

PRACTICAL EXPERIENCE IN DETERMINING SAFETY INTEGRITY LEVELS FOR SAFETY INSTRUMENTED SYSTEMS

Graeme R Ellis[1], Senior Safety Consultant, and Mike Wharton[2], HSE Manager
[1]ABB Engineering Services, Daresbury Park, Daresbury, Warrington, Cheshire WA4 4BT, UK
[2]Great Lakes Manufacturing (UK) Ltd, Tenax Road, Trafford Park, Manchester M17 1WT, UK

Most plants in the process industry handling dangerous substances rely on safety instrumented systems (SIS) to ensure that accident risks are tolerable. IEC61508 provides guidance on the design and operation of SIS to ensure an adequate reliability in service, supported by guidance for the process sector in IEC61511. Many sites are now required to demonstrate compliance with these standards retrospectively, particularly sites being regulated by the HSE under COMAH. IEC61511 outlines a number of methods that may be used for SIL determination including risk-graph, layer of protection analysis (LOPA) and hazard analysis (HAZAN). This paper, to be jointly presented by Chemtura and ABB, describes the methodology for SIL determination on the COMAH 'top tier' site at Trafford Park. The paper discusses the practical experiences of SIL determination and the benefits of using a structured and staged approach.

KEYWORDS: SIL determination, IEC61508, risk graph, LOPA

INTRODUCTION

This paper describes the methodology and practical experiences of a Safety Integrity Level (SIL) determination for Great Lakes Manufacturing (UK) Ltd (hereinafter Chemtura) at the Trafford Park site. The objective was to identify existing Safety Instrumented Systems (SIS) that are critical to maintaining safe operation of the process plants. The SIS were assessed to determine the target reliability in terms of the required SIL in accordance with the standards IEC61508 [IEC, 1998] and IEC61511 [BSI, 2003], to ensure that they provide an appropriate level of risk reduction.

The Trafford Park site is regulated by the Health and Safety Executive (HSE) and Environmental Agency (EA) under the Control of Major Accident Hazard (COMAH) regulations as a 'top tier' site. As required by the regulations, a safety report was submitted to the HSE in 2000 and as part of the site improvement plan there was a requirement to carry out SIL determination for all the SIS on the site.

The SIL determination described in this paper deals with steps 3 to 5 of the safety lifecycle described in IEC61508, resulting in specification of the SIS safety functions and integrity requirements. As a follow-up to this work, there is a requirement to verify the design of the SIS and specify the proof test intervals, in accordance with step 9 of the safety lifecycle.

BACKGROUND

The Trafford Park site first started operations as 'The Geigy Colour Company Limited' on Christmas Eve 1939. In the last 30 years the Site has been owned by Ciba Geigy and then as FMC before being bought by Great Lakes Chemical Corporation in 1999. In July 2005 Crompton Corporation merged with Great Lakes to form Chemtura Corporation.

A range of speciality chemicals including phosphorus flame retardants and fluids as well as industrial water treatment additives are manufactured on the site in a number of batch processing plants. There are several hazards associated with the batch reactors such as internal explosion, reaction runaway or overfilling. Raw materials including flammable materials such a LPG and xylene, and toxic materials such as phenol and phosphorous oxychloride are stored in bulk tanks. Finished products are also stored in tanks, and some of these have the potential to cause harm to the environment.

The design of new and modified facilities is carried out by an internal projects group and throughout the changes in site ownership a consistent standard of design has been maintained. Most plants are controlled by a Distributed Control System (DCS) with separate hardwired trip systems for critical protection duties. A COMAH safety report was submitted to the HSE in 2000 detailing the hazardous events that could occur on the site and the technical measures in place, including SIS, to reduce the risk of such events to an acceptable level.

A key requirement for COMAH is to demonstrate that critical safety systems have been designed to meet relevant good practice. For SIS the benchmark standard is IEC61508 and IEC61511 or an equivalent. Chemtura concluded that it could not fully make this demonstration and therefore decided to carry out a compliance check for all the systems on site. The key areas of concern were a lack of documentation to clearly identify critical systems and to justify that the design and operation of the system ensures adequate reliability against the protected hazardous event.

