SIL DETERMINATION AND PROBLEMS WITH THE APPLICATION OF LOPA†

Alan G King
Hazard & Reliability Specialist, ABB Engineering Services, Billingham, Cleveland UK. TS23 4YS

For a number of years, industry has been trying to apply the principles outlined in IEC 61508. In the process industry, this has resulted in a focus on the requirements of IEC 61511. In the field of SIL Determination, IEC 61511 provides suggestions of a number of different techniques – these are shown in IEC 61511-3. These include Event Trees, Risk Graphs, Safety Matrices, Fault Trees and Layer of Protection Analysis (LOPA).

In the first few years after these standards were published, industry embraced the use of Risk Graphs as the method of choice. Over time, many companies have used this method and found that it was (a) giving higher safety integrity level targets than were really needed and (b) was less flexible than other methods and so more difficult to use in many cases. This has resulted in a general move to other methods and in particular to the use of LOPA. Indeed, LOPA may now be the "Method of Choice" for SIL Determination. However, there are a number of pitfalls in the use of the LOPA method that have become evident through its use.

This paper reviews the application of LOPA and provides insights into the use of the method. It will also highlight some of the pitfalls that have been found during reviews carried out of a number of existing studies in the UK. The paper will be of benefit both to those who are new to the LOPA method but also to those who have been using the method for some time.

KEYWORDS: IEC 61511, IEC 61508, functional safety, risk reduction, LOPA, layer of protection analysis

INTRODUCTION

The application of the international standards IEC 61508 [1] and IEC 61511 [2],[1] together with the other sector standards that have been generated from IEC 61508, are seen today as representing current good practice in the management of functional instrumented protective measures across industry. From its publication in 1998 and 2000, IEC 61508 has been progressively adopted by industry across the world as a way of demonstrating proper management, design and application of safety-instrumented systems. With the publication of IEC 61511 in 2003, the process industry sector has to a large extent embraced this standard as the way of demonstrating to regulators and others that appropriate risk management is in place.

These standards cover the whole of the safety lifecycle – from the initial concept through to operation and maintenance. Within the requirements in the early stages of the lifecycle, relating to Hazard and Risk Analysis, there is the need to determine for each safety instrumented function a necessary target performance – most usually related to its probability of failure on demand – and described by a safety integrity level (SIL).[2] This is the target performance needed for effective management of the level of risk. The process of setting an appropriate target performance for a safety-instrumented function is commonly referred to as "SIL Determination". Methods for SIL Determination are illustrated by examples in Part 5 of IEC 61508 and Part 3 of IEC 61511; one of these methods is Layer of Protection Analysis (LOPA).

Layer of Protection Analysis has been around for many years, certainly since the early 1990s. However, over the past 5 years, it has become perhaps the "Method of Choice" for SIL Determination. It provides a numeric and more transparent approach to setting target requirements for safety-instrumented functions than some other more qualitative methods. At the same time, it is not as time consuming to do compared with some other numeric methods. LOPA is also seen as setting more realistic targets with less built-in conservatism. It is therefore considered to be a particularly cost-effective approach to SIL Determination.

However, Layer of Protection Analysis has, since its recent rise in popularity, suffered from poor practice. Maybe this is because it is perceived to be "easy" and "straightforward" to do. This may be true as far as the mathematics is concerned. However, in practice there are a number of pitfalls and challenges of which every user of this method needs to be aware, and be able to tackle successfully. This paper will describe the LOPA method and then highlight some of the problem areas and how to tackle them. As such the paper is not only for those who are less familiar with the method but also for those already using Layer of Protection Analysis.

[1] IEC 61511 is the Process Sector standard derived from the generic standard IEC 61508 on instrumented Functional Safety.

[2] There are four safety integrity levels defined in the standards IEC 61508 and IEC 61511. SIL 1 is the lowest performance level and SIL 4 the highest.

