EFFECTIVE RISK AND CONSEQUENCE ASSESSMENT FOR MAJOR HAZARDS AND PROJECT DESIGN EVALUATION

Jo Fearnley, Aker Solutions, Stockton-on-Tees, UK

Too many projects 'remember' to do safety and risk assessments when the designers are in full swing, and sometimes after the civil work has started. This means that any beneficial changes to reduce the risk are found to be expensive or cause delays to the project time-line, which is not popular with the project manager and client.

Spending a finite amount of money early in a project lifecycle – preferably at concept stage – can provide positive feedback at a time when layout and/or design changes are relatively easy to achieve and the cost benefit can be justified.

This paper discusses two examples of projects which have seen the benefit of this approach.

For one, the modelling undertaken for the project scope, using conservative data, as the design was preliminary only, was able to verify that the well thought through layout would not impose unacceptable risks on the plant, the buildings or the neighbours. The data enable a justified representative set of scenarios to be developed for the COMAH report. Further, when the project design is finalised, the COMAH predictive risk assessment can be finalised at a minimal additional cost, using the models already generated, adjusted for the final design data.

The second project asked for a preliminary quantified risk assessment at an even earlier stage in the project lifecycle to ensure that it would be possible to meet land use planning restrictions for a new plant. There was minimal design data, other than throughput and equipment sizing, but this enabled a base case to be developed. The preliminary QRA indicated unacceptable levels of risk, which was not surprising, as minimal hierarchical controls/layers of protection had been considered. By identifying the major risk contributors the design team and cost engineers were able to focus on the critical risk reduction measures needed for the site, enabling both a justified design basis and a good quality pre-FEED cost estimate.

INTRODUCTION

In the consultancy field it is a common experience to get a frantic phone call requesting a risk assessment to be completed as soon as possible when someone has realised that the project cannot move to the next stage without the relevant tick in the box. This mentality, and view that risk assessments are just a 'project requirement' rather than an integral part of the design process, is concerning as it shows a lack of understanding of the fundamental input that various risk assessments provide to a high integrity project design.

The most extreme example of this in my experience was a hazard and operability (HAZOP) study for some new equipment, held on the client site. As the meeting progressed, it became obvious that design changes resulting from the issues identified were causing concern to the client, with a significant amount of pressure on the team members not to raise deviations for discussion. It soon emerged that the equipment had already been installed, visible from the office window, and the plan to commission the equipment had stopped when they realised that without a HAZOP study they would be breaking company rules. Hence the tight deadline, and the aim to start commissioning the minute the HAZOP study was complete, as the rule did not specify that the actions had to be closed out, only that the meeting had been held!

Whilst the resultant issues for that project were mainly operability, which could be easily retrofitted through software changes post commissioning, not all projects would be so 'lucky'. Quite often a significant risk is identified during a risk assessment which needs considerable redesign to address the issue, so the earlier this is identified the easier and cheaper it will be to do.

WHY COMPLETE RISK ASSESSMENTS?

It might seem an unnecessary question, but through talking to a wide range of project design engineers it is a sad fact that many are not aware of the range of risk assessments which are available in the health, safety and environmental areas, and what benefit different ones offer. There are, of course, those who are fully conversant with the benefits, and/or necessity of the various assessments, but others never challenge the project planner, who puts together the plan, and woe betide anyone who tries to change it.

When contractors get involved, the question of contractual obligation joins the issues of what?/why?/when? If it is not stated, then it is not done – and if it is stated, but the estimate didn't budget adequately for it, then the minimum that can be done contractually is what seems to matter.

There are a myriad of reasons for completing risk assessments; fundamentally the reason is to have an optimally specified project, which delivers the required facility in an environmentally acceptable manner whilst reducing the risk of adverse exposure to on-site and off-site personnel from the materials handled. Add into this the need to reduce energy consumption, to minimise the risk of damage to equipment and increase the reliability and availability of the plant, then the consequential benefits from the money spent on early risk assessments should become obvious. Underlying all risk assessments is the basis that it is necessary to fully understand the process in detail to enable the risk to be managed in a suitable and sufficient way. There is a requirement in the UK to reduce risk to as low as reasonably practicable (ALARP), but for new build projects if the risk within the design basis is identified and addressed early enough then it may be possible to reduce many risks into the broadly acceptable region. The later in a project lifecycle that risk reduction is considered, the more expensive such measures frequently become.