Chemtura developed a screening tool for the assessment of instrumented systems in order to identify potentially critical systems that required further examination. The tool used was a simple qualitative assessment of the consequences of failure of the instrumented system on both people and the environment.

The systems identified in the screening exercise were then assessed using a SIL determination process based on the hazardous event severity matrix method described in Annex E of Part 5 of IEC61508. The hazardous event severity matrices were calibrated against tolerable risk criteria, and for persons located in hazardous areas for some for their working time, made allowances regarding assumed occupancy and likelihood of escape.

The SIL determination approach was reviewed after a number of assessments had been completed and raised two major concerns. The process had proved to be very time consuming taking several hours to complete each assessment. Also the process gave highly conservative results. It was expected that the majority of the safety instrumented functions would be rated at SIL 1 with the expectation of a possible small number of SIL 2 applications for very high hazard duties. In practice the majority of systems had been rated at SIL 2, with one or two at even higher levels.

Although recalibration of the hazardous event severity matrices was feasible and continued practice would help to increase the speed of the assessment, the decision was taken to consider an alternative approach.

REQUIREMENTS OF STANDARD

IEC61508 [IEC, 1998] is an international standard that sets out the principles and requirements for achieving functional safety with electrical, electronic and programmable electronic systems. The standard is non-mandatory but is generally regarded as a means of achieving best practice and is strongly supported in the UK by the HSE. Compliance with IEC61508 by COMAH sites is not enforced by HSE but they require a demonstration of equivalence for any alternative standard.

IEC61508 addresses the need to describe how reliable a safety instrumented system (SIS) needs to be, by using the concept of safety integrity level (SIL). The SIL of a SIS is defined in relation to the probability that it fails to perform the required protective function on demand, known as the average probability of failure on demand (PFD_{avg}). SIL Determination is the process of assessing the required PFD_{avg} for a specific SIS in order to provide adequate reliability and thereby reduce the risk of a specific hazardous event to an acceptable level. The relationship between PFD_{avg} and SIL is shown on Table 1.

IEC61508 applies to all sectors including industry, transport and health, and consequently uses concepts and terminology that are unfamiliar to the process sector. To address this issue IEC61511 [BSI, 2003] was issued, building on the requirements of IEC61508 and providing specific guidance to the process industry sector. Part 1 of IEC61511 describes the need for carrying out a process hazard and risk assessment to identify the overall safety requirements and then allocating the safety requirements that are required of the SIS. This has the following key steps:

- Identify the sequence of events leading to a hazardous event
- If practical modify the process design to be inherently safe
- Assess the consequences and likelihood of the hazardous event
- Determine the safety functions required to achieve the necessary risk reduction and if any of these are Safety Instrumented Functions (SIF)
- Determine for each SIF the associated Safety Integrity Level (SIL) that is required to ensure that the defined risk tolerability criteria is met

Table 1. Relationship between SIL and PFD

SIL	PFD_{avg} (band)
1	0.1–0.01
2	0.01–0.001
3	0.001–0.0001
4	0.0001–0.00001

Part 2 of IEC61511 states that in carrying out a hazard and risk assessment, "an organisation may use any technique that it considers to be effective, provided it results in a clear description of safety function and associated levels of performance". Guidance on methods to determine the required SIL is given in Part 3 of IEC61511. Figure 1, which is taken from the standard, shows graphically the risk-based approach that is required to demonstrate that the protective layers provide sufficient risk reduction to ensure that the residual risk is reduced to below the tolerable risk for a specific hazardous event. It should be noted that the assessment of protective layers needs to consider not only the SIS but also non-SIS prevention or mitigation measures.

