A DISCUSSION OF SOME COMMON PITFALLS IN THE APPLICATION OF LAYER OF PROTECTION ANALYSIS (LOPA) TO THE OVERFILL OF FUEL STORAGE TANKS AT BUNCEFIELD TYPE SITES†

Dr Colin Chambers[1] and Mr Jeffrey Pearson[2]
[1]HSL, Buxton, UK
[2]HSE, Bootle, UK

In response to the major accident, which occurred at Buncefield in December 2005, the Buncefield Standards Task Group (BSTG) proposed the use of the Layer of Protection Analysis (LOPA) methodology to determine the required integrity of in-scope fuel storage tank overfill protection systems.

The Process Safety Leadership Group (PSLG), which superseded the BSTG, established a LOPA working group to develop guidance for the application of LOPA at Buncefield type sites. Following publication of this guidance in December 2009, the fuel storage industry was asked to submit LOPA studies for their in-scope tanks based on this guidance.

These LOPA studies were reviewed by the COMAH competent authority (CA), overfill protection regulatory team (OPRT). It was found that these LOPA studies contained a number of common issues that required addressing. It was thus concluded that further clarity is required with respect to performing LOPA studies to the requirements of the PSLG guidance at Buncefield-type sites. Therefore, these 'common' issues are discussed in this paper, with reference to the PSLG guidance where relevant. The aim of paper is to increase understanding of the application of the LOPA methodology at Buncefield-type sites.

INTRODUCTION AND BACKGROUND

On December 5th 2005 at Buncefield a gasoline storage tank overfilled for approximately 26 minutes at which point the vapour cloud ignited, resulting in an explosion that lead to catastrophic consequences.

The Major Incident Investigation Board (MIIB) who investigated this incident made recommendations to improve safety in the design and operation of fuel storage sites (MIIB 2007). An important recommendation was that industry should agree to undertake a systematic assessment of safety integrity levels using commonly agreed methods.

Shortly after the Buncefield incident, the Buncefield Standards Task Group (BSTG) was formed, consisting of representatives from the fuel storage industry and the COMAH Competent Authority. Its aim was to translate lessons from Buncefield into effective and practical guidance that industry could implement as rapidly as possible. The BSTG report (BSTG 2007) suggested that the layer of protection analysis (LOPA) study method could be used to provide a consistent approach to Safety Integrity Level (SIL) determination.

There have been two reviews of LOPA studies submitted by the fuel storage industry since the Buncefield incident. The first LOPA study review was performed by HSL who reported to HSE a number of issues that required addressing (Chambers 2009). The findings of the HSL review of LOPA studies were taken into account in appendix 2 of the Process Safety Leadership Group (PSLG) final report "safety and environmental standards for fuel storage sites" (PSLG 2009), which gives guidance for the application of the LOPA method at fuel storage sites. This guidance was produced by the PSLG, who superseded the BSTG. The second review of LOPA studies was performed by the CA overfill protection regulatory team (OPRT) as part of the Buncefield follow up programme. The fuel storage industry was asked to submit LOPA studies based on the PSLG guidance (PSLG 2009) and were asked to supply information specified in the request.

A number of common issues were identified in the OPRT LOPA review:

- Quality of data and the appropriateness of data sources used.
- Inconsistencies in how dependencies between initiating events and protection layers are handled.
- Initiating event issues.
- Human factors not being adequately addressed.
- Omission of adequate supporting information needed to perform the assessment.
- Risk tolerance criteria being inappropriately applied.

This paper discusses example issues identified by the OPRT with suggestions of how they could be considered in a future LOPA study.

This publication and the work it describes were funded by the Health and Safety Executive (HSE). Its contents, including any opinions and/or conclusions expressed, are those of the authors alone and do not necessarily reflect HSE policy.

EXAMPLE ISSUES IDENTIFIED IN RECENT LOPA STUDIES

DATA QUALITY ISSUES

The LOPA study method can be thought of as a group of paths through a bow-tie diagram where all of the factors that can lead to an undesired event occurring are coupled with all those aiming to prevent a specific undesired event occurring. Each of these factors has associated with them a frequency or probability. It is the accuracy of these frequencies and probabilities that helps determine the accuracy of the LOPA study result, in this case an amount of risk reduction. Accuracy in the context of risk assessment and in particular a LOPA is relative to the uncertainties associated with the processes and systems dealt with in a LOPA study. Many of the frequencies and probabilities used to determine hardware, software and human activity reliability are only estimates because they all involve varying degrees of uncertainty.