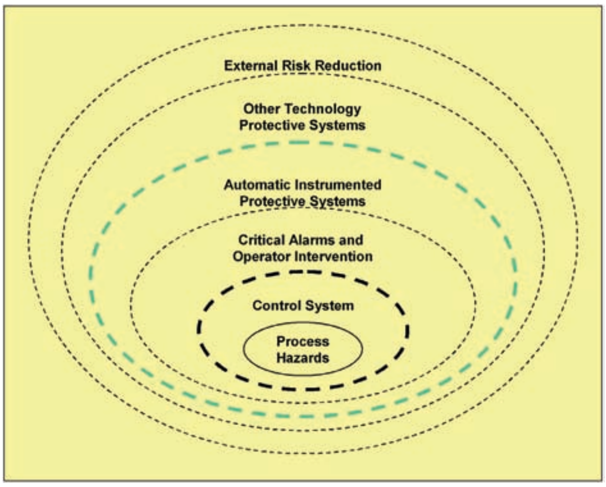
External Risk Reduction
Other Technology Protective Systems
Automatic Instrumented Protective Systems
Critical Alarms and Operator Intervention
Control System
Process Hazards

Figure 1. Layer model

WHAT IS LAYER OF PROTECTION ANALYSIS?

The layer model concept behind Layer of Protection Analysis is shown in Figure 1. Essentially, the process hazards are contained by the correctly operating control measures. Were the control measures never to fail, the hazards of the process would always be under control and further measures would not in theory be needed.

However, control measures do fail and the safe operation of the process then relies on the other layers to manage the process hazards. Firstly, critical alarms and operator intervention, followed by automated instrumented protective functions (trips and interlocks). Other technology measures such as pressure relief valves, and passive external measures such as blast walls and bunds around storage tanks apply when the instrumented measures have not performed.

The concept behind Layer of Protection Analysis is illustrated by the diagram shown in Figure 2.

On the right is the specific Hazardous Event of concern and, on the left, the Initiating Causes that could lead to that Hazardous Event. In between are the protective or risk reduction layers that can prevent the hazardous event from occurring. The diagram shows two Independent Protection Layers (IPL1 and IPL2), the principal Safety Instrumented Function (SIF) and one Conditional Modifier (CM1). Details of these terms will be described later.

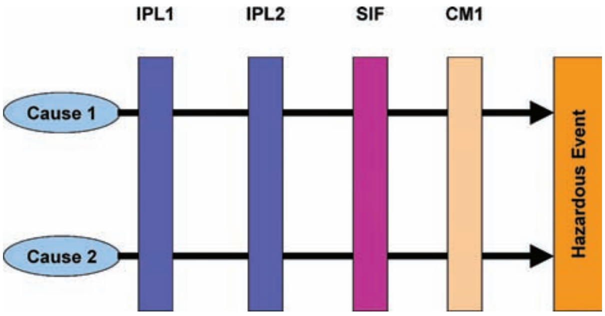

Figure 2. Layer of protection analysis

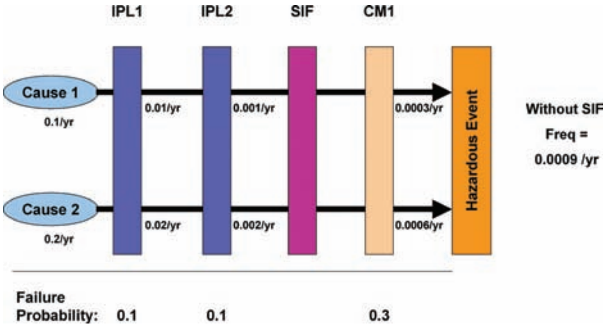

Figure 3. LOPA calculation

When conducting Layer of Protection Analysis, each of the initiating causes is assigned an appropriate frequency, and each of the risk reduction layers – excluding the safety Instrumented Function (SIF) – is assigned a probability of being in a failed state. The frequency of the hazardous event without contribution from the SIF is then calculated (see Figure 3).

