH, risk assessment, cost benefit analysis.

WHY SELECT MEASURES?

High levels of process safety are achieved by effectively managing people, processes and plant. Effective safety management systems address all of these elements of process safety. Plant issues pose particular challenges. History provides examples from a wide range of industries showing how plants have not been designed correctly. Mistakes have been made through ignorance, design error, poor decision making, short-sighted cost control and a poor analysis of uncertainty (Beale, 2006).

Modern approaches to process plant design seek to remove risks using inherent safety principles. When this cannot be done, a plant risk is created. Risk control measures then need to be used to reduce the risk to a residual level which is considered to be acceptable. Plant risk control measures are often expensive to implement and involve difficult decisions and judgements. Operating companies make these decisions using both their own processes and the relevant legal compliance frameworks.

A balance has to be struck between the need for speedy decision making, with the implied risk of poor analysis and incorrect conclusions, and over analysis, with the implied risk of avoidance of making decisions. Words spoken by the Archbishop of Canterbury in a different context summarise the views of many people regarding risk reduction engineering and option analysis – ‘deep contemplation in the shadow of the question mark’.

Table 1. Drivers for selecting risk reduction measures

Country	Strategic risk reduction decisions	Detailed risk reduction decisions
Australia	Detailed QRA to predict risk levels at the site boundary. Measures selected to meet acceptable risk targets. Subject to a Safety Case regime.	Hazop completed by operating company and design contractors. Hazop reviewed by authorities.
Austria	Determined by authorities.	Risk analysis completed by operating company and reviewed by authorities. Strong emphasis on code compliance for key design areas.
China	Determined by authorities in compliance with national legal requirements.	Specified by local design institute. Designs subject to independent risk analysis at the discretion of the operating company.
Finland	Determined by operating company (NB – plant in a completely unpopulated area).	Compliance with detailed standards. Supported by risk analysis by operating company.
France	Determined by authorities to minimise offsite hazard ranges.	Compliance with detailed standards. Supported by risk analysis by operating company.
UK	Specified by operating company using a goal setting approach. Challenged by authorities under a Safety Case regime.	Hazop and risk analysis. Decisions made by project teams with peer review.
USA	Compliance with detailed standards.	Compliance with detailed standards. Supported by risk analysis by operating company.

Recent project experience involving major hazard chemicals such as butadiene, acrylonitrile, methanol and styrene, has shown that very different approaches are used for selecting technical risk reduction measures around the world. Table 1 summarises the main drivers for selecting strategic measures – those involving plant layout, inventories and significant investment – and the main drivers for selecting detailed risk reduction measures based on this experience.

TECHNIQUES FOR SELECTING RISK REDUCTION MEASURES

A wide range of different risk assessment and decision making processes are used in the process industries for identifying and specifying risk reduction measures. Most of the larger companies use a mixture of different techniques to suit the specific technical,

cost and legal aspects of the project which is being undertaken. Commonly used techniques include:

FUNDAMENTAL ANALYSIS

Detailed laboratory safety tests are performed on the chemicals which are being handled to identify their hazardous properties. The tests are performed on actual samples to represent process conditions and worst case samples to represent possible deviations. This allows the chemical hazards to be identified and safe operating limits to be established for chemical storage and process activities. Opportunities for inherent safety are then assessed to remove hazards where possible. The process design team then design control and protection systems to ensure that the process cannot exceed it's measured safe operating limits. This approach is normally used for assessing chemical reaction runaway risks, fire/explosion risks inside process vessels and dust explosion risks. Well designed plants will be supported by accurate laboratory safety tests, the correct interpretation and application of the test results and the experience of the design team. This normally leaves limited room for meaningful option analysis for control and protection measures aimed at preventing major loss of containment or energetic releases. Risk reduction efforts are then focused on sitewide mitigation and emergency response measures, including fixed and mobile fire fighting systems. This approach is popular in many north European countries.

RISK MATRIX

Hazards are assessed qualitatively or semi-qualitatively to estimate their frequency of occurrence and hazard potential (Middleton & Franks, 2001). Each hazard is then positioned on a frequency/consequence matrix. The matrix typically includes risk tolerability criteria. Figure 1 shows the risk matrix which is used by the Ciba UK manufacturing sites. Importantly, this matrix includes three regions:

- **Intolerable risks**, where immediate risk reduction measures must be implemented.
- **ALARP region risks**, where option analysis is required above and beyond the requirements of relevant standards and good practice.
- **Broadly acceptable risks**, which are acceptable with compliance to relevant standards and good practice.

It is, however, important to realise that further analysis is required for any risks which are identified in the ALARP region (HSE, 1999). If the risk matrix is created as part of a hazop study (IChemE, 2000), ALARP region risks are often discussed by the team before making a final decision about which risk reduction measures should be employed. This uses the experience of team members but can lead to poor decisions as there is no objective assessment by an outside person, insufficient time may be devoted to risk reduction assessment and the team's decisions may be overruled at a later date in the project. To overcome these problems, some companies complete additional risk reduction assessments as a separate exercise during project safety reviews or when Safety Reports are created (COMAH, 1999).