Two recent projects have shown the benefits of completing process hazard risk assessments at an early stage in the project lifecycle. The projects also completed environmental risk assessments at this stage, however the environmental risk was not significant compared to the risk of human harm.

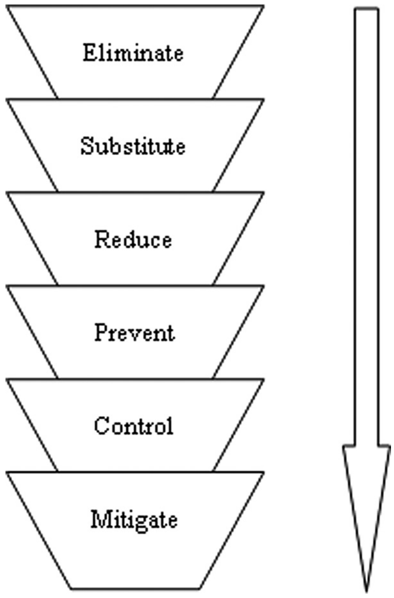

Figure 1. Typical hierarchical controls

CONSEQUENCE MODELLING

A new build project was at the scoping stage in the design. There was space available on one of the company sites, which provided an ideal location, cost-wise, for the new plant. However, as there was a significant amount of infrastructure already on site, the project wished to optimise the new plant layout, without compromising, or being compromised by, the existing facilities.

The company produced a preliminary scoping layout for the new plant, which segregated hazardous and non-hazardous sections of the plant, considered building requirements, and fitted into the space available. Construction access and room for future expansion was included in the scoping proposal. The project scope, and the interaction with the existing plant, was discussed at a very early stage with the competent authority (CA) for control of major accident hazards (COMAH) and the local authority to ensure their informed input was also included in the preliminary plans. This ensured that all planning permission and licence to operate aspects of the project were addressed as early as possible to facilitate ease of subsequent approvals.

Following this early definition work, a hazard identification (HAZID) study was held to determine the scenarios which could lead to safety, environmental and/or asset/financial risks. At this stage the preliminary data was available, such as the layout, process flow diagram, equipment sizing and piping and instrumentation (P&ID) diagrams. The level of detail available did not include any hierarchical risk reduction measures for the plant, see Figure 1, so no mitigation measures were initially considered.

The HAZID study team worked systematically through the process to identify the causes of potentially hazardous scenarios, documenting the range of initiating events, and resultant harm. The HAZID study provided an overview of the potential risks across the whole plant, considering human harm, environmental harm and asset loss. Due to the type of process, the environmental and asset loss categorisations were less severe than those for human harm, so the latter was used as the basis for further risk assessments.

Based on the HAZID study output, the team reviewed the range of events and locations, and determined approximately 35 scenarios with worst case human harm potential, due to consequence. The scenarios were modelled using the DNV Phast software, and the potential for fire, explosion and/or toxic exposure were considered. For each scenario the most extensive harm range for each incident was plotted onto the preliminary layout, such that the extent both within and external to the plant and site boundaries could be visualised.

The worst case consequence modelling enabled the preliminary layout to be confirmed as suitable for further development and refinement, with no major concerns. Further, the consequence models indicated only one scenario had the potential for an off-site impact, and those scenarios which could impact buildings on site, or the existing facilities were identified. Similarly the impact of each scenario on adjacent equipment could be assessed, to determine if any standard separation distances needed to be increased, or any minor layout changes would be beneficial.

By understanding the worst case consequence each type of event across the plant equipment, the front end engineering design could have considered whether there were any inherent design improvements. This could then remove the risk, or the potential severity provided input to the other hierarchical control measures for the design to reduce the risk as low as reasonably practicable.

To assist the ALARP assessment, a preliminary event initiating frequency assessment was developed for each scenario, such that the unmitigated risks could be plotted on the site risk matrix. In conjunction with the potential severity this served to give the design team a basis from which to develop the ALARP justification for the process, and support the budget cost estimate by including the required protection measures.