Therefore, data quality in this case may be thought of as a best guess estimate of, for example, reliability based on past experience and or knowledge of the processes/systems involved and information gained from modelling activities. Collecting data and judging data quality is not a trivial matter and requires specialist knowledge and experience so that this data can be used appropriately.

To help engineers who are not experts in reliability estimation or risk assessment, a number of data sources are available in the form of, for example, component reliability databases, reliability studies, example system reliability data published in international standards, specialist books and manufacturers reliability data. It is strongly suggested here that only those who are able to judge the appropriateness of data should lead LOPA or other similar activities. This then would appear to solve all our problems, we need only use this data within our LOPA study and we have a result. In reality this simplistic approach does not work because there are caveats associated with all forms of reliability data that can make their use problematic.

When determining whether reliability data is applicable for a given purpose a number of factors should be considered.

- Are the components or systems cited in the generic source the same as or similar to the ones under consideration?
- Are the usage conditions of the components or system being considered the same as those associated with the published data?
- Is the data from historical usage or is it the result of reliability predictions as is often the case with manufacturer's reliability data? The use of methods such as FMEDA should not be considered as a guarantee of data quality. Rather such a method, although systematic, is still only as good as the people using it and the assumptions made.
- The measures of reliability from different sources can be in different formats; this requires the analyst to be aware of this and when required to convert from one format to another.

Often, answers to the questions listed here are not known or are simply assumed. So how can the quality of data be considered acceptable and relevant to the systems being assessed? One approach could be to address all the points above by means of a checklist and then to make decisions based on the results. For example, a range of values from different and diverse sources could be determined and a conservative value from that range could be considered reasonable, allowing for data uncertainty. A problem with using multiple data sources is that data from one source is often repeated in other sources, thus apparently corroborating data sources can be misleading. Therefore, care should be taken to identify such cases, for example identical values from two different sources will be an indicator that the data is repeated and not independently determined.

The use of data from any site carries with it the assumption that good management control is implemented on site as stated in the PSLG final report Page 22, paragraph 32; *"For each risk assessment/SIL determination study, duty holders should be able to justify each claim, and data used in the risk assessment, and ensure that appropriate management systems and procedures are implemented to support those claims"* (PSLG 2009).

Data Quality Examples

Below are examples of data taken from LOPA studies submitted from Buncefield type-sites. The main issues are discussed with suggestions of how these examples could be handled in a LOPA study.

Human Error Data Examples

Many of the LOPA studies submitted by Buncefield type sites cited human error probabilities (HEP) taken from the informative annex of the standard (BS EN 61511, 2004). Annex F, table F.3 presents ranges of human error probabilities supported by very simplified text suggesting when that range could be used. Human error probabilities of 0.001 have been claimed in some Buncefield site LOPA studies, with supporting statements that this value represents a mid range value using table F.3. Human factors experts at HSE have stated that they regard a HEP of 0.001 as a very low human error rate for operators and that such claims should be supported by strong evidence covering factors including but not limited to: task analysis, training, periodic auditing (of the operator performing the task) and historical performance data.

One engineer stated that error probabilities used in their risk assessment were recorded at their company but that he did not know where they came from and he could only remember that they had always used these values. In this case it would be difficult for a company to justify the use of such data.

Some LOPA studies have cited as their data source the CCPS LOPA book (CCPS 2001) table 6.5 entitled 'examples of human action IPLs'. The PFDs cited in this book are stated as being from literature and industry, with the literature being previous CCPS human error publications and older publications from Swain (Swain 1983) regarding human reliability at US nuclear power stations. The text in table 6.5 is simplistic and does not appear to allow for human error performance shaping factors, which all human reliability experts suggest should be accounted for. The values recommended for screening in the CCPS book (CCPS 2001) table 6.5 appear to be reasonable for most applications and provided relevant management and operational systems are in place these values should be OK.

In some LOPA studies the HEART method (Williams 1985) was used to estimate human error probabilities. A typical issue with HEART analyses was that the method was incorrectly applied. A generic task type probability was selected from the main HEART table but no error producing conditions were applied thus resulting in an optimistic Human Error Probability (HEP) being selected. In those cases where the HEART analysis was correctly applied the HEP's determined appeared to be reasonable.