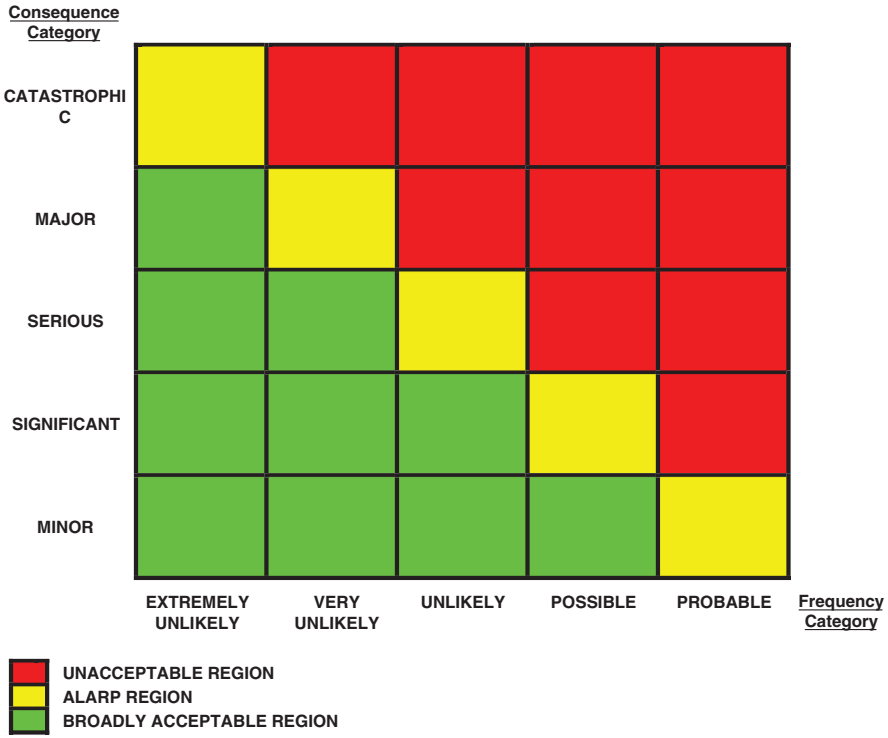

Figure 1. Ciba UK risk tolerability matrix

The risk matrix approach is very effective when there are a wide range of different hazards associated with a project and it has the benefit of being easily understood by wide groups of people, encouraging an inclusive approach to risk assessment. Technical staff can focus on the nature of each risk rather than on understanding an obscure and complex methodology and results can be communicated to senior management in an easily understandable format.

Practical problems occur in multinational organisations. They use management systems and decision making criteria which can be applied on a worldwide basis. Concepts which only apply to specific countries, such as ALARP, cannot easily be integrated into global EHS management systems. Indeed, risk is viewed in very different but equally valid ways around the world. As an example, corporate decisions about risk tolerability within Ciba are made using a risk matrix which measures consequence against the quality of risk control (see Figure 2). This allows risks to be ranked relative to one another as well as

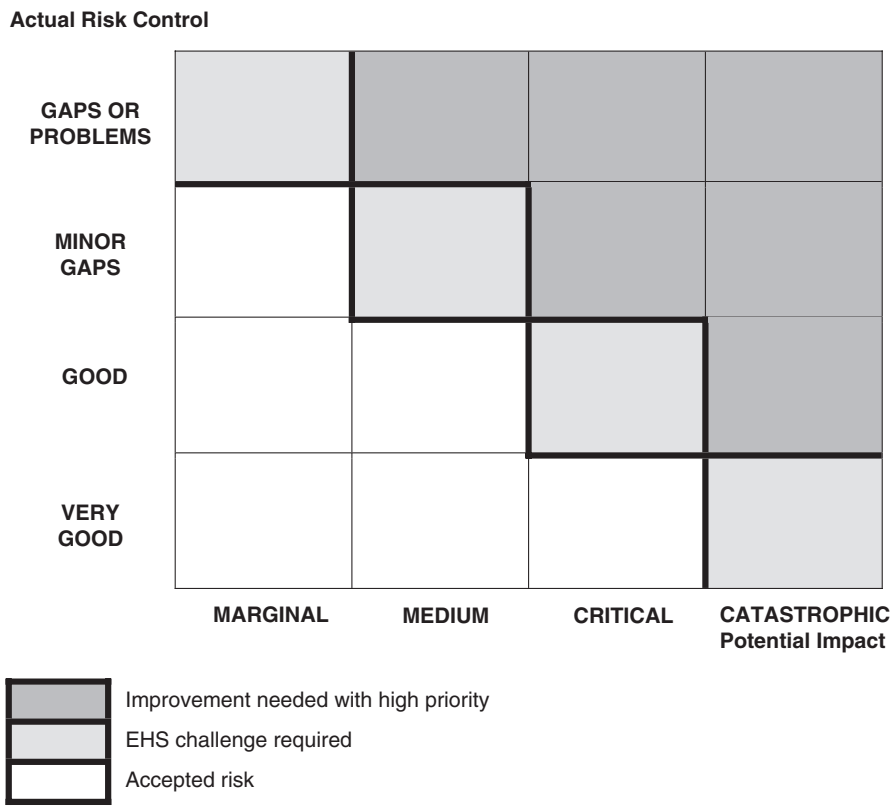

Figure 2. Ciba corporate risk tolerability matrix

identifying risks which are unacceptable and where immediate improvements are required. The senior management team can review risks globally, by business segment, by country or by site. Individual business segments and sites are then expected to drive risk reduction as part of a continuous improvement program.