In this illustration the hazardous event frequency without any contribution from the SIF is 0.0009 per year or 9×10^{-4} per year. The target frequency for the hazardous event (based on the severity of the event and the company risk criteria) is 1×10^{-5} per year. The ratio of these figures is $1/90$ or 0.011 and represents the average probability of failure on demand (PFDavg) required of the SIF to enable the target to be achieved. The analysis therefore concludes that for the principal Safety Instrumented Function the PFDavg must be a maximum of 0.011 and this is within the range for SIL 1.[3]

DEFINITIONS AND GUIDELINES FOR LAYERS

There are four types of layer to describe. The following sections review each type and indicate some guidelines for each of them.

INITIATING CAUSES AND ENABLING CONDITIONS

An Initiating Cause is a failure that, with no protective measures in place, can cause the hazardous event in question. For each initiating cause that is identified, an appropriate frequency of occurrence needs to be assigned. For example, failure of a particular temperature control loop on a specific plant may be an initiating cause and be known to occur around once in five years or 0.2/yr.

Some initiating causes may be associated with an enabling condition. An enabling condition may be defined as a condition that needs to be present to allow the initiating cause to start the sequence of events leading to the hazardous event. For example, if 40% of production involves

[3] For definitions of SIL 1 etc., see Part 1 of either IEC 61508 or IEC 61511.

manufacture of a temperature sensitive product, then the temperature control failure frequency would be multiplied by 40% in order to give the frequency with which failure of the temperature control loop occurs when a temperature sensitive product is being made, $f = 0.4 \times 0.2 = 0.08/\text{yr}$.

INDEPENDENT PROTECTION LAYERS

An Independent Protection Layer must be able to do three things: (a) Detect the value of a relevant process parameter, (b) Identify the parameter value as "out of limits" and (c) Take action to maintain a safe state or achieve a safe state. Essentially, it must be **effective** at preventing the hazardous event from occurring.

In addition to being effective, it must be **independent** from the Initiating Causes and also independent from all the other protection or risk reduction layers. It must also be **auditable** – an appropriate Probability of Failure on Demand (PFD) must be able to be justified.

SAFETY INSTRUMENTED FUNCTION

The principal Safety Instrumented Function (SIF) is the main safety instrumented function that protects against the specific hazardous event. The PFDavg for this function is determined by the Layer of Protection Analysis assessment.[4]

CONDITIONAL MODIFIERS

Conditional Modifiers are factors that relate to conditions necessary for the hazardous event to occur. These include factors such as:

- Occupancy – probability of a person in a position to be exposed to harm from the incident under consideration
- Occurrence of significant weather conditions
- Probability of ignition
- Likelihood of fatality
- Etc.

Each of these factors is expressed as a probability within the Layer of Protection Analysis. More information on this can be found in Reference [3].

LOPA PROBLEMS AND AVOIDING THEM

Layer of Protection Analysis can appear deceptively simple. This is perhaps the reason for many users being unaware of the problems and leading to mistakes in their analysis. This section will discuss a selection of problems seen by the author during independent review of Layer of Protection Analysis. It looks at each of the following areas: (a) Initiating Causes, (b) Independent Protection Layers, (c) Safety Instrumented Function, and (d) Conditional Modifiers. These are essentially the areas that users appear to find difficult when applying Layer of Protection Analysis.

Table 1. Initiating cause identification

	Type of initiating failure		
Mode of operation	Equipment	Human	Services
Normal operation			
Start-up			
Shutdown			
Abnormal (e.g. catalyst regeneration etc.)			
Maintenance			

PROBLEM AREA 1: INITIATING CAUSES

One of the key problems is not including all the initiating causes. Missing out causal failures means that the analysis will lead to insufficient risk reduction. This can be the result of a failure to think about issues upstream and downstream from the section of plant where the principal safety instrumented function is located. Very often, this means looking at the P&IDs for other sections of the plant.

The other factor is a failure to consider all modes of operation. It is too easy to think only about normal operation. It is important to review other modes of operation and to ask the question whether these may be associated with failures that could lead to the hazardous event in question. These modes of failure could include: Start-up, Shutdown, Abnormal modes of operation and also Maintenance activities.