Human Factors Data Discussion

Human factors experts at HSE and HSL agree that operator reliability can vary significantly from hour to hour and from operator to operator for numerous reasons. Some of these reasons considered individually and in combination, include but are not limited to: time of day/night, fatigue, illness, weather conditions, stressful situation, operator experience, operator complacency, situation ignorance and over reliance on others. Hence any measure of operator reliability is at best an estimate and almost certainly less predictable than equipment reliability whose failure modes are easier to identify and quantify. There are ways in which a, possibly, acceptable measure of human reliability can be estimated but each of these ways have caveats associated with them. For example, the uncertainties involved in human reliability estimation make using a long-term statistical average predictions potentially unreliable in the short term. Additionally, historical human error data will have been affected by risk reduction measures already in place. Therefore, if it is likely that no additional factors can be claimed to further reduce the HEP, because this would in effect result in double counting of credit for the same factors.

Human error analysis methods such as HEART (Williams 1985) and THERP (Swain 1964) are used to estimate human error probabilities by combining a number of factors, including the effect of relevant error producing conditions. Experienced practitioners should apply methods such as HEART and THERP and any assumptions used should be supported by evidence. Such an analysis is still only an estimate; however, approaches like this when correctly applied encourage the analyst to consider a range of factors in a systematic manner.

Human factors are relevant to all LOPA studies performed at Buncefield-type sites because many initiating events and some protection layers have a significant human error component. As part of the initial request for information, the CA asked Buncefield site operators to include in their LOPA studies a list of individuals involved in the LOPA study and their relevant job function (expertise). As one might expect, engineers, operators, SHE managers and a LOPA facilitator were typically listed. However, none of the LOPA studies listed a human factors specialist. Where operators perform safety critical tasks it is recommended that a human factors professional specialising in human reliability be consulted. The LOPA study leader should have sufficient human factors understanding to perform facilitation of LOPA and provide guidance on suitable human error probabilities and be able to seek specialist advice when required.

Whilst the authors are not human factor specialists, such specialists are employed at their respective organisations and these specialists have contributed to the human factors discussion in the PLSG guidance (PSLG 2009) and to the assessment of human factors issues in recently submitted LOPA studies.

Assessment of human error probabilities must start with an accurate description of the tasks an operator is expected to perform and the conditions under which these tasks can be performed. Then a systematic assessment of each task will help the analyst identify potential errors that relate to the specific hazardous event in question and to estimate the probability of these errors occurring. Such a simplified two stage assessment could be implemented by performing a task analysis and then use the information gained there to feed into a human error analysis method such as HEART (Williams 1985) or THERP (Swain 1964).

Manufacturers' Data Issues

The PLSG final report (PSLG 2009) Page 96, paragraph 68 states "*It is always preferable to base performance data on the actual operation under review, or at least one similar to it. Care needs to be taken in using manufacturer's performance data for components as these may have been obtained in an idealised environment. The performance in the actual operating environment may be considerably worse due to site- and tank-specific factors.*"

A typical example of use of manufacturer's data in recent LOPA studies was where the failure rate for a radar level detection device was cited in lieu of an Automatic Tank Gauge (ATG) system failure rate. Radar device reliability is dependant on the correct setup of the device. This is an issue not considered by manufactures when determining their failure rate data. In this case site historical data would have been a better measure of reliability and would have included all other components of the ATG and operator.

Published Data Issues

A major problem with published data in industry is that factors associated with the source data are often unknown and are likely to vary considerably, e.g. such factors are:

- same or different process type
- same or different operating conditions
- same or different site
- reliably or unreliably recorded

An example of inappropriate use of published data is the often-cited report from Cox Lees and Ang (Cox 1990), which discusses 'Classification of hazardous locations'. This report presents and discusses ignition probabilities in the presence of flammable atmospheres, and is often quoted from in LOPA studies for Buncefield sites to justify low claims for probability of ignition. The Cox, Lees and Ang data used is for offshore platform blowouts and not tank farm overfill scenarios. In this case little effort was made to associate published data with the site and scenario under consideration. Much published ignition probability data was pre-Buncefield incident and hence does not consider ignition of a large pancake shaped gasoline vapour cloud. Because of the lack of relevant ignition probability data it is recommended that the PSLG guidance as discussed in appendix 2, page 106 of the PSLG final report (PSLG 2009), should be used. The PSLG guidance suggests that arguments used to support a stated ignition probability of a Buncefield type vapour cloud should be based on the potential maximum area that could be covered by a vapour cloud. This was approximated to a radius of 250m from the tank under consideration at Buncefield; although other international incidents suggest that this area could easily be greater than that at Buncefield. Once a maximum area covered by a vapour cloud has been estimated then all potential ignition sources in that area need to be considered. This should include faulty equipment, temporary ignition sources, such as temporary generators, and off site ignition sources if the hazard area extends off site. Known permanent ignition sources can act as a limiting factor because a vapour cloud could ignite as soon as it reached them.