PEER REVIEW

Most large organisations use peer review processes for challenging key business decisions. EHS risks and capital investment projects are key business decisions for responsible organisations, so it is easy for them to incorporate EHS 'challenging' into their general business decision making processes. 'Challenging' normally involves presenting an issue or a project to an independent review team. They then use their experience to check that

the correct decisions have been made, including areas where EHS risks are not acceptably controlled and areas where excessive EHS expenditures are proposed.

Peer review will often work at different levels within an organisation. It may involve site staff for smaller projects and corporate staff for complex or large projects. Suppliers are often used to review design proposals as part of responsible care commitments. This can be very useful when the operating company has a limited knowledge about handling a hazardous chemical.

CHECKLISTS

Rather than relying purely on expert judgement, team decisions and risk assessment, it is possible to formalise a checklist of typical risk reduction measures. Priority risks can then be identified, for example, using a risk matrix (see above) and formally assessed using the checklist. This method provides a systematic framework for selecting risk reduction measures but has some important disadvantages. Firstly, it may stifle creativity and innovation because of the need to assess a long list of options formally for each identified risk. Secondly, it may be genuinely difficult to provide a concise list of risk reduction measures which are suitable for a diverse and complex industry such as specialty chemicals manufacturing. Thirdly, the selection of risk reduction measures is directly linked to the cost of each measure as well as the risk reduction benefits which would flow from adopting each measure. Cost estimation is difficult and time consuming and may divert specialist technical engineering design staff away from improving designs and towards costing designs which will not be built. Fourthly, a checklist approach could be used relatively easily for a new plant design. It is less useful for assessing existing plants and can lead to a blinkered view of actual risk and skew decisions and resources towards technical hardware improvements rather than operational control improvements such as human factors, plant maintenance and management of change. Table 2 summarises a checklist that was developed for a Ciba UK site. It should be noted that any cost estimates are unlikely to be applicable to other sites because of the problems associated with developing accurate cost estimates for risk reduction measures (see below).

COMPLIANCE WITH STANDARDS

Many problems in the process industry are similar and can be assessed using a common industry or corporate standard. The standard can be used as a solution to a generic problem and represents a risk assessment based on the experience and analysis which was used for creating the standard. This approach is in common use in many countries, such as the USA, China and northern Europe and is often embedded in the country's legal regime for safety.

Compliance with standards is not a foolproof guarantee of safety. Standards reflect recorded and accepted past experience but do not address unknown problems and uncertainty. They encourage a compliance driven rather than innovative and creative mindset and are often difficult to apply to novel situations. Grey areas, requiring interpretation,

Table 2. Example checklist for risk reduction options

Description of risk reduction measure	Installed cost (£)	N	Annual cost (£)	Running cost (£)	TAC
Pneumatic fire detection system	£2,000	15	£133	£100	£233
LHD cable fire detection system	£35,000	15	£2,333	£1,000	£3,333
Flammable gas detection system	£20,000	15	£1,333	£3,200	£4,533
Toxic gas detection system	£45,000	15	£3,000	£3,200	£6,200
Warehouse fire protection system	£200,000	35	£5,714	£500	£6,214
Tank farm fire protection system	£85,000	15	£5,667	£1,000	£6,667
Road tanker fire protection system	£15,000	15	£1,000	£1,000	£2,000
Plant fire protection system	£140,000	15	£9,333	£2,000	£11,333
Small manual fire protection system	£11,000	15	£733	£400	£1,133
Large manual fire protection system	£60,000	15	£4,000	£400	£4,400
Automated high level monitor	£106,000	15	£7,067	£1,000	£8,067
Manual high level monitor	£22,000	15	£1,467	£300	£1,767
Firewater supply pump	£23,700	15	£1,580	£2,400	£3,980
Firewater supply and run-off civils	£1.5M	35	£42,657	£20,000	£62,657
Large plant firewall	£83,000	35	£2,371	–	£2,371
Small area of Durasteel fire cladding	£1,200	35	£34	–	£34
Vessel passive fire protection per vessel	£7,000	15	£467	£200	£667
Steelwork passive fire protection per joist	£1,000	15	£67	–	£67
Small plant fire drains	£100,000	35	£2,857	£300	£3,157
Large plant fire drains	£170,000	35	£4,857	£500	£5,357
Fire system valvehouse	£20,000	35	£571	–	£571
Fire engine (second hand)	£20,000	6	£3,333	£3,000	£6,333
Acrylate inhibitor addition system	£20,000	15	£1,333	£300	£1,633
Dust explosion suppression system	£50,000	15	£3,333	£800	£4,133
One CCTV camera c/w monitor	£6,000	6	£1,000	£800	£1,800
Office block window filming	£22,000	35	£627	–	£627
DCS control system interlock	£1,000	10	£100	£100	£200
Hard wired control system interlock	£2,000	10	£200	£200	£400
Simple software driven SIL system	£5,000	10	£500	£500	£1,000
Complex software driven SIL system	£100,000	10	£10,000	£10,000	£20,000
Blowdown tank, piping and controls	£100,000	15	£6,667	£500	£7,167

