# APPLICATION OF LOPA AND SIL ASSESSMENT TO A NEW COMAH PLANT

Jerry Mullins
Principal Consultant, Abbott Risk Consulting, Manchester, UK

High hazard industries such as those regulated by COMAH face a number of key challenges including demonstrating that major accident risks are as low as is reasonably practicable (ALARP). The demonstration of ALARP includes calculation of risks and judgement on the need for further risk reduction measures. The demonstration of ALARP also involves showing that safeguards are fit for purpose, there are adequate layers of protection and that safety-instrumented systems provide the appropriate level of safety (SIL assessment). Techniques for demonstrating that risks are ALARP by means of risk assessment are well established. These methods include the use of risk matrices and full quantitative risk assessment. Risk assessment has also been utilised in defining the required number of layers of protection and the required performance of safety-instrumented functions.

The application of robust methods for Layer of Protection Analysis (LOPA) and SIL assessment are particularly important at the design stage, as it is at this stage that there is the greatest opportunity to reduce risks to ALARP. This paper will provide an overview of the methods used for a new COMAH plant and illustrate their usage by means of a case study.

KEYWORDS: COMAH, LOPA, SIL

## INTRODUCTION

A key requirement of COMAH, and other major accident hazards legislation, is the effective management of risk. Meeting this requirement generally involves the use of some form of risk assessment to demonstrate that the risk is as low as is reasonably practicable (ALARP) and demonstrating that plant meets current good practice in terms of design, construction and operation. Safety-instrumented functions (SIFs), such as trips, alarms and interlocks are a key component of many systems designed to prevent or control major accident hazards. The challenge of how to ensure that such systems provide the required safety performance has been addressed in the international standards IEC 611508 [ref 1] and IEC 61511 [ref 2]. Both standards require the use of risk assessment to determine a required target failure frequency or Safety Integrity Level (SIL) for each safety-instrumented function (see Table 1).

The standards include a number of possible risk assessment techniques, which can be used for SIL assessment. The simplest of these methods rely on semi-quantitative risk matrices of event severity and likelihood to assign SIL levels (referred to as Safety Layer Matrices). Another method, which builds on the risk matrix approach, is the so-called Risk Graphs, which incorporate additional semi-quantitative judgements on exposure time and the probability of avoiding the hazardous event. Both of these techniques are likely to be suitable for low hazard/low risk plant where the fault sequences are clearly understood. For more complex hazards and/or where the hazards/risks are greater, then more quantitative risk assessment is likely to be needed. In these cases, the standards advocate the use of a Layers of Protection Analysis (LOPA) [ref 3] or Fault Tree Analysis.

For new plants, there may be a need to assess a large number of fault sequences and safety-instrumented functions. Therefore, there is likely to be a need for a time efficient SIL assessment method combined with a need for a robust approach, which does not lead to overly conservative assignment of SIL levels with its associated implications in terms of higher plant design and operating costs. This paper describes the SIL methodology and its application to a proposed new plant on a COMAH top tier site.

## CASE STUDY EXAMPLE

The following case study provides an example of the application of the SIL assessment methodology to a new flammable gas recovery and storage plant. At present the flammable gas is flared off. The objective of the proposed plant is to recover and store gas of suitable quality (below 2% v/v oxygen content) as an energy source for various users within the site. The generated gas is to be pulled by an ID fan into a new flare stack. Depending upon the composition, changeover valves within the flare stack will allow the gas either to be vented and flared off or recovered into a gas holder. A simplified block diagram of the plant is shown in Figure 2.

The purpose of the SIL assessment study was to allocate SIL values for the safety- instrumented functions and identify where necessary additional protection requirements so that the design could be further developed and the project cost defined.

## PROCESS HAZARD REVIEW PROCEDURE

A Process Hazard Review (PHR) study was undertaken on the proposed design in order to identify fault sequences using a standard list of guidewords. The PHR study also included an assessment of the risk associated with each fault sequence by application of the company standard

**Table 1.** Definition of safety integrity levels

| Safety integrity level | Probability of failure on demand |
|---|---|
| 1 | 0.1 to 0.01 |
| 2 | 0.01 to 0.001 |
| 3 | 0.001 to 0.0001 |
| 4 | 0.0001 to 0.00001 |

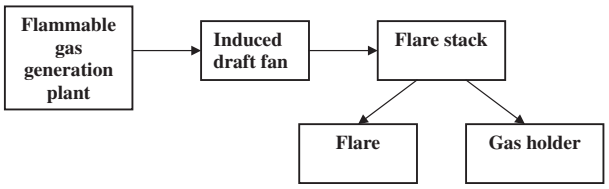


**Figure 1.** Simplified block diagram for new plant

semi-quantitative consequence and frequency scoring system as shown in Figure 1.