INDEPENDENCE IN LOPA

A fundamental concept of LOPA is independence between initiating events, conditional modifiers and protection layers. Independence between protection layers in a LOPA study can be equated to a minimum of common cause or dependant failure modes associated with the systems that implement different protection layers. At a higher-level independence is represented by the so-called onion layer model see Figure 1. (BS EN 61511 2004) aims to ensure that relevant control and protection systems are sufficiently independent from each other. Sufficient independence can be taken to mean that a failure in one protection layer cannot result in a dependant failure in another protection layer. This section of the paper will present common issues found in LOPA studies concerning independence.

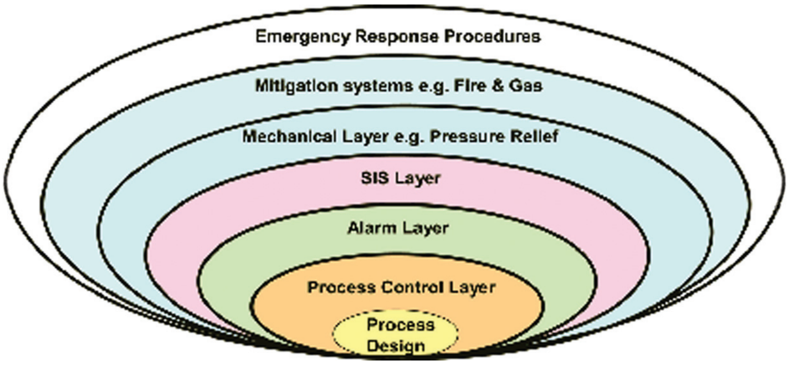
Emergency Response Procedures
Mitigation systems e.g. Fire & Gas
Mechanical Layer e.g. Pressure Relief
SIS Layer
Alarm Layer
Process Control Layer
Process Design

Figure 1. Onion layer model

PSLG Definition of a Basic Process Control System (BPCS)

An area that appears to suffer from a lack of clarity in LOPA studies is the definition of a Basic Process Control System (BPCS) and how the BPCS should be represented in a LOPA study. A LOPA study aims to implement the requirements of (BS EN 61511 2004) and as such the PSLG final report aims to give guidance on this subject with respect to bulk fuel storage tanks. The PLSG final report (PSLG 2009) Page 95, paragraph 62 defines a BPCS as:

"The BPCS is considered to comprise all the arrangements required to effect normal control of the working level in the storage tank, including operational controls, alarms through the BPCS and the associated operator response. For the purposes of the LOPA and the type of scenario under consideration, the BPCS would typically include several of the following:

- a level sensor on the tank;
- field data marshalling and communications systems;
- input/output cards;
- central processing units (logic controller, processing cards, power supplies and visual displays);
- operators and other workers required to perform the normal control function required to control the level of the storage tank;
- communication arrangements between operators if more than one operator is required to carry out the control function;
- final elements (which may be a remotely or locally operated valve or pump)."

BPCS issues A common error in LOPA studies is where credit is claimed for a BPCS component in isolation of the

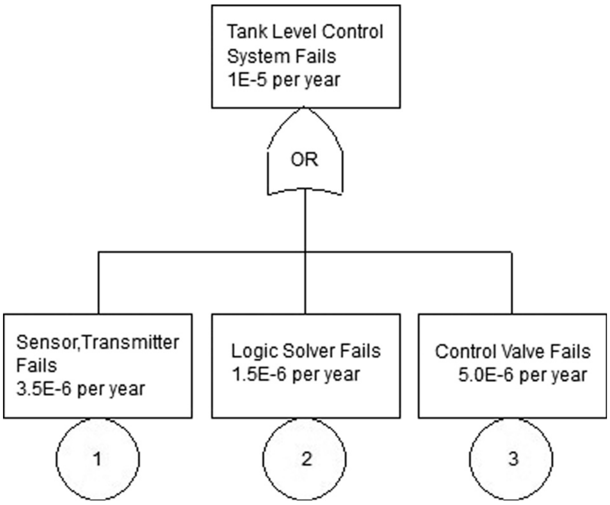
Tank Level Control System Fails 1E-5 per year
OR
Sensor,Transmitter Fails 3.5E-6 per year
Logic Solver Fails 1.5E-6 per year
Control Valve Fails 5.0E-6 per year
1
2
3