NOTE

1. N is the estimated useful life for calculating annual depreciation costs.
2. Annual cost is calculated as installed cost/N.
3. Running cost is the annual inspection, maintenance, running cost.
4. TAC = Total annual cost.
5. 'Fire protection system' means an automated insurance compliant system.
6. DCS interlock costs assume that the plant already has a DCS control system.
7. Costings based on 2003 prices and need to be adjusted for inflation.

exist in most standards and flexibility normally exists to interpret phrases such as 'should' rather than 'must'.

Standards are used by most multinational companies to promote EHS consistency. This can produce standards which are extremely loose to cater for differences between individual countries and regions, destroying the original intent and control within the standard. This problem can be mitigated by having more general corporate standards with a requirement that there must also be compliance with locally applicable standards and laws.

If standards are overly tight, illogical EHS decisions often ensue. For example, a standard for fire protection of ambient flammable liquid storage areas is likely to require certain fire protection measures according to the material flashpoint. A liquid with a flash point of 40°C will pose a low fire risk in a cold north European country but will pose a significant fire risk in a hot country such as Mexico. Strict application of this requirement would result in overprotection of the European storage area compared to a risk assessment which was completed based on first principles.

QUANTITATIVE RISK ASSESSMENT (QRA)

These are the most complex and costly methods of risk assessment and are used for assessing complicated risks objectively. They are commonly used to assess human fatality risks and can also be used as a basis for plant design and layout decisions. The technique is most useful for assessing the relative risks associated with a number of possible options for a project. The following types of risk are most often calculated:

- **Societal risk**, how risk affects groups of people and can cause multi fatality events.
- **Individual risk**, how risk affects individual workers so that risks can be compared between different groups of workers in different industries and so that the risks to the most exposed workers can be assessed.
- **Location specific individual risk**, calculating individual risks at different locations assuming that a person is permanently present outdoors at each location. This can be used to optimise the location of buildings and other centers of population on site and control development beyond the site boundary.

This type of QRA is an accepted tool for risk assessment in major hazard industries where a relatively small number of chemicals are being handled but where accidents could have devastating consequences, such as chlorine storage, oil and gas, petrochemical processing and fuel storage sites. Risk is quantified and can be compared to quantitative cost estimates to form a numerical cost benefit analysis. This allows different risk reduction options to be compared easily against defined criteria or relatively.

QRA is much less useful for sites which handle a wide range of chemicals and have many different hazards. Some risks cannot easily be modeled for QRA purposes. These include reaction runaway and dust explosion risks. Constructing an accurate QRA model is time consuming and resource intensive and the QRA results will not reflect the totality of the site risks. For this reason, specialty chemical companies favour fundamental analysis and risk matrix approaches over QRA.

It should also be noted that there are considerable uncertainties associated with QRA modeling (Beale, 2006). For example, a QRA of the Buncefield fuel storage depot would have almost certainly failed to identify the potential for a large vapour cloud explosion following a cold release of petrol (Crawley, 2006). Any risk reduction measures would therefore have been allocated to known hazards such as pool and tank fires rather than devastating vapour cloud explosions.

MEASURES SPECIFIED BY CONTRACTORS

Most large engineering projects are completed by specialist engineering contract companies. They produce plant designs which are then approved by the operating company. The fundamental experience and creativity which is required to define risk reduction measures therefore exists within the contracting company. China provides an extreme example of how this system operates. The economy is centrally planned and the state and regional governments establish 'design institutes' (Zhang & Allen, 2007) which specialise in plant designs for different regions of China and for different industry sectors. The 'design institutes' serve as a centre of expertise and produce designs for individual sites. These designs are often not challenged critically, or there is limited scope for challenge within project timescales. Risk reduction measures are then very much specified by the 'design institute' rather than the operating company.

MEASURES REQUIRED BY THE AUTHORITIES

Most countries have a legal control regime for major hazard industries. Countries like the UK have a 'goal setting' legal regime where the operating company is required to identify hazards and demonstrate that the required safety management systems and risk control measures are in place. In other countries, such as France, the legal regime is much more closely based on the enforcement of standards supported by calculations of worst case hazard ranges. Additional risk reduction measures are then required by the authorities according to the location of these hazard ranges in relation to offsite areas. From an operating company perspective, this approach will often require hazardous chemicals to be stored in central site areas, thus minimising offsite hazard ranges.

This may result in plant layouts which increase the frequency of accidents as central site areas tend to be congested. It will often also mean that discussions about risk reduction measures are slanted towards actions required by the Regulatory Authorities to minimise offsite hazard ranges rather than requiring the operating company to thoroughly assess the risks that they are best placed to really understand.

