COMMON MISUNDERSTANDINGS ABOUT THE PRACTICAL APPLICATION OF IEC 61508

Helen Pearce, James Catmur and Geoff Stevens

The use of IEC 61508 for determination of the Safety Integrity Level (SIL) of Safety Interlock Systems on refinery and petrochemical process plant is becoming commonplace. Many firms have started to incorporate the assessment for SIL into their Hazard and Operability (HAZOP) procedure for the identification of hazards in new build facilities. Aside from the practical pitfalls of combining HAZOP and SIL assessment, we have encountered instances suggesting the importance of risk criteria in applying IEC 61508 is not always understood.

This paper discusses the risk graph method (the example included in the IEC standard), and the pitfalls if the illustrations from the standard are applied without calibration for risk criteria. A variety of situations are reviewed, drawing on practical examples taken from HAZOP studies. A tool are calibration of the risk graph method is described and its integration into software used for HAZOP recording is explained. The approach provides a preliminary SIL assessment as part of the HAZOP process and leads into a separate review stage involving the HAZOP team and other specialists involved in the design and validation of the SIL classification.

INTRODUCTION

Many firms have adopted the IEC (International Electrotechnical Commission) Standard 61508 as central to their specification, design and operation of Safety Instrumented Systems (SIS). This standard (together with the associated IEC 61511 which has been developed specifically for the process sector) contains specific examples of methods to implement the standard such as the risk graph method that will be discussed in this paper. We notice that firms go straight to the application of these examples in their written procedures and in their web sites, without apparently considering the selection of risk criteria which we think is embodied in the standard. This paper revisits the principles, especially the selection of the tolerable risk target, and shows how this affects the practical implementation of the risk graph method. The discussion will include procedures that we believe allow the assessment of safety integrity to be implemented while avoiding some of the pitfalls. In our approach we have treated SIL determination as a specific case where all of the general issues relating to Quantified Risk Assessment apply.

SOME PRACTICAL PITFALLS IMPLEMENTING IEC 61508

In the practical application of the standard to a particular process plant we have worked from the point of view that there is no single provably correct solution. That means the acceptability of a particular application is to be determined by reference to the hazards assessed in the case in question following “industry good practice”. However, what constitutes good practice on the subject of SIL determination has yet to be established across the industry. The aim of this paper is to discuss a number of aspects of the subject that need to be addressed by the industry in order to promote greater uniformity in SIL determination.

We have found three practical problems which need to be addressed in the scope of good practice:

- Incomplete understanding of the process hazards which the SIS is designed to control
- Misunderstanding about allowances which are appropriate for other risk control devices, leading to incorrect application of broad “Rules of Thumb”
- Confusion on the contribution of systems involving operator intervention

The consequence of such difficulties can be excessive unproductive time taken for the SIL assignment or variability in the results of the assessment. One of the desirable aspects of using a standard should be that another group looking at the same system reproduces results from the original group involved in the assessment. We have found in applications of the risk graph method this is not always the case. Hauge, Hokstad and Onshus[2] go even further and report that a new group of people analyzing the same system is very likely to come up with SIL requirements different from the original analysis team.

IMPROVING UNDERSTANDING OF HAZARDS

Typical project procedures require SIL assessment for all Emergency Shut down (ESD) instrumented protection systems and these are commonly defined on cause & effects charts for the relevant unit. In our approach to HAZOP we include the cause and effect diagrams not as a specific Piping and Instrumentation Diagram (P&ID) node, but as a separate item at the end of the HAZOP of a plant section or the overall plant. It is often useful to include major plant hazards identified in earlier nodes to review the extent to which the instrumented protection system is effective in responding to the scenario. The IPS is not always the appropriate response and in such cases we also look to the described step by step. In our view, part of the difficulty applying IEC 61508 comes when those involved in SIL assessment have not shared the HAZOP discussion of the hazard that the system is designed to control.

Where there are a number of ESD trips associated with a unit hazard, for example reduced process side flow through a high intensity steam reforming furnace, possible hazard scenarios are explored using the HAZOP deviations ‘Low hydrocarbon feed flow’ and ‘Low steam/carbon ratio’. The team can develop an understanding of the need to protect the reformer tubes from overheating, causing thermal damage and potential rupture. Mechanisms for overheating include either reduced circulatory cooling, for example if there is local coking, or cessation of endothermic reforming reaction. The process designer may typically include high integrity Flow Alarm Low Low (FALL) sensor arrangements on each furnace pass in the ESD loops, but sometimes Temperature Alarm High High (TAHH) sensors are used on the exit of each pass from the radiant section. Occasionally you come across furnaces with both protections. Reliability concerns make skin thermocouples less common for the instrumented protection system (IPS) bur are often a supplementary warning high temperature (TAH) alarm for the console operator.