The appendices of IEC61511 Part 3 contain a number of possible methods for SIL determination, in each case these provide an illustration of the general principles rather than a definitive methodology. The methods described in order of increasing complexity include:

- Semi-quantitative method
- Safety layer matrix
- Calibrated risk graph
- Risk graph based in DIN standard
- Layer of protection analysis

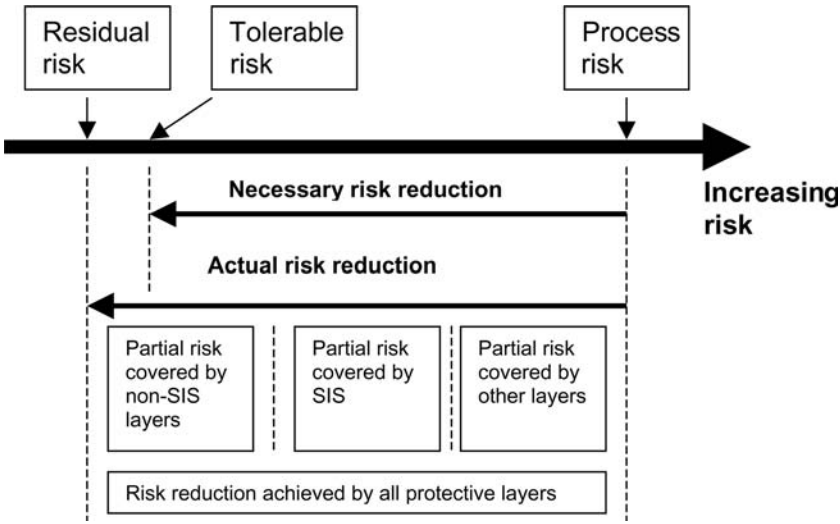

Figure 1. Risk reduction general concepts

SIL DETERMINATION METHOD

ABB has developed a standard methodology for retrospectively determining the SIL for existing safety instrumented systems. A challenge on existing sites is the large number of trip, alarm and interlock systems that need to be assessed. ABB has developed a staged approach as outlined in Figure 2. This approach has the objective of efficiently screening out low hazard and low risk events, with proportionately more detailed methods being applied to high consequence and high risk events. The approach utilises the risk graph method and layer of protection analysis (LOPA) methods from IEC61511, suitably calibrated against company and published risk criteria. In addition ABB utilises a more in depth quantified risk assessment (QRA) methodology for high risk situations, typically where the other methods are predicting the need for SIL2 or higher.

SIL determination team

It is essential that a knowledgeable and experienced multi-disciplinary team is used for the SIL determination study. As detailed in Part 3 of IEC61511, the following functions should be represented, led by a trained and experienced specialist:

- Operator of process under consideration
- Process engineer with knowledge of process design
- Representative of manufacturing management
- Process control engineer
- Instrument/Electrical technician with experience of process
- Risk analysis specialist

For the process area under consideration, all the reasonably foreseeable hazardous events with the potential to cause harm to people or the environment need to be identified. These include events such as fire or explosion, release of toxic gas or release of gases or liquids that can cause damage to the environment. A structured approach is used to identify both the hazardous event and all the credible initiating causes. This considers all stages of operation including; start-up, normal operation, shut-down, maintenance, loss of services, etc.

Any hazardous events that do not have an instrumented protective system (IPS) or do not require such a system to comply with relevant good practice can be eliminated at this stage. Other events can also be eliminated at this stage if the most severe consequences are limited to minor safety effects or business loss. The results of this process therefore provides a list of credible hazardous events with significant consequences that rely on one or more safety instrumented systems (SIS) to provide protection.

Identification of hazardous event

For new processes the hazard identification methodology in the design hazard studies 2 and/or hazard study 3 (HAZOP) are effective. If these records are available for existing plants then they can be used to prepare a list of the hazardous events for further assessment. In many cases however, it has been found that these records are unavailable,