In terms of failure, the obvious type of failure would be equipment failure – loss of control functionality. However, it is also important to consider other sources of failure, such as human failure and also failure of services such as steam, electrical power, cooling water, instrument air, etc. Any of these may be an initiating cause of the event in question.

To help ensure that all sources of initiating causes are included, a table similar to that shown in Table 1 could be used as a means of guiding thoughts and discussion.

In addition, it can be useful to create a demand tree[5] as a way to stimulate the identification of initiating causes in a systematic manner.

PROBLEM AREA 2: INDEPENDENT PROTECTION LAYERS (IPLs)

This section is going to look at three types of problems with IPLs: (a) claimed IPL not being a complete Independent Layer, (b) some problems with handling "Alarm Layers"

[4] There may in addition be other Safety Instrumented Functions providing risk reduction. Each of these other functions can be considered as an independent protection layer (IPL) if it meets the requirements for an IPL. For each of these functions an estimate of an appropriate PFDavg can be made, based on its architecture.

[5] A demand tree is a diagrammatic means of exploring causal failures prior to consideration of protective or risk reduction measures. For further information contact the author of this paper.

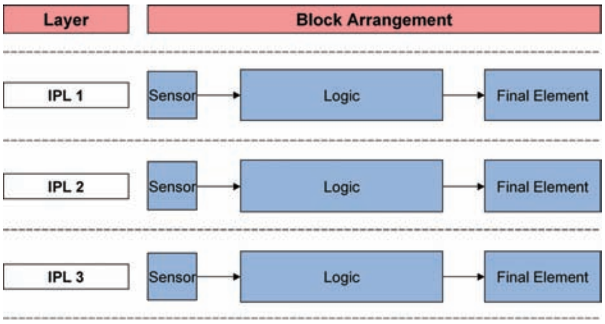

Figure 4. Independent complete layers

and (c) situations where some of the initiating causes are not protected by all IPLs.

(a) Incomplete Protection Layers
Each Independent Protection Layer needs to be both complete and independent. It needs to have its own independent means to (i) detect the value of a relevant process parameter, (ii) identify the parameter value as "out of limits", and (iii) take action to maintain a safe state or achieve a safe state. This concept is illustrated in Figure 4.

However, it is often not the case and the configuration is more like that shown in Figure 5. Both diagrams in Figure 5 are essentially the same arrangement; both lack completeness for IPL3.

What has been labelled as IPL3 is using the same Final Element as IPL2. It is not a complete layer and it is simply providing an additional sensor for IPL2. Its sensor should properly be considered as part of IPL2. This is shown in Figure 6.

The message here is don't simply count a sensor as a whole layer. If a sensor shares the same final element as another sensor, treat the two sensors together as a single layer.

(b) Alarm Layers
The same type of problem occurs with alarm layers. With alarms it is perhaps even easier to miss the issue. Consider Figure 7.

Figure 7 shows what a truly independent, complete alarm layer looks like. It is separate from the control layer and separate from the trip layer (SIF). Note, the operator action uses a different final element from that used by the control layer and also different from that used by the trip layer. This is important because the time when the situation totally relies on the operator action is when the trip layer is in a failed state; if the trip layer were in a working state, it would be able to prevent the hazardous event. Furthermore, the demand on the alarm layer may have come from a control layer failure and so the defined action needs to be independent from the control layer. Figures 8 to 11 show some examples of configurations where the alarm layer is not fully independent.

For the arrangement shown in Figure 8, a failure of the sensor often means both a loss of control and no activation of the alarm. For the arrangement shown in Figure 9, a failure of the sensor often means activation of neither the alarm nor the trip.

For the arrangement shown in Figure 10, a failure of the controller output or the control valve means that the alarm action will not be effective. For the arrangement shown in Figure 11, the successful action of the operator is only essential when the trip has a fault and will not function. The key issue here is to ask the question, "What do the operating instructions show for the response to the alarm?" It may well be that there is no indication in the instructions and the operator has been simply left to work out what to do should the alarm occur. The question should then be asked, "What independent action could the operator take in response to this alarm?"