The project has now been able to submit their planning permission, with a well specified front end design and cost basis for justification to progress to detailed design stage. In addition the project has a fully justified basis for the safety critical events which will be used to develop the representative set of scenarios for the COMAH submission. The worst case consequences are already known and are not likely to prevent any authorisations, and the detailed design has the basis for a fully developed ALARP justification for the COMAH safety case. Once the final design, including hierarchical protection measures, is progressed the final scenario modelling will be straightforward as the base models already exist. The models will simply require the addition of justified event frequencies, weather conditions and population data. The modelling then supports the development of the individual risk, societal risk and occupied buildings risk assessments. Spending the money early in the project lifecycle will mean a lower spend requirement in the latter stages, and overall a very similar spend, but without consequential additional design costs from identifying a potential concern late in the design process. The project sponsors also have the reassurance that the project risks are understood and well managed throughout the project lifecycle.

RISK CONTOUR MODELLING

A different project was still in the concept phase when concern was raised that, due to the rural location and relatively small site, there was a possibility that planning permission may not be granted. In addition to potential visual and noise concerns there was a possibility that the off-site risk contours would exceed the land use planning targets.

The risk contour data was for off-site preliminary risk assessment, as the planning guidance is for the risk of fatality to be below 1×10^{-6}/year outside the site boundary. If this could be achieved then the planning application would be more straightforward than if higher risk was present. The aim was to identify the three target risk contours of interest, i.e. 1×10^{-5}/year, 1×10^{-6}/year and 1×10^{-7}/year. The risk contours do not consider occupancy or vulnerability, but simply assume that a person is present and at risk.

It was therefore decided to undertake a concept stage HAZID study and identify a representative set of scenarios for a preliminary quantified risk assessment (QRA). The underlying aim of completing the preliminary QRA at the concept stage of the project was to check that a showstopper, such as exceeding the fatality targets, was identified and dealt with early.

The representative set of scenarios included a range of site-wide external risks, generic failures of equipment, and critical human error related scenarios from routine or infrequent operational and maintenance activities. As the design data available was limited, the failure frequency estimates for each scenario were initially conservative, as hierarchical protection measures had not been identified. For the consequence modelling preliminary line and vessel sizing were used to estimate potential release quantities. The scenarios were modelled using the DNV PhastRisk software, and the potential for fire, explosion and/or toxic exposure were considered.

The first pass run indicated unrealistically large contours, so, in agreement with the project, the original premise of no protection factors considered was changed such that some basic measures and generic error probabilities were included.

Discussion of the preliminary data led to design basis changes, such that some scenarios were designed out completely or addressed through specifying a design which was inherently safe. In particular, where the concept design had used lower design pressures for certain equipment items, in theory to reduce project costs, it was evident that the risk from overpressure failure was unacceptable, and the design basis was changed to consistent design pressures such that the risk was designed out.

The preliminary data was discussed in conjunction with layout and equipment options, and a revised model developed. In addition, scenarios which had a significant contribution to off-site risk contours were identified, and consequence models for these reviewed separately to see how they could be addressed.

Without reworking the QRA model too many times, it became obvious which scenarios were the ones with most influence on the risk contours, such that these could be assessed in more detail in the front end engineering (FEED) stage of the project. Further, certain scenarios indicated that more major design and/or layout changes were needed to meet the off-site risk contour targets. Identifying such significant issues at an early stage in the project means that these can be dealt with whilst the cost implications are limited. One option identified was to buy additional land around the site, such that the site boundary can extend, and hence the risk to off-site populations is reduced.

At the concept stage changes are on paper only, with additional design costs, but no capital expenditure on purchased equipment or construction costs are involved. Where significant implications arise, which cannot be resolved through on-site changes, such as an unacceptable risk to off-site populations, then decisions can be taken on whether to proceed with the project, or what other options may be available.

For this project the options are still in discussion, both internally and with the local authorities, to determine the way forward for the project. Once the way forward is agreed then a more detailed QRA will be needed. However the benefit of having completed the preliminary QRA is that issues are known about, and it would not be expected that serious deficiencies in the project scope would be identified at a late stage in the project, for example during the hazard and operability study, which would need significant expenditure to rectify or redesign.

SUMMARY

Whilst not enough projects complete adequate risk assessments early in a project lifecycle, these two examples show the benefit of doing so. For one project the worst case consequence assessments gave confidence that the design basis was sound, and proactive ALARP justification could be achieved during the detailed design stage. For the other project the preliminary QRA highlighted issues which can be proactively managed whilst the project expenditure is relatively limited. If these had been found much later in the project lifecycle then the cost implications could be much more severe.