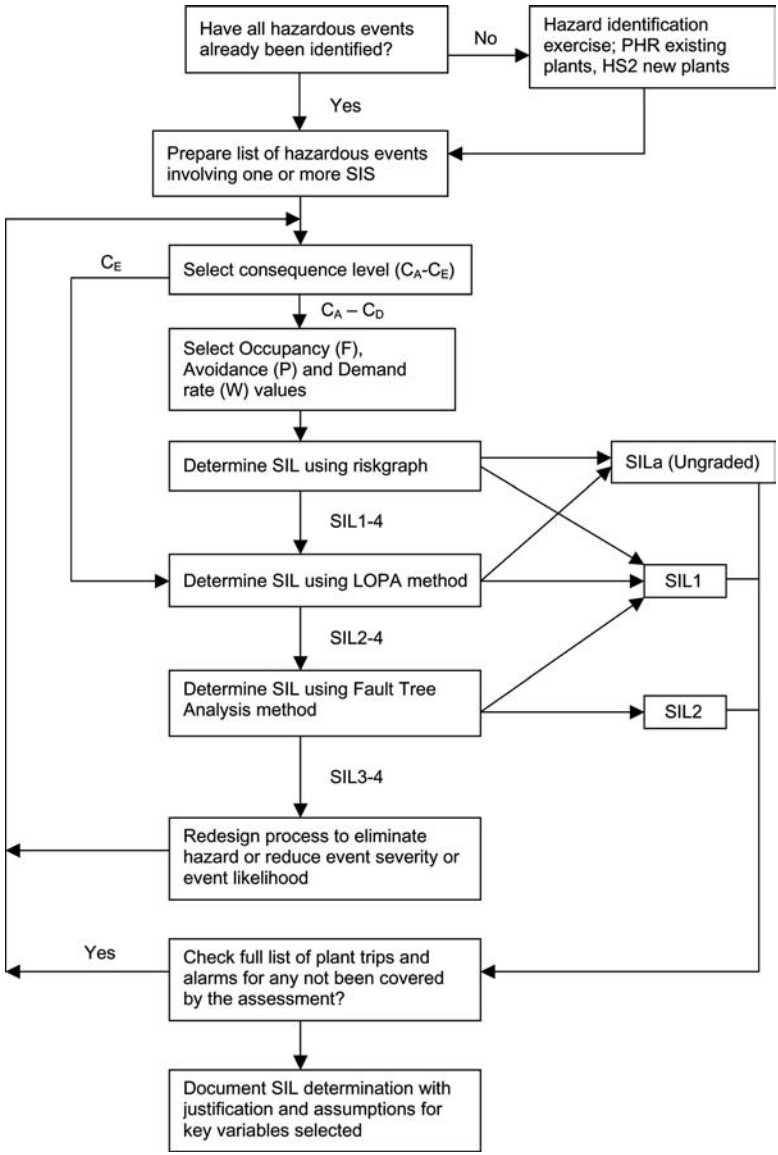

Figure 2. SIL determination methodology

incomplete or difficult to interpret. A particular weakness is a failure to identify the ultimate consequences of a process deviation, a common problem with HAZOP teams.

If further hazard identification is required for an existing process, ABB recommends use of a technique such as Process Hazard Review (PHR) or an equivalent [Ellis, 2005]. PHR is a team-based technique that considers each unit operation in turn and uses a set of guidewords to identify potential loss of containment scenarios. The method is much quicker than a comparable retrospective HAZOP study and is particularly effective in extracting the experience of operations staff.

Select consequence level

For each hazardous event the worst credible consequences are assessed in terms of harm to people or the environment, only taking credit for safety features that are inherent in the design or passive protection measures. The approach is conservative in nature to account for any uncertainty. This assessment is based on team judgement backed up by the results of consequence assessment modelling, the latter is recommended for events with the potential for major injury or fatality.

Based on the results of the consequence assessment a severity rating is selected in line with company risk criteria. For Chemtura at Trafford Park Table 2 provides word models for harm to people on-site with similar word models for people off-site, harm to the environment from airborne or water borne releases, and business loss.

For hazardous events that have a number of possible outcomes the worst case or dominant consequence level is assessed. In some cases it is necessary to consider more than one outcome from the hazardous event at the SIL determination stage. An example is the loss of containment of a flammable and eco-toxic material that could ignite and causes harm to people or run-off from the site causing harm to the environment.

Target event frequency

SIL determination is a risk-based approach based on company or published risk criteria. Such criteria provide guidance for the hazardous event frequency that would be considered 'as low as reasonably practicable' (ALARP). Chemtura risk criteria are based on published

Table 2. Word models for consequence category for on-site harm to people

Chemtura severity rating	SIL consequence level	Definition	On-site harm to people
1	C_E	Catastrophic	Multiple fatalities ($\sim$10)
2	C_D	Disastrous	Fatality or multiple major injuries
3	C_C	Serious	Major injury or multiple severe injuries
4	C_B	Significant	Reportable accident/LTA
5	C_A	Minor	First aid cases

data [HSE, 2001]. For example, the individual risk of fatality to a person off-site is judged to be broadly acceptable with no requirement for further risk reduction if the frequency is at or below 1×10^{-6} per year, and unacceptable if the frequency is above 1×10^{-4} per year. Between these limits the frequency should be reduced as far as reasonably practicable, hence it is known as the ALARP band. A practical target event frequency for an existing SIS is set towards the bottom end of the ALARP band at 3×10^{-6} per year, on the basis that any further risk reduction would require significant expenditure and could not therefore be justified.

