THE APPLICATION OF PROCESS SAFETY BEST PRACTICE IN A NUCLEAR ENVIRONMENT

Nigel Dibben and Janet Skinner, Aker Solutions, Stockton-on-Tees, UK

A new facility is to be built at a UK nuclear site. There is recognition that the plant presents a relatively low risk in terms of nuclear hazards, but that there are significant chemotoxic hazards and conventional hazards. The project team sought to determine whether using process safety best practice in some aspects of the safety assessment would provide a more appropriate design.

A process safety specialist with no nuclear background was brought in to the project to assess some areas of the design using a SIL assessment methodology (compliant with IEC 61511) using layers of protection analysis (LOPA). This assessment was carried out in parallel to the conventional nuclear approach to allow comparison of the impact on the design of the two methodologies.

At the time of writing this paper, the results are being assessed and no decision has been made on the approach to be used. Discussion with the competent authorities is required.

The SIL assessment methodology was familiar to many of the process and instrumentation engineers involved but required on-the-job training of others. The procedure used was generally understood and accepted rapidly but those participating. Of particular value was the knowledge brought to the reviews by experienced operational staff with a nuclear background. Their contribution was important in verifying the probabilities of layers of protection.

As a result of the assessment programme, reductions in instrumented protection functions were proposed and a saving in the overall project cost is expected. In addition to the cost savings, complexity was removed from a number of areas which is anticipated to reduce the scope for operational errors and maintenance issues in the future.

The paper will compare the methodologies used for the assessment of radiological risk with the SIL assessment methodology to identify where one or the other added or removed complexity. Preliminary results indicated that the adoption of risk-based assessment using the LOPA approach reduced the need for protective systems without compromising radiological or chemotoxic safety.

The paper will discuss the benefits of the application of the LOPA approach, the challenges that it posed and the impact on the design and the design team.

KEYWORDS: SIL, LOPA, nuclear, chemotoxic hazards

INTRODUCTION

A facility was being designed to reprocess material which has properties that are hazardous for radiological, chemotoxic and conventional reasons. The safety design work had been carried out on the basis used for radiological hazards. This meant that the potential worst consequence drove the protection proposed without any account of mitigation or protection factors. Aker Solutions' consultants were commissioned to lead SIL (safety integrity level) assessments of the hazards with chemotoxic origins.

PROCESS BACKGROUND

The details of the plant cannot be disclosed in this paper. The plant handles a radioactive input which is separated by the process into a radioactive output and inactive wastes. The process involves the use of non-radioactive chemicals with chemotoxic properties to aid the separation. Overall, the plant will handle substances classified as radiologically hazardous, with combined radiological and chemotoxic properties, chemotoxically hazardous and effectively non-hazardous.

OBJECTIVE OF THE ASSESSMENT

The design of the facility had followed site and client guidelines and requirements regarding the protective measures against hazardous substances and events. With the site and client background being in radiological substances and hazards, their requirements had created the need for extensive safety measures involving high-integrity instrumentation and control measures for protection. These measures were applied to all hazardous materials although several sections of the plant did not handle material with radiological hazards. Many of the chemotoxic hazards arose in areas where the radiologically hazardous material had been separated and the remaining processes were purely chemical in nature. It was recognised that the safety assessment had specified requirements for a number of systems that would not be required in a conventional chemical plant. As the plant would need in part to comply with

nuclear legislation and in part to comply with chemical legislation (in particular the Control of Major Accident Hazards (COMAH) Regulations), it was considered by the client that economies could be gained by reassessing the safety measures under conditions that would be acceptable to COMAH.