Figure 2. Fault tree

rest of the BPCS and that the individual component claimed for has a dangerous failure rate of less than 1×10^{-5} per hour. The BPCS performance limit as defined in (BS EN 61511 2004) and discussed in (PSLG 2009) applies to a BPCS function as a whole and therefore, if BPCS components are claimed for separately, their aggregate dangerous failure rate cannot be lower than the BPCS function performance limit. For example, for a fully automatic level control system, typically comprising a level sensor/ transmitter; logic solver and actuator (control valve), the dangerous failure frequencies could be combined as per the fault tree depicted in Figure 2. The relevant failure frequencies could be sensor/transmitter $= 3.5 \times 10^{-6}$ per hour; logic solver $= 1.5 \times 10^{-6}$ per hour; actuator $= 5 \times 10^{-6}$ per hour. In isolation each component has a failure frequency lower than the BS EN 61511 performance limit of 1×10^{-5} per hour but when combined as in Figure 2 the total dangerous failure rate of 1×10^{-5} per hour holds. The dangerous failure rate is not the whole picture, systematic failure should also be considered. Factors such as software failure, human factors and system design and operation also need to be considered. Most LOPA studies, do not adequately consider systematic shortcomings of the BPCS.

Initiating Event Issues

BPCS as an IE and PL When claiming credit for the failure of the BPCS as an initiating event in a LOPA study the minimum dangerous failure rate that can be claimed is 0.0876 dangerous failures per year or approximately one failure in eleven years. It may also be possible to claim credit for the BPCS acting as a protection layer; in this case a maximum risk reduction factor of 10 may be claimed.

Some submitted LOPA studies claimed credit for a BPCS derived protection layer when the initiating event was failure of the BPCS. For example, credit cannot be claimed for an ATG high level alarm if failure of the ATG is the initiating event.

The PLSG final report (PSLG 2009) Page 99, paragraph 91 states "*The demonstration of independence is most straightforward if the initiating event does not involve a failure of the BPCS, e.g. if the initiating event involves misrouting flow to the storage tank and there is sufficient independence between the person making the routing error and the person controlling the filling of the tank.*"

The failure of any components common between an initiating event and a protection layer or between different protection layers should be carefully considered before credit is claimed. If for example, an independent high level alarm layer relies on the same operator who has responsibility to monitor the tank filling operation then careful consideration must be made of the operator's ability to handle both events reliably and under all reasonably foreseeable circumstances. Another common component could be the tank control/isolation valve. Failure of a shared valve would render the ATG alarm layer and the so-called independent alarm layer inoperable.

Use of shared components in a strict sense would mean that the protection layers involved would not be independent and as such would not conform to protection layer independence rules stated in BS EN 61511 (BS EN 61511 2004) and the PSLG guidance (PSLG 2009). BS EN 61511 (BS EN 61511 2004) suggests that if the shared component failure likelihood is very low compared to that for the rest of the protection layers, then it could be considered sufficiently independent. However, this could be difficult to demonstrate especially when having to account for systematic issues associated with the protection layers.

Initiating Event Cross Check Issues

An initiating event described in a submitted LOPA study outlined a procedure where a second operator confirmed the first operators ATG reading by dipping the tank. The 'confirmed' tank level was then used by the first operator to calculate the tank ullage and set the batch size stop level required for the tank fill operation. A tank dip error probability of 0.001 was claimed for the second operator and the same error probability was claimed for the first operator. The first and second operator error probabilities were then multiplied together to give a combined error probability of 0.000001 or one failure in one million opportunities.

Analysis On closer examination of the tank level confirmation task it can be seen that there are two issues. The first and most significant issue is that dependency between the two operators has not been recognised. Human factors specialists state that there are likely to be dependencies between two operators or an operator and their supervisor who work together at the same site; therefore the same error probability should not be claimed for both operators. The PLSG final report (PSLG 2009) Page 118, annex 6, discusses cross checks and operator dependency. In particular, paragraphs 189 and 190 suggest that a second operator check may not reduce the overall error probability significantly and in some cases may not reduce the error probability beyond that claimed for one operator. THERP (Swain 64) provides a clear dependency model that can be used to avoid this issue.

The second issue is that the operator error probabilities used of 0.001 were optimistic and unjustified because they were not based on historical data or on a systematic human error analysis, or on substantiated published data; but instead were based on values taken from a single source, namely IBS EN 61511-3 annex F, table f.3 (BS EN 61511 2004). The human error data in the informative part of this publication is generic and of unknown origin.