It is vital that the LOPA analyst identifies any form of shared alarm arrangement. Failure to do so will result it a higher level of residual risk. It is possible to adapt LOPA to model the actual sharing across the layers or to use Fault Tree Analysis (FTA) to model the actual arrangement. However, if the alarm layer is not a complete independent layer, then the conservative approach is not to claim any risk reduction for the alarm layer.

Another issue relating to alarms, which receives less attention than it deserves, is the time available for response. Too often, the probability of no response to an alarm is set at 0.1 with no justification given for the value selected. The

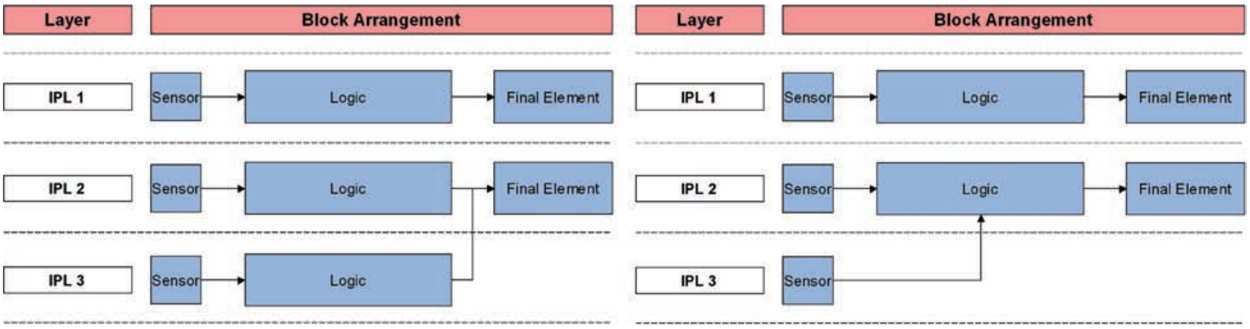

Figure 5. IPL3 is no longer a complete independent layer

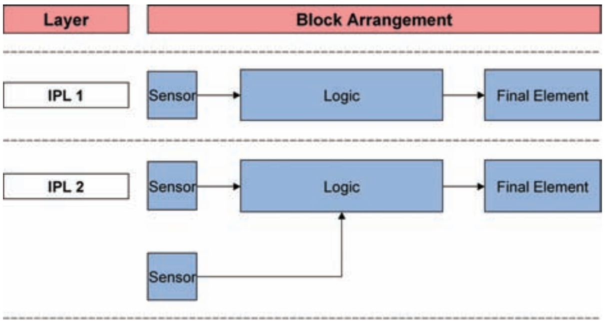

Figure 6. What was the IPL3 sensor now incorporated into IPL2

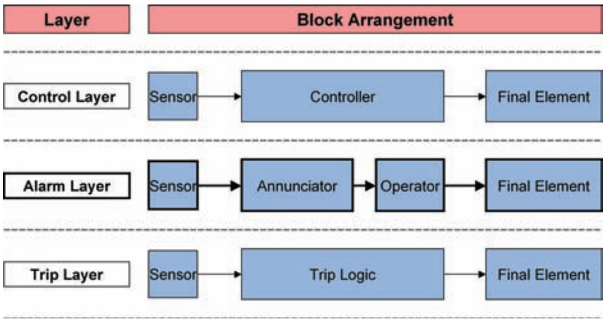

Figure 7. A fully independent "alarm layer"

time available for response to an alarm can be quite short and it can also require some level of process diagnosis before a decision on an appropriate response can be made.