Risk graph method

The risk graph method is a relatively simple approach for hazardous events with a severity in the range $C_A - C_D$, which is not suitable for more severe events classified as C_E. A number of parameters are initially assessed as detailed below.

The occupancy factor (F) is the fraction of time the exposed area is occupied by the person at greatest risk, with values of either F_B(100%) or F_A(10%). This must take into account an increased likelihood if the person initiates the hazardous event or is in the exposed area to investigate an abnormal occurrence in the build-up to the hazardous event.

The avoidance factor (P) is the probability that the exposed person is able to avoid the hazardous situation, with values of either P_B(100%) or P_A(10%). The latter value can only be claimed if there is an independent method of alerting the exposed person to the hazard and there is a means of escape. For environmental hazards, a 10% probability of the receptor not being exposed to the hazardous event can be used if there are mitigation barriers on the pathway to the receptor.

The demand rate (W) is the frequency at which the hazardous event would occur in the absence of any protective layers. The assessment of frequency needs to account for all the initiating causes that could lead to the hazardous event and include any allowable credit for control system intervention. Table 3 shows the values for the W and the word model to assist with selection of an appropriate value.

The above parameters for F, P and W, in conjunction with the C value determined earlier, are plotted on the risk graph in Figure 3 taken from part 3 of IEC61511.

The risk graph provides an overall SIL value for the protective systems from ungraded (SILa) to SIL4. To determine the SIL requirement for the SIS alone, the SIL for the non-SIS

Table 3. Demand rate word models

Demand rate (W)	Frequency per year	Word model guidance
W_1	<0.1	Could occur during remaining lifetime of plant
W_2	0.1–1.0	Has occurred during lifetime of plant
W_3	1.0–10.0	Has occurred several times

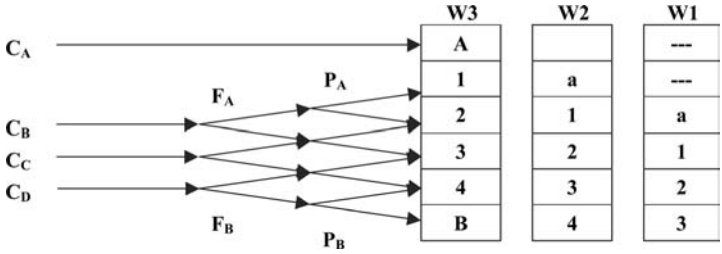

Figure 3. Calibrated risk graph

must be subtracted from this value. For example, if the overall requirement was SIL3 and a SIL2 relief system provided partial protection, the SIS would need to be SIL1.

This method is effective for quickly assessing an SIS as either ungraded (SILa) or SIL1. It is a conservative method and therefore tends to over-specify the SIL for more severe events. It is recommended that in these cases a more detailed method such as LOPA is used, as described below.

Layer of Protection Analysis (LOPA)

LOPA was initially developed in the US and details of the method have been published elsewhere [CCPS, 2001]. It provides a more in depth assessment than the risk graph method but can be completed fairly quickly compared with a technique such as fault tree analysis (FTA).

The hazard identification process described earlier should have identified all the credible initiating causes of the hazardous event, such as failures of equipment or human error. For each cause the LOPA team needs to estimate the failure frequency based on site experience with reference to generic failure rate data where available.

This is a key aspect of the LOPA process and it is recommended that relevant generic data is collected in advance. In addition it is important to maintain consistency and ensure that a conservative approach is taken to allow for uncertainty. For example, IEC61511 states that the failure rate of a standard basic process control system (BPCS) should not be better than 10^{-5} per hour, or approximately one failure in 10 years.