In the case discussed, the ESD system action typically leads to isolation of all natural gas (and other fuels to the furnace if present) and isolation of feed process streams including trip of any circulating compressors.

We have found difficulties arise when start-up conditions are considered in isolation from normal process flow. The process designer may provide a 20% mechanical stop on the steam isolation valve to maintain a minimum flow during normal process operation. This means it will not be possible to isolate using the valve with the minimum stop. If however, the instrument engineer believes maintaining this flow is not necessary provided the reformer firing has been stopped (because the circulating steam will cool and eventually become wet, potentially damaging the reformer or shift catalysts), the cause and effect diagram may show closure of the steam isolation valve. This conflicts with the process designer's intention to provide a 20% mechanical stop on this valve.

The point is that such issues need to be settled at the HAZOP stage. If they are not resolved (but surface during SIL assessment), protracted unfruitful argument may result.

REPEATING ASSESSMENT FOR SIMILAR FUNCTIONS

Another aspect we have found in teams working in parallel confirms the finding of Hauge, Hokstad and Onshus[2] that large amounts of additional analysis can sometimes be generated to determine SIL requirements for what are more or less standard safety functions. In particular, we have found the risk graph method can lead to quite heated debate on matters such as the credit to be given for protective systems other than the SIS and how the SIS must override protective features provided by the process designer.

FAILURE TO SELECT A RISK CRITERION

Although the IEC 61508 standard explains that a risk acceptability criterion must be established before the standard can be applied, we have found understanding of risk criteria and their relationship to IEC 61508 is often incomplete.

While some approaches use an "Event severity classification" including human safety, property damage and business interruption, other SIL procedures focus only on plant safety. Economic losses (downtime or equipment damage) are generally not considered. But typically in HAZOP discussions, the team recognizes that economic loss can be severe (due to interrelation of many Units, e.g. whole refinery shuts down for many individual unit prolonged outages) and make recommendations to improve the operability (and hence the service factor) of the facility. With a narrow "safety only" focus there is a danger that the process licensors' high integrity process protection designs will be downgraded to the minimum safety SIL rating without considering the economic impact on plant operations.

RELATIONSHIP BETWEEN HAZOP RECOMMENDATION, RISK SEVERITY AND SIL

It is expected that properly conducted HAZOP studies led by different chairmen on different plants of the same type would identify the same hazard and offer comparable recommendations. For example, in the reformer case described above, the high integrity FALL unit trip might be described with independent sensors perhaps voting 2 of 3.

However, it could be that on the first plant furnace tube rupture was one of only three potentially fatal hazards and the SIL assessment might show that the sensors needed to be a SIL 1 protection system. If on the second plant the rupture was one of 100 potentially fatal hazards, the SIL assessment based on the same risk criterion might recommend that the protection system be SIL 3.

This means that the same HAZOP recommendation might be discussed in both cases, but for the plant that is more dangerous overall (larger number of significant hazards) the SIL assessment would ensure that the protection function has a higher SIL delivering a higher level of confidence that the SIS will shut down the plant when required to do so.

This concept aligns to the ALARP (As Low As Reasonably Practicable) principle. If the plant has only a few significant hazards it is likely to be closer to the tolerable risk level. Therefore the level of resource you should expend to reduce each risk could be quite low (as implied by SIL 1). If the plant has many hazards the overall risk is likely to be closer to the intolerable limit so, according to the ALARP principle, you should expend more effort to reduce each risk (as implied by SIL 3). In fact, in this situation, the first priority should be to reduce the overall level of risk by reducing the risks associated with the hazards at source rather than by increasing the integrity of means of protection.

This approach to SIL should not be interpreted as 'designing down' the protection system integrity to achieve a maximum tolerable (plant wide) risk threshold. This is contrary to the ALARP philosophy, particularly in its contemporary interpretation. Rather we think it is sensible to adopt a mid-range risk criterion between upper and lower ALARP limits from the outset.

Many consider SIL sets a reliability target for an IPS/ESD loop, based on the risk associated with the failure scenario it is intended to protect against. The preceding arguments suggest it is not just the risk of the particular scenario, but the risk in the context of all the hazard scenarios on the facility and their contribution to the overall risk acceptability criterion.