Figure 12 shows the sequence following a process alarm. The maximum time available for response can be assessed from the alarm set point and the rate of change of the process conditions. It is all too easy when discussing response to an alarm to envisage a single alarm appearing and an operator acting under ideal conditions. Whilst the attention of the operator may be drawn to an alarm quite quickly by its visual and audible annunciation, working out what is happening to the process and what best to do may take significantly longer; the operator may indeed wish to consult the shift manager before taking action, e.g. to stop the plant. Furthermore, the means of action may not be in the control room itself. Human Error Probability (HEP) assessment for use with LOPA needs to be conservative rather than optimistic. The following graph for diagnosis and decision-making is based on the CCPS guidance in "Guidelines for Chemical Process Quantitative Risk Analysis"[6] and is also to be found in the THERP[7] methodology for screening purposes.

This suggests that for a human error probability of 0.1 associated with diagnosis, the time available for diagnosis and decision should be a minimum of 20 minutes together with additional time to allow for communication and action.

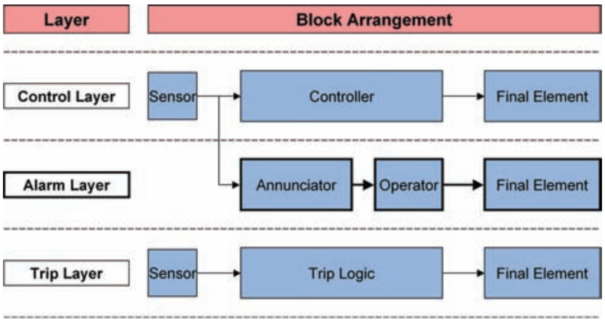

Figure 8. Alarm shares control sensor

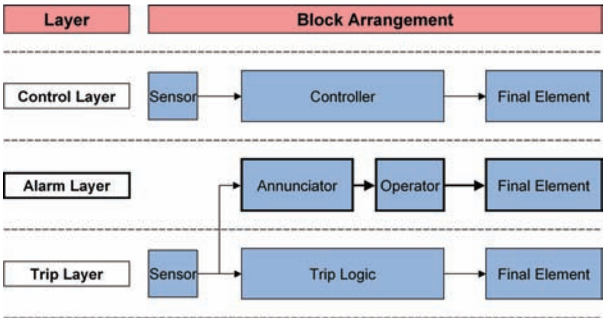

Figure 9. Alarm shares trip sensor

(c) Not all Initiating Causes Protected by all IPLs

With some types of LOPA analysis, the methodology builds in the assumption that each IPL protects against all the initiating causes. This is frequently not the case. What does this look like and how does it impact on the LOPA assessment? It is illustrated in Figure 14 below and needs either (a) a flexible LOPA method or (b) a change to use Fault Tree Analysis (FTA).

All of the layers affect all initiating causes, except for IPL2 which provides no risk reduction for Cause 3 and for IPL3 which provides risk reduction for Cause 3 alone.

PROBLEM AREA 3: PRINCIPAL SAFETY INSTRUMENTED FUNCTION NOT PROTECTING ALL INITIATING CAUSES

The assumption is usually made that the principal safety instrumented function (SIF) protects against all the initiating causes of the hazardous event in question. This is usually true but is not always the case. This is illustrated in the following example.

[6] "Guidelines for Chemical Process Quantitative Risk Analysis" 2nd Edition CCPS, 2000

[7] THERP: Technique for Human Error Rate Prediction in "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications" – A D Swain & H E Guttmann, NUREG/CR-1278 August 1983.