The LOPA team next identifies the protective layers that could prevent the hazardous event under consideration, such as relief systems, bunds and any other SIS. In order for a protective layer to be considered as a risk reduction measure it must meet all the following criteria:

- It prevents the undesired consequences when it functions as intended.
- It is independent of the initiating cause and the components of any other protective layer.
- Its performance can be validated.
- For human response, the operator must be trained and able to respond in time.

For each independent protective layer the LOPA team estimates the reliability or probability of failure on demand (PFD) using a similar approach to that for failure rate data described above. An initial estimate is made for the PFD_{avg} of the SIS at this stage, typically this would be mid-range SIL1 with a PFD_{avg} of 0.05. A spreadsheet is used to give an intermediate event frequency, such as a pool fire occurring on the plant. Each initiating cause frequency is multiplied by the PFD for the relevant IPL's, and the resulting frequencies are summed to give the intermediate event frequency. The benefit of this approach is that account can be taken of situations where IPL's provide protection for only some of the initiating causes.

To determine the hazardous event frequency, such as a pool fire causing a major injury, the intermediate event frequency is multiplied by estimates for the occupancy in the hazard area and the probability of avoiding the stated level of harm. These are similar to the F and P factors from the risk graph method except that any justifiable value can be used.

The final step in the LOPA method is to compare the estimated hazardous event frequency with the target frequency set earlier. If the estimated value is higher than the target then further protective layers may be required or the SIL rating of the SIS may need to be increased. Alternatively, if the value is much lower it may be possible to relax the SIL for the SIS. This stage of the process is iterative in nature and allows the design to be optimised in an effective manner.

Fault tree analysis

LOPA is effective in assessing most hazardous events, typically giving a rating of ungraded or SIL1. In some cases LOPA gives a SIL2 or higher requirement, typically for high severity or high-risk events. It is recommended that the SIL rating in these cases should be confirmed using a fully quantified technique such as Fault Tree Analysis (FTA). This paper does not describe the FTA method, details have been published by the IChemE [Turney, 1996].

PRACTICAL EXPERIENCE

The SIL Determination exercise for the Chemtura Trafford Park site was carried out over a 3–4 month period with half-day meetings approximately once per week. Before the meetings the Process Engineer prepared a list of all the instrumented protective systems (IPS) for the processes to be assessed and screened out any systems that could readily be identified as non-safety related.

A core team was assembled consisting of a facilitator from ABB, the Site Process Engineer and the Site Control/Instrument Engineer, supplemented by an appropriate operations representative for the process. The Process Engineer had been closely involved in preparation of the COMAH safety report and was familiar with the risk analysis contained in the report.

The key data required for the SIL determination was a list of IPS's, piping and instrument diagrams (P&ID) for the process being assessed and consequence assessment

details from the COMAH Safety Report. Previous hazard studies were generally not available in a suitable form and Process Hazard Review (PHR) was used to identify the hazardous events. The list of IPS's was also checked to confirm that all hazardous events on the process had been identified.

The staged process described in the previous section was generally used for the SIL Determination. The exception was that for all low severity events with consequence levels of 4 or 5, the SIS were assigned by default as 'ungraded', unless it was known that the demand rate was high. For the hazardous events at consequence levels 1 to 3, the risk graph screening stage was omitted and all systems assessed using LOPA.

A total of 175 IPS were assessed, of these 20 were found to be protecting against asset damage and were screened from further assessment. Of the remaining systems, 75 were assessed as protecting against hazardous events at GLCC severity levels 4 or 5, and hence assigned by default as 'ungraded'. For the remaining 80 systems, Table 4 shows the results of the SIL Determination, with 68% of the systems assessed as 'ungraded', 25% as SIL1, 7.5% as SIL2 and none higher than SIL2. It is felt that this split is typical of a plant in the chemical process sector, particularly the avoidance of any SIL3 or SIL4 systems.

Having identified a hazardous event the team was required to assess the worst credible consequences and based on this to assign a severity level. Use of word models facilitated this process but for more severe events the modelling carried out for the COMAH Safety Report was used for reference. In the absence of this information the team would have needed to take a pessimistic view of the likely outcome and make a recommendation for modelling to be carried out to confirm the assessment.