EXAMPLES OF POOR SPECIFICATION

TEXAS CITY (USA), 23RD MARCH 2005

A large vapour cloud explosion occurred in the isomerisation unit at the BP Texas City refinery, causing 15 fatalities and more than 170 injuries. BP commissioned two reports

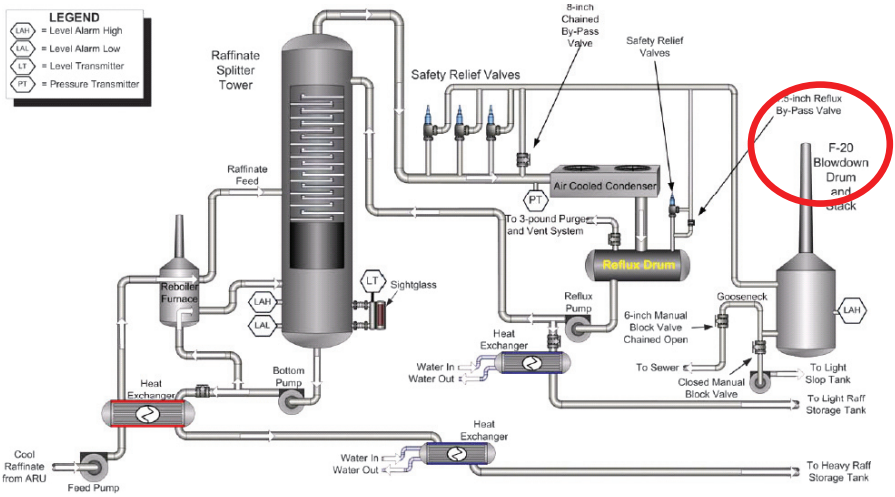

Figure 3. Design of raffinate splitter blowdown tank vent system

(BP, 2005a & BP, 2005b) and the Baker report was issued following an independent investigation (BPRISRP, 2007). A wide range of initiating causes and learning points were identified in these reports but one important issue related to the selection of technical risk reduction measures. The pressure relief system which protected the raffinate splitter tower vented into a blowdown drum which was connected to a tall stack. The stack vented to atmosphere rather than being connected to a flare system (see Figure 3). This meant that any large hydrocarbon vapour releases would be released into the refinery area, creating a large flammable cloud. If the stack had been routed to a properly designed flare system, these vapours would have been burnt off safely, removing the vapour cloud explosion risk.

A number of interesting points are identified in the Baker report:

1. The original blowdown tank stack was not connected to a flare when it was built in the 1950's, presumably in compliance with the relevant refinery design standards of the time.
2. OSHA, the Regulatory Authority cited the lack of connection of the blowdown drum stack to a flare in 1992 but subsequently withdrew the citation. This was presumably based on discussions with the operating company or a re-assessment of the safety risks.
3. The blowdown drum was replaced in 1997 by the then owners, Amoco. A like for like replacement was made even though this design feature did not comply with the latest corporate standards. The decision was presumably made on economic grounds and a view may have been taken that new design standards did not apply to old equipment.
4. BP acquired the Texas City refinery in 1998 but did not change the blowdown drum stack design. This type of issue would normally be identified in due diligence audits at

the time of the acquisition. BP would then have had to prioritise expenditure on the acquired company as part of a longer term program to bring the refinery up to the standards required by BP.

This highlights an issue faced by many sites. Plants may have been designed to comply with old standards and do not meet modern standards. In some cases, it is economic to upgrade the plant. In other cases, operating companies are faced with the option of either closing the plant or spending a large amount of money to upgrade the plant. Closing the plant could transfer fixed costs to other plants, prejudicing the long term future of the whole site. Funds may not be available for plant upgrades if adverse economic conditions are prevailing. These decisions can be very difficult to make.

After an accident of the scale of Texas City, BP is unlikely to build new plants with the design flaw of no vent connections to a flare. BP is lobbying for a change in US design codes to make other sites aware of this process safety issue. The world's newest refineries are being built in Asia and some still do not have the required vent connections to a flare system, even though they were constructed after the Texas City accident.

BUNCEFIELD (UK), 11TH DECEMBER 2005

One of the UK's most devastating peacetime accidents occurred at Buncefield when a petrol storage tank was overfilled. It is postulated that a large vapour/mist cloud then developed and ignited to produce a devastating explosion. A Major Incident Investigation Board was set up and a report was issued in 2007 (Buncefield MIIB, 2007). Initiating causes and learning points from the accident have been published. They cover a range of operational control, land use planning and emergency response issues as well as issues associated with not identifying that a vapour cloud explosion was a credible event at the site.

Logically, risk reduction measures would have been specified to address known and identified hazards. Protection measures against explosions would only have been specified if a precautionary approach had been taken. This might have involved measures such as flammable vapour detectors, high reliability inventory isolation systems and modifications to emergency plans and emergency resources.

The known and identified hazards were associated with fires and tank overfill should have been identified as a credible cause of fire. A robust option analysis would have identified the need for additional prevention and protection measures to prevent overfills. The IEC61508/61511 standard (IEC, 1998) addresses one key aspect of these systems – SIL (Safety Integrity Level) reliability requirements for critical interlocks. Most companies apply this standard by designing SIL levels to meet a required risk target using a LOPA (Layer of Protection Analysis), risk matrix, risk graph or fault tree analysis technique. Once an acceptable risk target has been met, option analysis is not normally carried out.