SIL ASSESSMENT METHODOLOGY

The decision was made by the client to investigate the degree with which the design could meet the requirements of the European standards for safety integrity levels, interpreted in the UK as BS EN 61511 (BSI, 2004a). Aker Solutions have experience with applying the standard to chemical plants and uses, in particular, the technique known as layer of protection analysis (LOPA) described in Part 3 of the standard (BSI, 2004c). The LOPA technique is considered a potentially useful tool in performing risk assessments for COMAH purposes in guidance prepared for the Health and Safety Executive (Amey Vectra). The methodology has recently been reviewed by consultants commissioned by the Health and Safety Executive in the light of the Buncefield event (HSE, 2010). Further information on the use of the LOPA technique can be read in the Buncefield report (HSE, 2009) with reference to tank overfill in particular but the technique is described in depth and can be generalised to other process applications.

In this methodology, the hazards are identified, initiating event frequencies (IEFs) estimated and modified by conditional modifiers (CMs) if appropriate. In the form employed by Aker Solutions, the hazards are separately assessed for safety to persons, impact on the environment and commercial loss. The layers of protection are then documented under the headings

- Process plant design/integrity
- Basic process control system
- Operator monitoring or response to process alarms
- Passive protection
- Mitigation

For each layer, the probability that it will fail to protect is estimated and written into the assessment. For example, if the basic process control system has a probability that it will work on demand nine times out of ten times that it is required, then the probability of failure is 1/10 or 0.1. This figure is recorded. Protection layers may affect some or all of the hazard types: safety, environmental and commercial. By separating the probability of failure in this way, separate assessments of the residual event frequency can be calculated and separate solutions can be recommended for each hazard type.

To facilitate the assessments in the project that is the subject of this paper, a consultant was engaged who had no previous in-depth knowledge of the nuclear industry but who was experienced in SIL assessment for the chemical industry. This meant that nuclear industry assumptions could and would be challenged more often.

THE SIL ASSESSMENT PROCEDURE – APPLICATION TO THE PROJECT

The raw data for the SIL assessment was in the form of:

- output from HAZOP studies
- initiating event frequencies derived from the radiological assessments
- piping and instrumentation diagrams
- tolerability levels set by the client

The client had already undertaken HAZOP studies which would be defined as level 1 (IChemE, 2008). The HAZOP studies used radiological and chemotoxic keywords and the hazards identified became the subject of the SIL assessments. The hazards, whether radiological or chemotoxic, had already been assessed under radiological procedures to produce the extensive list of protection systems and devices.

The output from the HAZOP studies was in the form of fault schedules and these not only listed the hazards but also provided the potential consequences to personnel on and off the site. Environmental consequences were not generally significant and therefore were not assessed in most cases. Where they were assessed, the consequence was taken into account in the SIL assessment.

Initiating event frequencies had also been assessed in advance of the SIL assessment sessions as part of a probabilistic safety assessment (PSA) and design basis analysis (DBA) as normally required by the Nuclear Directorate (ND) (HSE, 2006). These varied from calculated fault tree assessments to database figures and standard frequencies. In most cases, justification of the frequency was provided as recommended in the research report by the HSE (HSE, 2010). There were occasions where the frequencies were challenged during the assessment process and in these cases, a full record was maintained of the reasons and conclusions reached. Operator experience was used in the assessment process but the initiating event frequencies were generally based on corporate records and experience or industry-wide data. At the time of writing, the exact rôle of the regulatory authorities had not been fixed but the assessments were carried out on the basis that the Nuclear Directorate would review the radiological hazards and that the Hazardous Installations Directorate would review the chemotoxic hazards via a COMAH safety report.

Teams were assembled for the SIL assessment sessions. The teams generally included process engineers, instrument/control system engineers, safety case authors and operations staff (from the ultimate client). Aker Solutions provided a facilitator and the software to record and display the assessment and to calculate the residual risk levels.

UNDERTAKING A SIL ASSESSMENT

Sessions were usually planned to last for about four hours as experience has shown that longer sessions, as with HAZOP studies, become decreasingly productive over time. In the project several different teams were assembled for different

parts of the plant. In total, there were eight distinct sections and five different teams which also varied a little over time as members became unavailable temporarily or permanently. As a result, at the start of each session, a quick poll was taken as to who was familiar with SIL assessment and if necessary a short training session was held.