SPREADSHEET FOR SIL ESTIMATION

We have developed two spreadsheets to assist the implementation of IEC 61508 procedures. The spreadsheets serve to set out the procedures in the standard step by step to assist those involved in the SIL assessment understand the approach. They also record the findings so that the completed forms act as a record of the assessment team proceedings.

In the simple spreadsheet, a form is used to describe the section of plant being considered. The design intent is entered as well as the hazardous scenario. These can come directly from the HAZOP team report if the SIL assessment is carried out immediately after completion of the HAZOP study in the way we recommend.

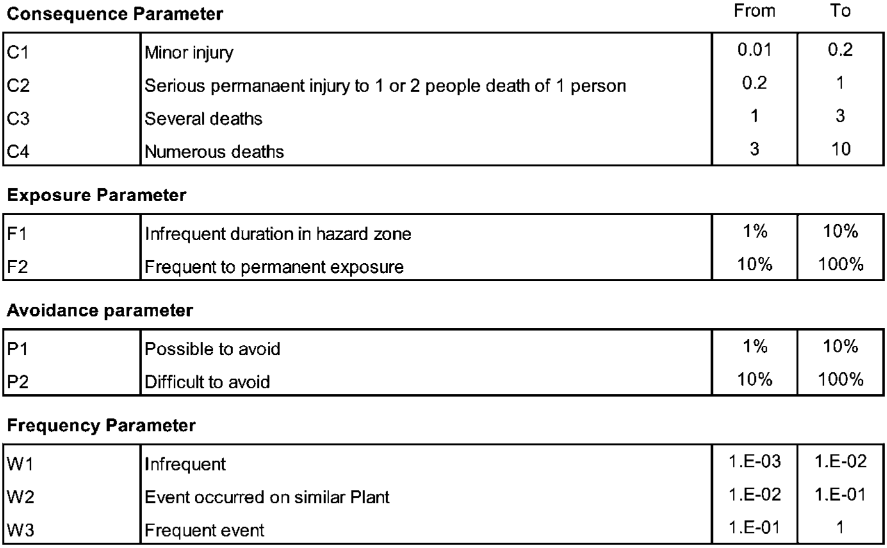
The form is completed by entering values for Frequency (W in the IEC 61508 risk graph approach), Consequence, Exposure and Avoidance. We use the terms as described in the standard and in addition suggest numerical ranges to completely clarify the meaning we understand from the text. The following ranges are those we suggest (see Figure 1).

To assist further the selection of frequency parameter W, we provide a simple table of types of control loop with suggested failure frequencies (see Table 1). The Assessment team can begin the assessment by first entering the type of instrumentation and then proceed to consider if they are content with the initial suggestion or have reasons to vary it for the system under consideration.

The table can then be completed as the SIL assessment team debates their view step by step. In practice it is convenient to project the computer screen so that participants can see their assessment as it is entered.

As well as the parameters defined in the IEC 61508 standard the form provides a means of making an allowance for additional protection independent of the IPS being evaluated. The following table (Table 2) shows the meaning of the values entered.

Under certain circumstances it is reasonable to take account of physical protective measures when assessing consequence and likelihood to a particular IPS demand scenario. For example, if a Pressure Safety Valve (PSV) is provided which has been sized to protect against the same hazard scenario as an IPS (for example a Level Alarm Low Low (LALL) covering an level control/level alarm Low (LC/LAL) arrangement) it is reasonable to



Consequence Parameter

		From	To
C1	Minor injury	0.01	0.2
C2	Serious permanaent injury to 1 or 2 people death of 1 person	0.2	1
C3	Several deaths	1	3
C4	Numerous deaths	3	10

Exposure Parameter

F1	Infrequent duration in hazard zone	1%	10%
F2	Frequent to permanent exposure	10%	100%

Avoidance parameter

P1	Possible to avoid	1%	10%
P2	Difficult to avoid	10%	100%

Frequency Parameter

W1	Infrequent	1.E-03	1.E-02
W2	Event occurred on similar Plant	1.E-02	1.E-01
W3	Frequent event	1.E-01	1

Figure 1.