It is also interesting to note that it is suspected that the formation of the large flammable cloud was partly caused by liquid pouring over the tank and hitting deflector plates which had been installed to improve the performance of the tank fire sprinkler protection systems. The deflector plates may have increased the formulation of droplets, creating a flammable mist.

KAPRUN (AUSTRIA), 11TH NOVEMBER 2000

A fire occurred in a train on a steep funicular railway serving one of Europe's main ski areas. 170 people were killed (Beale, 2001). The transport system relied on unusual and specialist technology (funicular railways in mountain tunnels) with little or no provision for dealing with accidents. As such, there would have been very few standards which specifically addressed the design of funicular railway systems and any that did exist would have been based on a relatively limited amount of operational experience.

The railway system operated and was presumably considered to meet all required legal safety standards based on compliance with standards. If a more creative approach had been used based on risk assessment, some major design and safety issues would have been identified, namely:

- Identifying how a fire could start and spread in a train which was supposed to be fire resistant.
- The absence of fire fighting equipment (eg. fire extinguishers) inside the train or inside the tunnel, making it impossible to extinguish a fire.
- The absence of effective escape routes from the train and the tunnel as the train fitted tightly into a tunnel.
- Difficulties in access for emergency services. A long steep walk was required into the tunnel and there were no helicopter landing sites close to the tunnel for evacuating casualties.
- The reasons that the fire doors at the ends of the tunnel were open when they should have been closed to prevent fire and smoke spread.
- The apparent absence of an emergency plan and poor operator training for dealing with an emergency.

Additional risk reduction measures could have then been put in place to prevent and mitigate this accident.

SOLVENT RELEASE, CIBA SITE, 2003

Approximately 3te of cold hydrocarbon solvent was emitted from a bursting disc onto a works roof. The bursting disc was protecting a process vessel. The solvent temperature was well below it's flash point. This incident was minor but could have been far more serious.

This incident showed how important it is to identify risk reduction measures correctly at a detailed level of plant design as well as at a high sitewide/Safety Report level. A hazop study had been conducted for the vessel and the team failed to identify that it was possible to overpressurise the vessel if a solvent cleaning line to the vessel was left open. As such, risk reduction measures were not explored for this hazard and at least one important risk reduction measure was not specified for the plant. A simple and inexpensive measure, adding a high pressure feed isolation interlock, would have prevented the hazard.

The most likely reason for missing the hazard was fatigue at the end of a long hazop session. If each hazard had been option assessed in detail, this would have created even more fatigue. Experienced Ciba hazop leaders consider that the most effective way of

specifying risk control measures at this level of detail is to rely on expert judgement and team experience rather than formal option analysis systems, but the creativity and alertness of the team must be maintained through what is often a very tedious process.

REACTOR VENT RELEASE, CIBA SITE, 2003

A vapour release of an odorous chemical occurred on a calm and cold winter's night. The release affected offsite areas some distance from the site boundary. The release occurred following a pressure relief event on a newly installed reactor.

The reactor design was based on a thorough process and engineering assessment of an old plant. A large capital investment was made to allow the old plant to be closed as it did not meet modern design standards. The new plant included an automated DCS control system, SIL rated interlocks, mechanical pressure relief systems and blowdown tanks, fire detection and fire protection systems. It was considered that all required risk control measures had been implemented. An oil and a water phase separated, creating a layer of accumulated monomer. The potential for layering had not been identified. This led to an uncontrolled polymerisation reaction. All of the safety systems worked as designed but a small vapour release was emitted from the blowdown tank vent. This was predicted to be a low frequency event.

Despite the fact that a wide range of risk reduction measures had been specified, all of which would have safely controlled a range of human, equipment and software failures, a relief event still occurred. After the incident, questions were raised about the need to install additional risk reduction measures. Emergency scrubbers, tall vent stacks or emergency incinerators could have been installed at very high operational and capex cost. Some of these measures would have caused additional safety risks. It was concluded that reasonable risk reduction measures had been installed and that the main cause of the accident was poor process control and inadequate process knowledge.

STYRENE STORAGE TANK, UK SITE, 2000

A fire risk assessment was being completed for an old tank farm which housed bulk styrene storage tanks. The tanks were housed in two adjacent containment bunds. Each bund was protected with an automated bund foam pouring fire protection system. The tanks in one bund had no sprinkler protection to provide cooling to the tank walls. The tanks in the other bund had sprinkler protection. This appeared to be completely illogical as fires in one bund would impact the other bund.

It was subsequently discovered that the tanks were installed at different times. When the first tanks were installed, the insurance company required a foam pouring system to be installed. Some years later, the tank farm was extended. The site had a different insurance company and they required sprinkler protection to the new tanks to comply with their requirements. The original tanks were not upgraded as they were existing tanks.

Design to standards had therefore created an inconsistent fire protection philosophy. Experienced fire fighters also recommended that the original design without sprinklers

was safer. The sprinkler design allowed water to splash into the bund, breaking the protective foam layer and allowing fire burn back.