Details of the hazardous scenarios on the fault schedules, provided from the radiological studies, were input into the SIL assessment tool in advance of the meeting so as to save time. The scenarios were reviewed in sequence and the assessment completed. Completion of the each assessment would entail evaluating residual risk, considering and noting the protective measures already proposed under the prior radiological assessment as many of these measures were defined to cover mixed or chemotoxic-only hazards. Where the measure protected against chemotoxic hazards only, it was classified as suitable for removal. At the end of each session, a rough copy of the assessment was provided to each member for review.

RESULTS OF EXERCISE

The assessments indicated that the standards of IEC 61511 could be achieved with changes and reductions in the degree of instrumentation and other safety features. Proposals were made for a number of independent safety features to be downgraded to basic process control system (BPCS) management or to be removed altogether. This had a subsequent effect on design in that in some cases the dual line of defence required by the nuclear criteria created new hazards such as the risk of expansion and accidental release of fluids trapped between the control valves. In a number of cases, additional pressure relief and lines became redundant and could be removed from the design where the requirement for dual lines of defence ceased to exist. As well as removing lines of defence, in some cases, additional measures became necessary to meet risk reduction requirements. Some of these cases appeared to be excessive to normal practice but arose because of higher than expected consequence levels. In some of these cases, consequence levels were reassessed and a reduction was found to be valid.

In total, more than half of the protective devices required under the nuclear guidance could be removed and with them levels of complexity which would have necessitated additional maintenance effort and operator training. Our perception was that the rules for radiological protection were based on risk aversion as they took little account of probability and were largely based on absolute consequences.

BENEFITS

A number of benefits were seen to the process. On the operational side, the assessment was a team process which encouraged sharing of solutions between different design disciplines. While design “on the fly” had to be avoided, discussion of possible solutions assisted the specialists with solving problems outside the meeting. This also assisted in increasing the acceptability of solutions by all team members as doubts and concerns could be aired and resolved rapidly. The team approach also accelerated the assessment process with most of the assessments, including final recording, being completed in one session with multiple attendance followed by relatively little editing by one person before publication of results.

By comparison with the design basis analysis (DBA) principles, one key factor was the ability to consider vulnerability as a conditional modifier and consequently to lower the level of protection required without compromising the risk to the population concerned. In particular, the plant areas were normally unmanned and operating personnel visited for about 30 minutes in a 12 hour shift so, the risk was reduced by a factor of approximately 95%, subject to certain constraints.

Another factor which can count towards the risk reduction in the LOPA method is mitigation such as bunding and emergency response which could be applied to the chemotoxic hazards under the regime of IEC 61511. In the probabilistic safety assessment used in the radiological assessment, mitigation was recorded but not counted. This meant that in some cases, engineered protective functions could be removed if adequate mitigatory factors existed on the basis that the chemical processes would fall under the COMAH legislation. This assumption could fail if the plant is assessed in its entirety under nuclear legislation.

Subject to the results being acceptable to the Nuclear Directorate, a significant cost benefit had been achieved with reduction in requirement for duplication of lines of defence as required by design basis analysis (DBA).

PROBLEMS

Some problems arose with the method by which the SIL assessment process was applied. These were not seen as issues with the LOPA system but rather with the way in which it was applied in this project. One problem which was not encountered was resistance and the project team proved in general to be very receptive to the use of the SIL assessment approach.

The issues which arose from the timing of the assessments, that is, after the HAZOP 1 had been completed, were mainly in that the basis for the SIL assessments relied on the fault schedules and a fresh view was not taken of the potential chemical hazards. This led also to the need in a number of cases for redefinition of the hazard scenarios as the fault schedules combined a range of cases (e.g. for different acid concentrations) into one case.