Table 1. Suggested frequencies

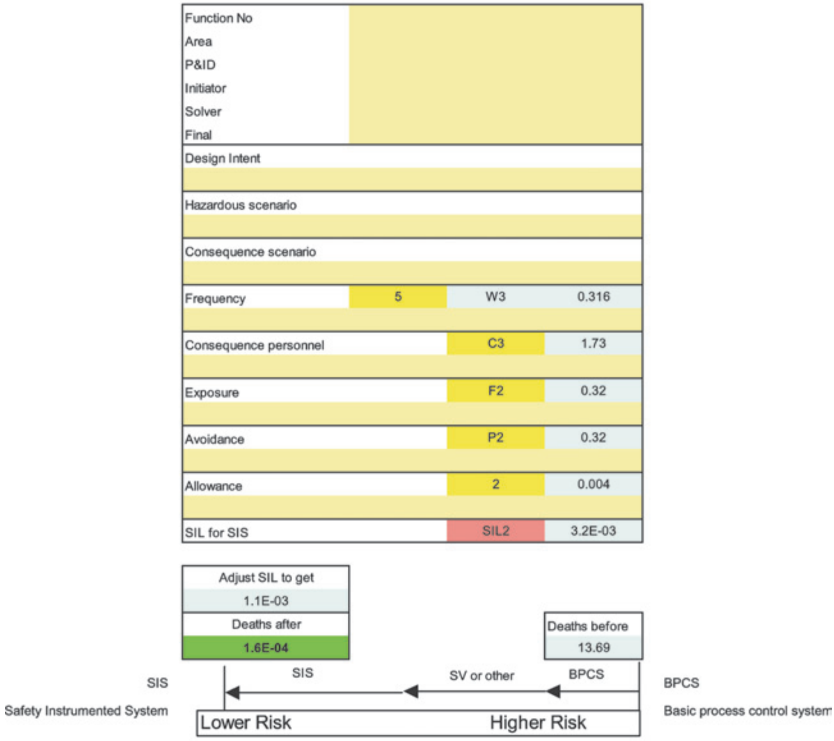
ID	Loop	Value (pa)	Frequency Parameter
1	TI Temperature Indicator	0.09	W2
2	LI Level Indicator	0.55	W3
3	PI Pressure Indicator	0.34	W3
4	TCV Temperature Control Valve	0.27	W3
5	LCV Level Control Valve	0.50	W3
6	PCV Pressure Control Valve	0.09	W2
7	TS Temperature Switch	0.09	W2
8	LS Level Switch	0.06	W2
9	PS Pressure Switch	0.18	W3
10	Pump	0.08	W2
11	Vessel	0.001	W1
12	Pipe	0.001	W1

assume that if the primary control system fails in some way there will be a demand which can be met by either the PSV or the IPS. The ESD system is provided to stop loss of level leading to gas breakthrough and downstream vessel pressurisation. If the ESD system were not provided, or did not work, gas blow-by would result in the downstream vessel becoming pressurised. If the relief valve is also provided and designed for this case, some allowance should be provided when the SIL for the ESD is assessed.

The simple spreadsheet provides only a partial approach to SIL assessment because it does not explicitly require a risk tolerance level to be set. We have developed a more detailed approach based on a ranking matrix which requires a specific risk target, such

Table 2. Protection allowance

ID	Loop	Value (pa)
1	MOV Motor Operated Valve	0.003
2	PSV Pressure Safety Valve	0.004
3	Human error without training	1
4	Initial training only	1
5	Retraining class room	0.3
6	Recertification simulator	0.1
7	Initial training only	1
8	Retraining class room	0.1
9	Recertification simulator	0.01



Function No			
Area			
P&ID			
Initiator			
Solver			
Final			
Design Intent			
Hazardous scenario			
Consequence scenario			
Frequency	5	W3	0.316
Consequence personnel		C3	1.73
Exposure		F2	0.32
Avoidance		P2	0.32
Allowance		2	0.004
SIL for SIS		SIL2	3.2E-03

Adjust SIL to get
1.1E-03
Deaths after
1.6E-04

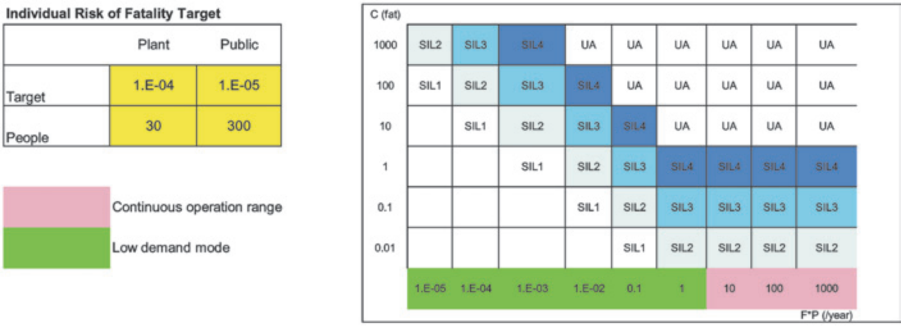
Deaths before
13.69

Figure 2.

as individual risk of fatality criteria for staff and public. The method generates a diagram showing the SIL requirement for particular combinations of consequence and frequency of occurrence (see Figure 3).