The allocation of consequence categories was undertaken on the basis of the following general definitions:

**Minor consequences**: minor injury to worker, off site nuisance.
**Serious consequences**: Single non-major loss time accident, short-term minor effect off site.
**Major consequences**: Single worker major injury or multiple minor injuries, few off site people require hospital treatment.
**Extremely serious consequences**: One or a few worker fatalities, a few serious off site injuries requiring hospital treatment.
**Catastrophic consequences**: Many worker fatalities, one or a few off site fatalities, many injuries.

The allocation of event frequencies was based on plant experience plus judgement on the effectiveness of the safeguards in place.

Figure 2 also shows how the risk values were ranked. Risks in the "intolerable" region cannot be justified except in extraordinary circumstances. Risks in the "tolerable if ALARP" region are tolerable only if risks are ALARP i.e. if further risk reduction is impracticable or the cost of improvements is grossly disproportionate to the improvement gained. Within the "broadly acceptable" risk region, risks are judged to be low and no further formal ALARP assessment is required. In accordance with the PHR procedure, all major accident hazards that were ranked as either "intolerable" or "tolerable if ALARP" were assessed using LOPA. The PHR procedure also required that any such fault sequences which included a safety-instrumented function should be subject to SIL assessment.

## LAYERS OF PROTECTION ANALYSIS

In the LOPA analysis, identified protection systems are represented as Independent Protection Layers (IPLs). For simplicity an IPL is assigned in the PHR methodology as equivalent to a 2 orders of magnitude reduction in event frequency providing three tests are met: independence, effectiveness and auditability (in terms of maintaining the effectiveness of the safeguard). In the LOPA assessment, an IPL would be assigned an IPL value of 1. A risk matrix can be plotted showing consequence category, initiating event frequency along with the required number of safeguards. Figure 3 shows the matrix adopted in this case study. Where a fault sequence has the appropriate number of IPLs then the risk may be considered to be "broadly acceptable" and no further action is required. Otherwise, the priority of the risk reduction is proportionate to the number of required additional IPLs, which in turn is dependent on consequence and frequency. In each case, implementing the required number of additional safeguards will reduce the event frequency such that the fault sequence is in the "broadly acceptable" risk region. The LOPA technique is complementary to the risk matrix approach described above. The former approach is intended to provide a measure of risk for a particular fault sequence taking into account both engineered and administrative safeguards. In contrast, the LOPA approach is intended primarily as an engineering substantiation tool i.e. determining whether sufficient, robust safeguards are in place to guard against a particular fault sequence.

| Outcome<br><br>Likelihood | Minor | Serious | Major | Extremely serious | Catastrophic |
|---|---|---|---|---|---|
| Probable > 1/yr | | | | INTOLERABLE RISK | SCENARIO 2 |
| Possible > $10^{-2}$ /yr | | SCENARIO 1 | | | |
| Unlikely $10^{-2}$ - $10^{-4}$/yr | | | TOLERABLE IF ALARP | | |
| Very unlikely $10^{-4}$-$10^{-6}$/yr | | | | | |
| Remote $10^{-6}$ - $10^{-7}$/yr | | BROADLY ACCEPTABLE | | | |

**Figure 2.** Risk assessment matrix

| Outcome / Likelihood | Minor | Serious | Major | Extremely serious | Catastrophic |
|---|---|---|---|---|---|
| **Probable > 1/yr** | 1.0 | 2.0 | 3.0 | 4.0 | 5.0 |
| **Possible > $10^{-2}$ /yr** | No action | 1.0 | 2.0 | 3.0 | 4.0 |
| **Unlikely $10^{-2}$ - $10^{-4}$/yr** | No action | No action | 1.0 | 2.0 | 3.0 |
| **Very unlikely $10^{-4}$-$10^{-6}$/yr** | No action | No action | No action | 1.0 | 2.0 |
| **Remote $10^{-6}$ - $10^{-7}$/yr** | No action | No action | No action | No action | 1.0 |

**Figure 3.** LOPA assessment – required number of IPLs

## SIL METHODOLOGY

The initial SIL for each protection system was calculated in accordance with the guidance in IEC 65108 [ref 1] plus that published by UKOOA for application to offshore oil and gas installations [ref 4]. The SIL scoring system used in the study is shown in Table 2. The allocated SIL is a function of the consequence of failure (C), the probability of personnel being in the area of the hazard (F), the probability of avoiding danger (P) and the probability of demand on the safety system. The assignment of initial SIL values was undertaken in accordance with the matrix shown in Table 3. It should be noted that the probability of demand on the system was determined assuming no safety systems were in operation. This initial SIL allocation essentially treats all the safeguards in place against a particular fault as one safety system i.e. it takes no account of the number of individual safeguards. This initial SIL value may therefore be overly conservative. The final SIL for each safety-instrumented function within the protection system was determined by dividing the initial SIL by the number of Independent Layers of Protection identified in the PHR study. For example, a safety system with an initial SIL 2 with four Layers of Protection will have a final SIL of 0.5. This final SIL value will therefore apply to any safety-instrumented function within the overall protection system.