Issues arose when considering the consequence assessments. In all cases, these were assessed as “worst case”. This could mean most critical weather, most vulnerable person, most hazardous material, etc. and could exaggerate the risk rating. Weather and vulnerability could be taken into account through conditional modifiers but the variations in hazardous properties of the materials handled

were not taken into account during the assessment with the risk being based on the most hazardous. This could be handled by assessing the risk for each material individually and combining the resultant values.

Care was taken to ensure that the assessment covered purely chemotoxic hazards. There was the possibility of a failure upstream to release nuclear material into the chemical process and the conclusions will need to be checked to ensure that this cannot occur where proposals have been made tot reduce the protective measures following the SIL assessment.

The LOPA approach favours a simplistic relationship between one hazardous scenario and one safety consequence (plus one for environmental and one for commercial) but the fault schedule work that had preceded the assessments in this project had in some cases related one scenario to more than one consequence or vice versa. These simplifications which did not adversely affect the probabilistic safety analysis had to be rectified for the SIL assessment.

The nuclear assessment considered a number of cases which are not within the scope of conventional process safety such as crane movement, sample handling and vehicles. Where possible, the LOPA technique was applied to these with reasonable results.

One of the key problems was converting some of the safety case authors to thinking in terms of risk and probability.

OTHER FACTORS

Taking into account that some of those involved were normally dedicated to radiological processes and risks, we observed that there were significant similarities in all but name. Initiating event probabilities rarely differed from chemical industry 'standards' and there was no impediment to using other standard probabilities when required. With some team members having carried out probabilistic safety analyses in the past, the theory behind the SIL assessment process was relatively quickly understood. The techniques that lay behind the probabilistic safety analysis also proved useful in validating the probabilities of failure of particular protection measures such as control loops and valves. These had previously been calculated to considerable accuracy and the values could be used in the LOPA assessments.

However, there remained one area of uncertainty with the process at the end of the project in that it remains to be approved by the safety authorities, both in-house and HSE/ND. As it follows lines approved by HSE for COMAH safety cases and as COMAH is expected to apply to the chemotoxic hazards, this is not seen as a critical restriction.

CONCLUSION

In a case where the safety measures had been designed exclusively with radiological risk assessment practices and nuclear legislation in mind, reassessment of process risks using SIL assessment by the layers of protection analysis method proved to have a positive effect on cost reduction without any reason to expect an increase in overall risk. Because the methods have slight differences, not all cases examined led to no change or a reduction in protective measures, some required additional safety integrity systems. However, the overall result was a saving in complexity and cost.

ACKNOWLEDGEMENTS

The author wishes to thank the client who permitted this anonymous version of the paper to be prepared.

REFERENCES

Amey Vectra, Lines of Defence/Layers or Protection Analysis in the COMAH context, *Amey Vectra published on http://www.hse.gov.uk accessed 6 April 2010*.

BSI, 2004a, Functional safety – Safety instrumented systems for the process industry sector, Part 1: Framework, definitions, system, hardware and software requirements, BS EN 61511-1:2004, *BSI*.

BSI, 2004b, Functional safety – Safety instrumented systems for the process industry sector, Part 2: Guidelines for the application of IEC 61511-1, BS EN 61511-2:2004, *BSI*.

BSI, 2004c, Functional safety – Safety instrumented systems for the process industry sector, Part 3: Guidance for the determination of the required safety integrity levels, BS EN 61511-3:2004, *BSI*.

HSE, 2006, Safety assessment principles for nuclear facilities, 2006 edition, revision 1, *HSE*.

HSE, 2009, Safety and environmental standards for fuel storage sites, Process Safety Leadership Group final report, *HSE*.

HSE, 2010, A review of Layer of Protection (LOPA) analyses of overfill of fuel storage tanks, Research Report RR716, *Health and Safety Laboratory for the HSE*.

IChemE, 2008. HAZOP: Guide to best practice, 2nd edition, *IChemE and EPSC*.