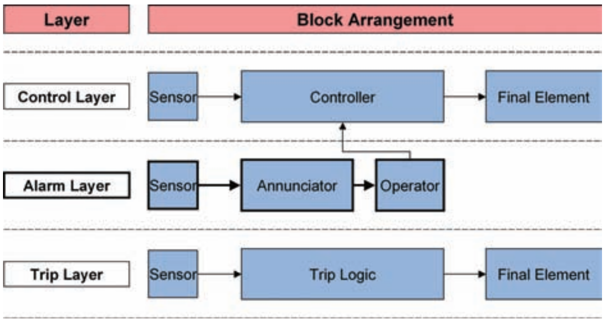

Figure 10. Operator uses control for response

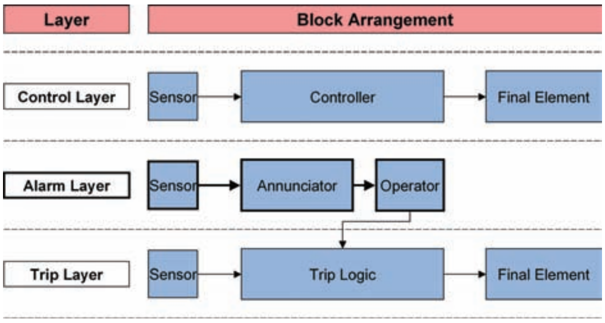

Figure 11. Operator uses trip for response

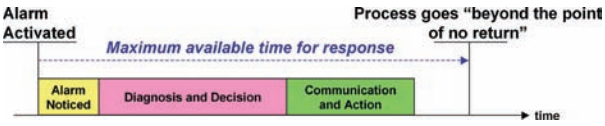
Alarm Activated
Process goes "beyond the point of no return"
Maximum available time for response
Alarm Noticed
Diagnosis and Decision
Communication and Action
time

Figure 12. Model indicative of alarm response

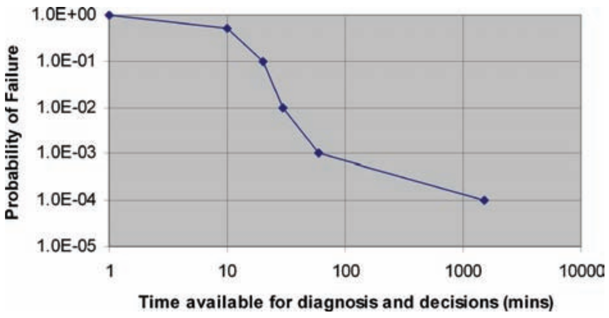

Figure 13. Model indicative of time for diagnosis and decisions

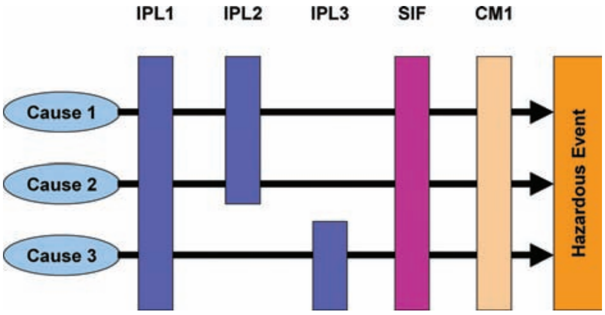

Figure 14. Not every IPL protects all initiating causes

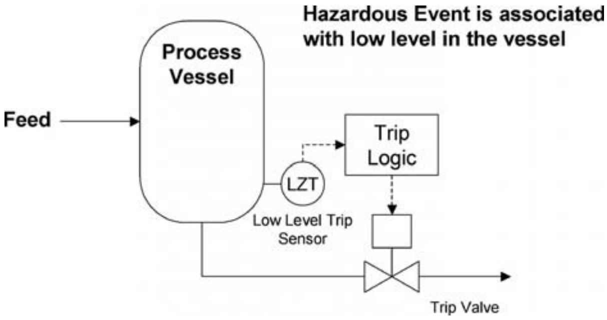

Figure 15. Process vessel with a low level trip function

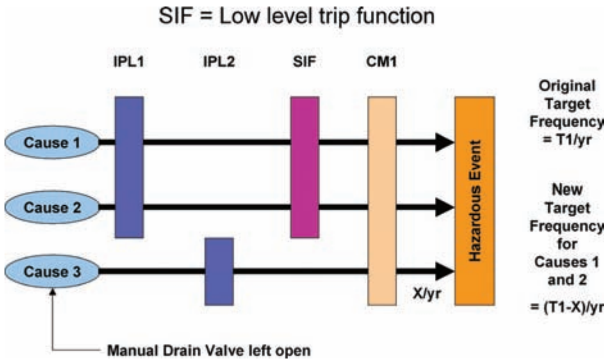
SIF = Low level trip function
IPL1
IPL2
SIF
CM1
Cause 1
Cause 2
Cause 3
Hazardous Event
X/yr
Original Target Frequency = T1/yr
New Target Frequency for Causes 1 and 2
= (T1-X)/yr
Manual Drain Valve left open