To allow credit to be claimed for a cross check the PSLG guidance sets out criteria to be met, which requires the cross check to be a formal requirement, i.e. set out in a procedure, and to be independent, effective and proper auditable records to be kept, see page 118 of appendix 2 of the PSLG guidance (PSLG 2009). Many LOPA studies claimed credit for cross checks that were either ad-hoc or did not meet criteria cited in the PSLG guidance.

Systematic Identification of Initiating Event

Many of the submitted LOPA studies did not state whether a structured method was used to identify a relevant set of initiating events. This has been shown to be an issue in some LOPA studies because dominant initiating events known from experience for a Buncefield type scenario were omitted.

There are many methods that can be used to systematically identify initiating events for a Buncefield scenario, for example HAZOP or PHA, which are likely to exist before a LOPA study is undertaken. A stand-alone method called a demand tree is described in annex 3 of appendix 2 the PSLG guidance (PSLG 2009), which is demonstrated by an example and is suggested to be a useful approach even when a HAZOP exists.

With respect to well-known events such as a Buncefield explosion, where guidance has been published, the common initiating events may have already been identified. In such cases, adding further initiating events is likely to require unnecessary recourse. Typically, between 3 and 5 dominant/important initiating events would appear to be adequate for a Buncefield type event, unless, for example, a tank is subject to filling from multiple sources, in which case the analyst may wish to use separate LOPA record sheets to account for the different tank filling scenarios.

However, for LOPA in general all initiating events need to be considered to ensure that all the necessary risk reduction measures are identified.

Protection Layer Issues

An independent protection layer (IPL) needs to be independent of other protection layers and of the initiating causes against which that independent protection layer is claimed to provide risk reduction. This is a requirement of clause 9.5 and 11.2 in BS EN 61511-1(BS EN 61511 2004) and is a key simplifying feature of LOPA. To ensure that protection layers are independent, it is vital that they are clearly identified.

The PLSG final report (PSLG 2009) Page 97, paragraph 77 states "*The LOPA methodology relies on the identification of protection layers, and in specifying protection layers it is important that all the rules for a protection layer are met.*"

BS EN 61511-3, Annex C states, "A valid protection layer needs to be:

- Specificity – a PL is designed to prevent or mitigate the consequences of one potentially hazardous event. Multiple causes may lead to the same hazardous event, and therefore multiple event scenarios may initiate action by a PL;
- Independence – a PL is independent of other protection layers if it can be demonstrated that there is no potential for common cause or common mode failure with any other claimed PL;
- Dependability – the PL can be counted on to do what it was designed to do by addressing both random failures and systematic failures during its design;
- Auditability – a PL is designed to facilitate regular validation of the protective functions." For example, via a suitable proof test.

Some LOPA studies described protection layers that did not meet the criterion cited in BS EN 61511 (BS EN 61511 2004) or the PSLG guidance (PSLG 2009). For example, an independent alarm layer has been cited in many LOPA studies; however the description only covered the level detection device and the alarm with no reference to how the alarm would be responded to or how transfer of fuel would be terminated. The whole protection layer description should have included, the level detector, alarm, operator response to the alarm and the means of preventing overfill. Not only should all these factors be included in the protection layer description but also they should all be accounted for in the PFD calculations.

CONDITIONAL MODIFIER ISSUES

The PLSG final report (PSLG 2009) Page 104, paragraph 123 says that "*conditional modifiers are risk reduction factors that are either external to the operation of the facility or are part of the general design of the facility without being specific to the prevention of tank overflow.*"

Conditional modifiers should not be confused with enabling events, which are required to be present for the initiating event to be able to lead to the consequence.

Many LOPA studies cite the detection of overfill by an operator as a conditional modifier. Based on the definition given in the PSLG guidance, detection of an overfill is a mitigation layer and should not be counted as a conditional modifier, See PSLG guidance (PSLG 2009), annex 2, page 101, paragraph 100 onwards for a description of how a mitigation layer should be assessed in a LOPA.

Paragraph 123 also states "*Conditional modifiers are represented by a probability of occurrence and not as a probability of failure, which is used to represent a protection or mitigation layer.*" This is an issue that arises many times in LOPA studies, where failure probabilities are cited instead of probabilities of occurrence. In some LOPA studies probabilities of failure were used for some conditional modifiers and probabilities of success were used for others.