Failure rate and reliability data for the LOPA method proved to be a major discussion point for the team. The generic data on equipment failures and human error rates helped but these needed to be checked against plant experience. For example, there had been some experience of agitator blades becoming detached from their shaft, associated with runaway reaction hazards. Consideration of the number of reactors of this design and the instances of blades becoming detached within known memory, allowed an estimate of failure frequency to be made. There was also an action to review the method of attachment and propose an improvement. In all cases a clear record was made of the justification for the data used in the assessment, so that it could be challenged at a later date based on improved information.

Table 4. Results of SIL determination

Chemtura severity rating	Ungraded	SIL1	SIL2
1	9	5	3
2	18	3	3
3	27	12	0
Total	54 (68%)	20 (25%)	6 (7.5%)

LOPA is a fairly in-depth method that forces the process design to be reviewed in a detailed manner by the assessment team. One of the major benefits is a check of the protective layers, identifying concerns about reliability and in particular addressing any dependency between the protective layers. In addition the review allowed the process design and the number of protective layers to be re-assessed, especially where a high SIL was determined. Examples of issues raised by the team were as follows.

- Ensure the independence between protective layers, for example, avoiding control and protection sensors on a single impulse line.
- Confirm that process alarms are functional and that operators are trained and able to respond in a timely manner.
- Consider process improvements to reduce the severity or likelihood of an event. For example, providing a common vent line on storage tank farm allowing one tank to overflow into another, reducing the risk of loss from the system.
- Restricting access into a hazardous area, such as a bund, to reduce the probability of occupancy.

The SIL2 systems were generally associated with the potential for accumulation of reactants in a batch reactor leading to the potential for a runaway reaction. A previous reaction hazard assessment had shown that the reactor relief system was not sized for this event in the worst case, therefore placing a high requirement on the SIS. At the time of writing this paper, the reaction runaway hazard is being assessed using quantified risk assessment (QRA). The QRA involves fault tree analysis to provide a detailed estimate of event frequency and computer based consequence assessment modelling to estimate the severity of a reactor explosion. This will refine the SIL determination and allow further risk reduction measures to be considered in order to demonstrate that risks have been reduced to ALARP.

Having completed the SIL determination exercise giving a required SIL for all SIS on the site, the next stage is to verify the SIS design as achieving the required reliability. This must involve a competent Control Engineer and requires a verification of the design including an analysis of the SIS architecture and setting of appropriate proof test intervals.

CONCLUSIONS

This paper has described in detail a safety integrity level determination carried out for all the safety instrumented systems on the Chemtura site at Trafford Park, in accordance with the guidance in IEC61511. A staged approach was used to allow the study to progress in an efficient manner and ensure that the level of assessment was proportional to the scale and nature of the hazards.

The methodology was based on a proven generic approach developed by ABB, tailored to meet the specific requirements for the site and the company risk criteria. The SIL determination involved a small team of experienced staff with an independent facilitator from ABB. Challenges for the team were assessing the consequences of hazardous events and providing estimates for failure rates and reliability of protective systems. In the former

case the results of consequence assessment modelling proved useful and in the latter case generic reliability data backed by site experience was used. A team approach to making such judgements proven effective and a written justification for the data selected allows the values to be challenged in the future.

The results of the SIL determination were acceptable to the site, with most SIS assessed as 'ungraded', several SIL1 systems and a few SIL2 systems that are being re-assessed using a more detailed fault tree analysis method. The study raised a number of improvement recommendations due to the in-depth and structured methodology.

REFERENCES

IEC, Functional safety of electrical/electronic/programmable electronic safety-related systems, IEC61508, First edition 1998.

BSI, Functional Safety–Safety instrumented systems for the process industry sector, IEC61511, Parts 1, 2 &3, 2003.

Ellis G R, Action against accident hazards, Hydrocarbon Processing, March 2005.

HSE, Reducing risks, protecting people; HSE Books, 2001.

CCPS, Layer of Protection Analysis: Simplified process risk assessment, 2001.

Turney R & Pitblado R, Risk assessment in the process industries, 2nd edition, Institution of Chemical Engineers, 1996.