Figure 16. LOPA assessment of the hazardous event

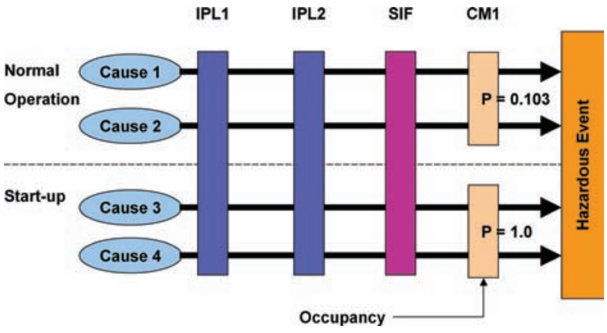

Figure 17. LOPA assessment including occupancy as CM1

Figure 15 shows a process vessel with a low level trip safety instrumented function. The hazardous event of concern is associated with low level in the vessel.

The concern here is that for one of the initiating causes, i.e. leaving the manual drain valve open, there is no protection from the principal Safety Instrumented Function, the low level trip. This means that the analyst needs to assess the contribution to the hazardous event frequency from this cause and then subtract this contribution from the original target frequency for the hazardous event. This new target frequency is used to determine the SIL requirements for the principal Safety Instrumented Function – the low level trip. This is illustrated schematically in Figure 16.

PROBLEM AREA 4: CONDITIONAL MODIFIERS

Conditional Modifiers represent one of the more difficult factors to include in the analysis. The factors in this category include: Occupancy,[8] weather conditions, ignition etc., as discussed earlier. One of the problems with conditional modifiers is providing reasonable justification for the values used.

This paper focuses briefly on one of these modifiers: Occupancy. Factors affecting the occupancy probability include:

- Day or Night – some activities only occur during normal day hours (8 hr) – e.g. planned maintenance
- Routine activities that occur regularly throughout 24 hrs when plant is running – e.g. walk-round, sampling etc.
- Occasional activities associated with specific plant operating modes – operator actions for start-up
- Plant upset policy – investigation by operators.

There may need to be a different occupancy probability for different modes of plant operation – normal occupancy, start-up etc.

Occupancy Example

For Start-up, let us assume that the probability of a person being present is 1.

For Normal Operation, let us assume that there are two components: (a) a routine patrol that takes place every 8-hour shift and involves spending 10 minutes in the relevant area on each occasion. In addition, there are (b) maintenance activities limited to day hours (8 hours in 24 hrs) with an estimate of occurrence on 25% of days during the year.

$$\begin{aligned}\text{Probability of person present (routine)} &= 3 \times 10/(24 \times 60)\\ &= 0.02\\ \text{Probability of person present (maintenance)} &= 0.25 \times 8/24\\ &= 0.083\\ \text{Overall estimate of occupancy probability} &= 0.02 + 0.083\\ \text{(for normal operation)} &= 0.103\end{aligned}$$

When this is applied to Layer of Protection Analysis, it appears as illustrated in Figure 17.

CONCLUSIONS

Layer of Protection Analysis (LOPA) is an increasingly popular method for SIL Determination. However, there are a number of shortcomings in its application across industry. This paper has highlighted many of them and indicated how to avoid the associated problems. The use of Layer of Protection Analysis needs well-trained and experienced people to lead assessments to ensure successful outcomes; otherwise, the level of risk reduction installed across industry will be less than adequate to meet the intended risk targets.

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. “Layer of Protection Analysis – Simplified Process Risk Assessment”, CCPS 2001.
4. “Guidelines for Chemical Process Quantitative Risk Analysis” Second Edition CCPS 2000.
5. “Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications” – Final Report, A D Swain & H E Guttmann, NUREG/CR 1278.

[8] The probability of a person in a position to be exposed to the incident under consideration.