For Buncefield type events the main conditional probabilities are considered to represent: calm weather; ignition and explosion of a large flammable cloud; person(s) in the hazard area; probability of fatality and finally, the probability of environmental consequence, although it is recommended that environmental consequences are considered separately from safety consequences. Many LOPA studies treat each of these conditional modifiers in isolation often using the same arguments in more than one conditional modifier. For example, some LOPA studies have cited low site manning levels as justification for a low probability of fatality, when the probability of person(s) being in the hazard area has already accounted for in a previous conditional modifier. This is a clear case of double counting of credit for the same factor. A helpful way to view conditional modifiers is as a sequence of dependant factors, partly because they are all multiplied together mathematically in the LOPA calculation sheet. For example, the probability of fatality should be thought of as the "probability of fatality given that person(s) are in the hazard area at the same time as a large vapour cloud ignites and explodes." This way of thinking will cause the analyst to think clearly about those factors that could reduce the probability of occurrence of the conditional modifier under consideration.

SUPPORTING EVIDENCE ISSUES

Supporting evidence is vitally important for any risk assessment because without it, an assessor cannot know where the data values used lie in a range from overly optimistic to overly pessimistic and either case is not desirable for SIL determination. When the author first looked at LOPA studies from Buncefield type sites in 2006, most of the supporting evidence was in the form of statements made by engineers citing a single source, be that literature, generic failure rate database or historical failure data. Very few sought to justify the data they used for their site and process. Additionally, few thought to use more than one data source to allow for bias and data uncertainty, which are both present in any non-site and process-specific data source.

Some recent LOPA studies assessed by the CA have shown improvement hopefully because of the PSLG guidance published in December 2009. The PSLG final report (PSLG 2009) contains numerous statements emphasising the requirement to provide supporting evidence for all claims made in a LOPA study, in particular for those cases where non-conservative assumptions are made. An example taken from annex 2, page 94, paragraph 57 states "*As with any quantitative risk assessment technique, it is important that where probabilities or frequencies are assigned numerical values, these values are supported by evidence. Wherever possible, historical performance data should be gathered to support the assumptions made. Where literature sources are used, analysts should justify their use as part of the LOPA report.*"

Although the amount of supporting evidence presented in LOPA studies appears to be increasing, the evidence supplied varies considerably within individual LOPA studies and from one study to the next. Therefore, the authors would urge LOPA analysts to think carefully about what evidence there is to support assumptions, probabilities and frequency values claimed. In cases where evidence is uncertain or non-existent, the UK government's precautionary principle requires that conservative values should be used in a risk assessment (UK ILGRA 2002).

Examples of good supporting evidence with respect to data quality are listed here but not necessarily in order of relevance:

- Statistically significant historical performance data recorded as required by robust procedures for the site and process under consideration in the LOPA study.
- Statistically significant historical performance data recorded as required by robust procedures from similar sites and processes to those under consideration in the LOPA study.
- Systematic analysis using appropriate methods such as FMEDA, HEART, FTA, and reliability block diagram.
- Generic component reliability database specific to the relevant industrial sector.
- Generic component reliability database.
- Data from published literature.
- Manufacturers' reliability data.

Another form of supporting evidence is a clear and unambiguous description of relevant site, plant, procedures and operation relevant to the LOPA study. An unambiguous description could include narrative; diagrams and where useful reference to documents and assessments such as mini fault trees that can be used to make clear how systems and or operations work together. If documents are referenced then if possible these documents should be supplied with the LOPA.

Many submitted LOPA studies lacked adequate descriptions of their site, plant, operations and other on-site and off-site risk factors. This can lead to the LOPA reviewer being unable to properly assess the LOPA. It is the authors' experience that many LOPA analysts, who are involved with a site, make assumptions based on their knowledge of that site and forget that external LOPA reviewers may not have that knowledge. This affects all areas of a LOPA study from initiating event descriptions, BPCS and protection layers descriptions to descriptions of on-site and off-site populations.

It is generally accepted that a document should be proof read before publication, preferably by someone who has not had involvement with the production of the document; it is suggested in this paper that a LOPA study would greatly benefit from such an independent review and that the reviewer's comments and observations should be reflected in the post review LOPA.

RISK TOLERABILITY CRITERIA (RTC)

RTC can be stated as the likelihood of an undesired consequence to an exposed population from an undesired event. For a Buncefield type event, the RTC could be stated as, for example, the maximum tolerable risk of fatality to person(s) from the explosion of a large flammable vapour cloud. Risk tolerability criteria are discussed on page 90 of appendix 2 of the PSLG final report (PSLG 2009).