The SIL methodology described above has its consequence categories determined in terms of loss of human life and injury. However COMAH also applies equally to the protection of the environment. Therefore when carrying out a SIL assessment, it may also be necessary to consider environmental consequences as well. An example environmental SIL scoring system and SIL allocation method is shown in Tables 4 and 5. The process can also be extended to cover economic losses such as plant damage, length of shutdown and direct financial loss. In such cases, where different types of loss are included in the SIL assessment, the individual SILs derived for a particular fault sequence are compared and the highest value adopted.

**Table 2.** SIL scoring system

| Risk parameter | | PHR classification |
|---|---|---|
| Consequence (C) | A | Minor |
| | B | Serious |
| | C | Major |
| | D | Extremely serious or catastrophic |
| Exposure (F) | A | Persons present in the danger area $<$10% of the time (over a 24 hour period) |
| | B | Persons present in the danger area $>$10% of the time (over a 24 hour period) |
| Possibility of avoiding the resulting hazard (P) | A | Possible to avoid danger |
| | B | No reasonable possibility to avoid danger |
| Probability of the demand on the system (W) | 1 | $<$ once in 10 years |
| | 2 | $<$ once per year |
| | 3 | $>$ once per year |

## PHR STUDY RESULTS

The PHR study resulted in a large number of fault sequences being identified. These fault sequences were ranked by the

**Table 3.** Determination of SIL values

| SIL | CFPW Score |
|---|---|
| – | AAA1, AAA2, AAA3, AAB1, AAB2, AAB3, ABA1, ABA2, ABA3, ABB1, ABB2, ABB3, BAA1, BAA2, BAB1, BBA1, CAA1 |
| 1 | BAA3, BAB2, BBA2, BBB1, CAA2, CAB1, CBA1, DAA1 |
| 2 | BAB3, BBA3, BBB2, CAA3, CAB2, CBA2, CBB1, DAA2, DAB1, DBA1 |
| 3 | BBB3, CAB3, CBA3, CBB2, DAA3, DAB2, DBA2, DBB1 |
| 4 | DBB3, CBB3, DAB3, DBA3, DBB2 |

**Table 4.** Example environmental SIL scoring system

| Risk parameter | | Classification |
|---|---|---|
| Consequence (C) | A | Minor environmental impact, largely confined to site |
| | B | Significant off site impact, not a MATTE |
| | C | MATTE under COMAH |
| | D | MATTE with long term damage |
| Probability of the demand on the system (W) | 1 | < once in 10 years |
| | 2 | < once per year |
| | 3 | > once per year |

**Table 5.** Example determination of environmental SIL values

| SIL | Score combination |
|---|---|
| – | A1, A2, A3, B1 |
| 1 | B2, C1 |
| 2 | B3, C2 |
| 3 | C3, D1, D2 |
| 4 | D3 |

team in accordance with the risk matrix shown at Figure 2. The allocation of consequence and frequency scores was based on the judgment of the team. Also, on site worker populations were assumed to be at their normal locations. As per the PHR methodology, only those fault sequences assessed as being in either the "intolerable" or "tolerable if ALARP" risk region were assessed in terms of LOPA and additionally only those involving safety-instrumented functions were assessed in terms of SIL.

The case study included in this paper is based on two example fault sequences and associated safety functions namely:

**Scenario 1**: overfill protection in gas holder.
**Scenario 2**: air ingress detection upstream of induced draft fan.

The fault sequence involving air ingress upstream of the induced draft fan was assessed as being in the "intolerable risk" region whilst gas holder overfill was assessed as being in the "tolerable if ALARP" region (see Figure 2). For each scenario, the number of existing safeguards identified in the PHR study (see Table 6) was compared with the required number of safeguards as per Figure 3. From this assessment, the following conclusions were drawn:

**Scenario 1**: The current design has two Independent Layers of Protection whereas the LOPA guidance requires a minimum of 4.0 IPLs. The LOPA study therefore con-

**Table 6.** SIL study output

| Scenario no. | Safety system | Scores C | F | P | W | Initial SIL | Safeguards | No of IPLs | Final SIL | Actions/comments |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 (Gas leak from holder due to overfill) | Overfill protection in gas holder | B | B | B | 1 | 1 | 3 individual continuous level monitors with high level alarm through PLC system<br>High-high alarm with hard wired limit switch to stop collection<br>Gas monitoring on gas holder roof with high level alarm | 3 | 0.33 | Consider including audible alarm on gas holder roof to allow operators to evacuate on high level alarm |
| 2 (Internal explosion due to air ingress and ignition) | Air ingress detection upstream of induced draft fan | D | B | B | 1 | 3 | 4 oxygen monitors - 4 into gas holder PLC (2 upstream/2 downstream of gas holder)<br>Explosion relief panels | 2 | 1.5 | Consider use of quantitative risk assessment to evaluate SIL |

cluded that the current design requires further substantiation in terms of safeguards.