ECONOMIC CONSIDERATIONS

As well as identifying and assessing the risk reduction benefits of potential risk reduction measures, operating companies must also estimate the costs of each measure so a judgement can be made about the cost effectiveness of each option.

COMMONLY USED METHODS OF COST ESTIMATION

Companies use a range of techniques for this type of cost estimate:

- Expert judgement based on the knowledge and experience of design engineers and production managers. This technique is popular as it is practical and can be completed quickly. It does not, however, provide a formal demonstration that a cost benefit analysis has been completed.
- Analysis of historic costs for similar projects. This can be derived from real site project experience, experience at other worldwide sites and discussions with suppliers. The analysis can be completed quickly and some evidence can be provided that a structured approach has been used. It does, however have to be used carefully as it is easy to miss important practical issues which can have a major cost impact (see below).
- Broad brush engineering cost estimates. Most companies use capital investment decision making processes which involve progressive project screening and increases in accuracy. This allows unviable projects to be stopped quickly before large amounts of resource are devoted to the project. For example, in Ciba, this involves a Terms Of Reference (TOR) using a cost accuracy of +/– 50%, a Project Proposal (PP) using a cost accuracy of +/– 30% and a Final Project (FP) using a cost accuracy of +/– 10%. Once a project has been approved at these three stages, it passes to the implementation phase. Even the highest band of TOR cost estimate requires specialist engineering resources. These resources are limited and there is concern that engineers will be used to work on theoretical designs which will not be built rather than spending more time on real design work on projects which will be implemented.
- Detailed cost estimates. This provides an accurate cost estimate based on the practical project issues which affect costs. This is a time intensive activity.

HISTORIC COST DATA TRENDING

Cost estimates have to be used with great caution as experience has shown that there are often plant specific issues which have a major impact on cost. These issues include:

- Cost of plant downtime if modifications have to be made outside planned shutdowns.
- Cost of false trips for new safety systems on continuous plants.

- Instruments may be easy to install or the vessels may have inadequate mechanical stabbings. Major mechanical vessel modifications may be required.
- Equipment may be boxed in by other plant and equipment. Lifting and installation costs could be prohibitive.
- Newly installed equipment has to be compatible with existing equipment, which is sometimes old. It may sometimes be necessary to replace a whole control system rather than a single interlock.
- Costs are very dependent on the existence of existing infrastructure. A fire protection system will be much cheaper if a source of pressurised water is available locally, a valve house exists and feed pipe gantries are available. Firewater containment drains are much cheaper if they are close to existing drains. Some drains are very expensive to install because of the local site topography and the presence of other underground services locally.
- Economies of scale. Unit costs will reduce for larger projects as overheads can be spread across a wider range of activities.

The cost of many basic raw materials, including steel, has increased disproportionately faster than the general rate of inflation. This has had a major impact on the cost of some risk reduction measures in recent years. These cost increases must be factored into any historic cost analysis calculations.

CALCULATING LIFECYCLE COSTS

It is important to consider all relevant costs when carrying out a cost benefit analysis. The cost will typically involve a relatively large upfront cost which will be depreciated over the lifetime of the asset, impacting the company's balance sheet, profit and loss account and cash flow statement. There will also be ongoing costs such as staff training, equipment maintenance, inspection and testing and plant downtime. Downtime will be caused by planned maintenance and unscheduled equipment breakdown and maloperation. These are operational costs which affect the profit and loss account.

UNINTENDED CONSEQUENCES

It is easy to fall into the trap of 'silo' thinking when completing cost benefit analysis studies. The team may subconsciously focus on measures to reduce risk rather than inherent safety to remove risk. Deployed resources may be skewed towards major hazard safety improvements rather than occupational safety, environmental and asset protection investments.

Experience has shown that adding risk reduction measures to older plants actually causes a short term increase in plant risks in order to reach the longer term goal of lower risks (Beale, 2004). This is because stable systems which have been in use for a long period of time are changed. Risks are generated when plant changes are made. These often involve human factors. Systems and documentation are not always updated correctly, staff take time to understand the new systems and procedures can become confusing.

DECISION MAKING – LINKING COST AND RISK REDUCTION

Experience has shown that companies use five main techniques for selecting risk reduction measures:

1. ***Acceptance of externally driven requirements.*** If projects are being completed to tight timescales or if technical resources are in short supply, companies will sometimes accept decisions driven by other organisations due to the disruptive effect of challenging decisions, even though they are not considered to be correct by the operating company. Examples include: plant layout requirements driven by the Regulatory Authorities which take little account of practical onsite issues to minimise offsite hazard ranges: planting trees next to tank farm storage areas to provide visual environmental screening so as to secure planning permission from Local Planning Authorities; and installing fixed fire protection systems in low risk areas of the site to satisfy insurance requirements.
2. ***Acceptance of expert opinion.*** Some companies recognise that aspects of process safety can be complex and choose to rely on the advice of internal experts or specialist consultants when making certain decisions. This approach is often used in north European organisations when risk reduction measures are specified using a fundamental analysis technique. Examples include designing a reactor basis of safety when reactor runaway risks exist, designing powder handling systems which are subject to powder fires and dust explosions and specifying fire protection system requirements. The disadvantage of this technique is that it relies heavily on the analysis and experience of a small number of specialists. This approach is often also used when packaged equipment, such as power and nitrogen generation plant, is purchased from a specialist supplier.
3. ***Peer review/challenging.*** Most companies use peer review to challenge important decisions. A project team is assembled to produce a recommended design solution. This is based on their collective analysis and judgement. They then have to present their plans to an independent review team. The review team examines commercial, practical, financial and EHS issues and use their broad experience to check and improve the project design.
4. ***Simple cost benefit analysis (CBA).*** Operators of UK 'Top Tier' COMAH sites (COMAH, 1999) required to use a systematic approach for selecting risk reduction measures. If detailed CBA is not practical, it is still possible to list the additional measures which could be employed, discuss each measure and consider a broad cost estimate for implementation. A summary of why each measure was accepted or rejected is then provided to produce an audit trail. This provides an audit trail for decision making but is still subject to a large degree of expert opinion.
5. ***Detailed quantitative cost benefit analysis.*** When accepted techniques exist in an industry for numerically calculating risk levels, it is possible to construct QRA models. Sensitivity analysis can then be completed to calculate the predicted impact on risk levels if different risk reduction measures were implemented. Detailed costs can then be assigned to each measure to rank the cost effectiveness of each of the

identified risk reduction measures. An ICAF (Implied Cost of Averting a Fatality) is often used.

$$ICAF = C / (R_0 - R_i)$$

C = cost of risk reduction measure (£).
R_0 = baseline predicted average number of fatalities per year.
R_i = reduced predicted average number of fatalities per year after upgrade i.

This allows decisions to be made using relative risk ranking or absolute criteria. Examples of relative risk ranking criteria would be 'implement the ten measures with the lowest ICAF'. Examples of absolute criteria would be 'implement all measures with an ICAF < £400,000. Detailed CBAs are used in industries such as oil and gas and rail transport. They are rarely used in the specialty chemicals industry as process safety risks cannot easily or accurately be modelled using QRA.

CONCLUSIONS

A wide range of techniques can be used for specifying risk reduction measures. Some rely heavily on detailed standards; some are driven by regulatory requirements; some rely on expert judgement; others rely on detailed quantitative calculations. None of these methods are guaranteed to specify the correct range of measures. Different techniques are more effective in some situations than in others.

A balance has to be made between bureaucratic analysis and the need for operating companies to make timely investments in measures that will actually be effective. Operating companies also have to balance their choice of risk control measures across the different types of hardware and software risk reduction measures which are practical. A focus on technical measures is sensible for a new plant. For older plants, better risk reduction improvements may be obtained from people and system related measures, improving operational control. The search for measures must be balanced and should not focus entirely on technical hardware requirements.

Large organisations, such as multinational companies, have to manage a wide range of risks. They will need to use different techniques for specifying risk control measures according to the risks that they face.

REFERENCES

(Beale, 2001) 'Recent railway industry accidents: learning points for the process industry', IChemE Hazards XVI Symposium Series No. 148, 6-8 November 2001.

(Beale, 2004) 'Developing a major hazards learning culture - interpreting information from the Ciba Specialty Chemicals Bradford near miss reporting system up to 2003', IChemE Hazards XVIII Symposium Series No. 150, 23-25 November 2004.

(Beale, 2006) 'Uncertainty in the risk assessment process – the challenge of making reasonable business decisions within the framework of the precautionary principle', IChemE Hazards XIX Symposium Series No. 151 Burgoyne Memorial Lecture, 28-30 March 2006.

(BP, 2005a) 'Process and operational audit report, BP Texas City', BP Plc, James W. Stanley, 15th June 2005.

(BP, 2005b) 'Fatal accident investigation report, isomerisation unit explosion final report,' BP Plc, John Mogford, 9th December 2005.

(BPRISRP, 2007) 'The report of the BP U.S. refineries independent review panel', chaired by James A. Baker III, January 2007.

(Buncefield MIIB, 2007) 'Initial report', Buncefield Major Incident Investigation Board, 13th July 2007.

(COMAH, 1999) The Control of Major Accident Hazards Regulations, 1999.

(Crawley, 2006) 'Buncefield was not unique', Frank Crawley, The Chemical Engineer, April 2006.

(HSE, 1999) 'Preparing Safety Reports: Control of Major Accident Hazards Regulations 1999', HSG190, HSE Books, 1999. ISBN 0 7176 1687 8.

(IChemE, 2000) 'Hazop guide to best practice', IChemE, 2000.

(IEC, 1998) Functional Safety Of Electrical/Electronic/Programmable Electronic Safety Related Systems, Parts 1 to 7, 1998 (also published as BS EN 61508).

(Middleton & Franks, 2001) 'Using risk matrices', Mark Middleton and Andrew Franks, The Chemical Engineer, September 2001.

(Zhang & Allen, 2007) 'Investing in new facilities in China: critical success factors', Jimmy Zhang and Andy Allen, The Chemical Engineer, March 2007.