Many of the recent LOPA studies submitted to the COMAH CA as part of the Buncefield response program did not adequately describe their maximum tolerable risk. It is suggested here that an adequate description should include, but not necessarily be limited to, the following:

- Adequate consideration of both the on-site and off-site consequences.
- A clear statement of RTC – e.g. the risk of 'fatality' to 'a single person', from an overfill of fuel leading to a 'Buncefield type explosion'.
- State the type of risk being considered, e.g. scenario risk, individual risk, societal risk, and environmental risk. All, except scenario risk, should be considered in the context of the COMAH Regulations. See annex 2 of the PLSG final report (PSLG 2009) for further information of these risk types.
- Appropriate target for the mitigated event frequency; necessary to determine the so-called LOPA ratio, or the risk gap that requires closing.
- ALARP demonstration if the residual risk is in the tolerable if ALARP region.
- If required, as part of the ALARP demonstration, a cost benefit analysis can be used that adequately accounts for *all* benefits (avoidance of costs) associated with a Buncefield type event.

A common issue indentified in many of the recently submitted LOPA studies was that the hazard area used appeared to be less than that identified in Figure 23, in appendix 2 of the PSLG guidance (PSLG 2009). The hazard area discussed in the PSLG guidance is based on the damage caused at the Buncefield incident. The hazard area is considered to be 250 m from the tank for outdoor fatalities and up to 400 m from the tank for potential fatality of persons within non-blast-rated buildings. Because the relevant hazard area was not considered in some LOPA studies the number of potential fatalities was potentially under estimated. In some cases accounting for the hazard area associated with the Buncefield incident led to the requirement for societal risk to be considered.

It is suggested that on a scale drawing of the site, a boundary of 250 m and 400 m diameter be drawn around each tank so that the consequences of a Buncefield type explosion can be adequately considered.

CONCLUSIONS

The process safety leadership group (PSLG), which superseded the BSTG, established a LOPA working group to develop guidance for the application of LOPA at Buncefield type sites. Following publication of this guidance in December 2009 (PSLG 2009) the fuel storage industry were asked to submit LOPA studies from the 50 UK sites that have in-scope tanks, based on this guidance.

These LOPA studies were reviewed by the COMAH competent authority (CA), overfill protection regulatory team (OPRT). The initial results of this review indicated that, in a number of cases, there is a need to address areas in LOPA studies that fall short of the PSLG guidance.

The most common issues identified during the assessment process have been discussed in this paper, with reference to relevant sections of the PSLG guidance (PSLG 2009).

This paper has sought to provide a degree of clarity regarding some commonly identified LOPA issues and suggests how these issues could be addressed in future LOPA studies.

REFERENCES

BS EN 61511, 2004, Functional safety. Safety instrumented systems for the process industry sector. Parts 1, 2 and 3.

BSTG, 2007, Final report, Safety and environmental standards for Fuel Storage sites. http://www.hse.gov.uk/comah/buncefield/bstgfinalreport.pdf, Date accessed 1/12/2010.

Chambers, C., Wilday, J., and Turner, S., 2009, A review of Layers of Protection Analysis (LOPA) analyses of overfill of fuel storage tanks, HSE research reports, RR716.

CCPS., 2001, Layer of protection analysis: simplified process risk assessment, AIChE.

Cox, A.W., Lees, F.P., and Ang, M.L., 1990, Classification of hazardous locations, IChemE books.

MIIB, 2007, Recommendations on the design and operation of fuel storage sites Buncefield, available at the Buncefield web site http://www.buncefieldinvestigation.gov.uk/reports/index.htm. Date accessed 1/12/2010.

PSLG, 2009, Final report, Safety and environmental standards for fuel storage sites, HSE books.

Swain, A.D., and Guttman, H.E., 1983, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. (NUREG/CR-1278, SAND800 200, RX, AN), Sandia National Laboratories, Albuquerque, NM.

Swain, A.D., 1964, Technique for Human Error Rate Prediction (THERP) SC-R-64-1338, Sandia National Laboratories, Albuquerque, NM.

UK ILGRA, 2002, The precautionary principle: policy and application, available at http://www.hse.gov.uk/aboutus/meetings/committees/ilgra/. Date accessed 1/12/2010.

Williams, J.C., 1985, HEART – A proposed method for achieving high reliability in process operation by means of human factors engineering technology in Proceedings of a Symposium on the Achievement of Reliability in Operating Plant, Safety and Reliability Society. NEC, Birmingham.