**Scenario 2**: The current design has two Independent Layers of Protection, which corresponds to the LOPA guidance requirement of a minimum of 2.0 IPLs. The LOPA study therefore concluded that the current design has an adequate number of safeguards.

The initial SIL values for the two scenarios, based on the scoring system shown in Tables 1 and 2, are shown in Table 6. The final SIL values, taking into account the number of IPLs, for each fault sequence are also shown in Table 6. For this plant design, as per most process plant, the objective was to ensure that all safety-instrumented functions will be SIL 1 or lower in order to minimise costs. From this assessment the following conclusions were drawn:

**Scenario 1**: The initial SIL for this protection system is 1 and taking into account the number of IPLs in this protection system results in a final SIL of 0.33 i.e. the safety-instrumented functions in the protection system do not require to meet any specific reliability requirements. The PHR study also included an action to consider including an audible alarm on the gas holder roof to allow operators to evacuate on high level alarm. The effect of implementing this additional safeguard would be to alter the SIL score value for the possibility of avoiding the resulting hazard (P) from "B" to "A". This in turn would result in an overall initial nil SIL value for this scenario. Implementing this action would reinforce the conclusion that the safety-instrumented functions in this protection system are not required to meet specific reliability requirements.

**Scenario 2**: The initial SIL for this protection system is 3 and taking into account the number of IPLs in this protection system results in a final SIL of 1.5. The high initial SIL score reflects the high risk associated with this fault sequence. For high hazard/risk scenarios such as this one, the semi quantitative method of SIL evaluation presented in this paper is judged inappropriate. For these cases, the risk assessment used a more quantified risk analysis involving the use of frequency targets, consequence assessment and numerical estimates of the event frequencies. Risk targets needed to be set by the company prior to the study. The frequency targets for individual events as applied in the PHR study were $1 \times 10^{-5}$/yr and $1 \times 10^{-6}$/yr for "extremely serious" and "catastrophic" events respectively. As part of the quantified risk assessment, the initial categorization of Scenario 2 as being in the "catastrophic" category was confirmed by means of a consequence assessment combined with population data. The calculation of the event frequency without the safety-instrumented function was determined as follows:

Initiating event frequency

$= 1 \times 10^{-2}$/year (from operational experience)

Failure rate for explosion relief panels (IPL)

$= 1 \times 10^{-2}$/year (assumption)

Probability of workers in affected area

$= 0.1$ (plant data)

Probability of worker injury

$= 1$ (based on consequence modeling)

The resulting event frequency was $1 \times 10^{-5}$/yr. The required probability of failure on demand of the safety instrumented function i.e. the oxygen monitoring system is given by the ratio of the event frequency and the target frequency. In this case the required probability of failure on demand is 0.1 with a corresponding SIL of 1.0 (see Table 1).

## EXTENDING THE METHODOLOGY

In the case studies presented here, only engineered protection systems that are independent have been considered. This is clearly a conservative approach. Although this approach is satisfactory in many applications, there may be instances in which additional safeguards need to be considered including operator action. In this PHR methodology, human actions can be taken into account by assigning such actions an IPL score of 0.5 and a corresponding generic probability of failure on demand of 0.1. Alternatively, for high hazard/risk scenarios, specific failure probabilities can be determined using appropriate human reliability data. In addition, engineered safety systems that are not independent of each other can be modeled in terms of reliability using techniques such as fault tree analysis combined with appropriate failure rate data.

## CONCLUSIONS

This paper provides an example of the application of the LOPA and SIL assessment methodology as applied to new process plant. The purpose of the assessment was to determine the appropriate number of safeguards to ensure that fault sequences are ALARP and to determine the reliability required for safety-instrumented functions on the plant. A case study is presented which shows a method for carrying out a LOPA and SIL assessment and demonstrates how more quantitative techniques such as use of reliability data and frequency targets can be used where the semi quantitative approach is judged inappropriate.

## REFERENCES

1. IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems, International Electrotechnical Commission, Geneva, 1998 & 2000.
2. IEC 61511: Functional safety – Safety instrumented systems for the process industry sector, International Electrotechnical Commission, Geneva, 2003.
3. Centre for Chemical Process Safety (CCPS), Guidelines for safe automation of chemical processes, American Institute of Chemical Engineers, New York, NY, 1993.
4. UKOOA, Guidelines for instrument Based Protective Systems, 1995.