EXAMPLE OF USE OF SPREADSHEET IN PRACTICE

Some of the pitfalls applying IEC 61508 can be avoided by linking the HAZOP study of a unit with the SIL assessment. In this way the experience of the HAZOP leaders in developing team working can be harnessed to reviewing the related aspects of control systems and ESD interlocks. The application of IEC 61508 requires consensus on the risk ranking of hazardous effects from loss of containment and/or critical instrument or protection system failure. The discussions in the HAZOP provide a basis for developing such a consensus.



Individual Risk of Fatality Target

	Plant	Public
Target	1.E-04	1.E-05
People	30	300

🟥 Continuous operation range

🟩 Low demand mode

C (fat)									
1000	SIL2	SIL3	SIL4	UA	UA	UA	UA	UA	UA
100	SIL1	SIL2	SIL3	SIL4	UA	UA	UA	UA	UA
10		SIL1	SIL2	SIL3	SIL4	UA	UA	UA	UA
1			SIL1	SIL2	SIL3	SIL4	SIL4	SIL4	SIL4
0.1				SIL1	SIL2	SIL3	SIL3	SIL3	SIL3
0.01					SIL1	SIL2	SIL2	SIL2	SIL2
	1.E-05	1.E-04	1.E-03	1.E-02	0.1	1	10	100	1000

F*P (/year)

Figure 3.

We have found it helpful to introduce the SIL sessions by writing up some ground rules which include describing ESD loops the SIL is applied only to with reference to a cause & effect diagram (see Figure 4).

The value of linking HAZOP to SIL is partly to compress the overall schedule for both studies by transfer of understanding on hazards from the HAZOP to the SIL assessment. During the HAZOP study, we identify instrumented protection systems (IPSs) that

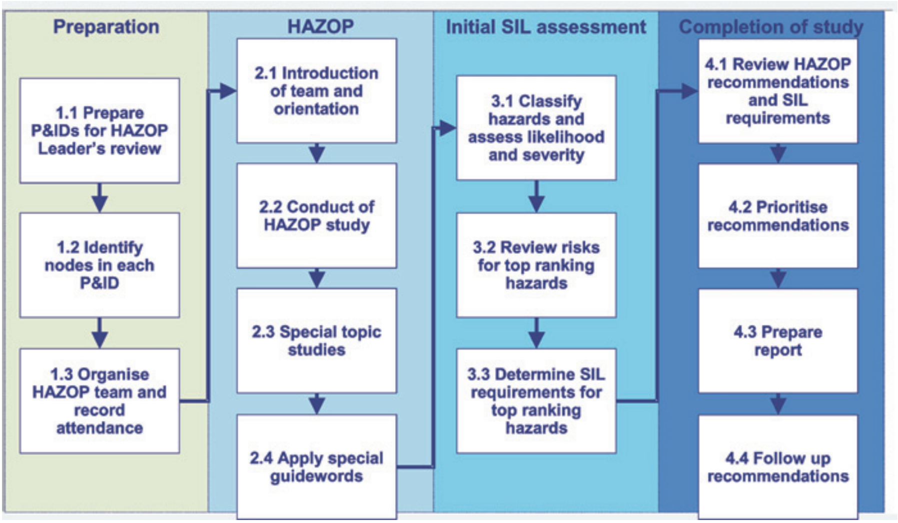

Preparation
1.1 Prepare P&IDs for HAZOP Leader's review
1.2 Identify nodes in each P&ID
1.3 Organise HAZOP team and record attendance
HAZOP
2.1 Introduction of team and orientation
2.2 Conduct of HAZOP study
2.3 Special topic studies
2.4 Apply special guidewords
Initial SIL assessment
3.1 Classify hazards and assess likelihood and severity
3.2 Review risks for top ranking hazards
3.3 Determine SIL requirements for top ranking hazards
Completion of study
4.1 Review HAZOP recommendations and SIL requirements
4.2 Prioritise recommendations
4.3 Prepare report
4.4 Follow up recommendations

Figure 4.

are intended to mitigate loss of containment scenarios. These should generally correspond to automated ESD systems. Thus we can identify IPSs requiring SIL analysis. We can also identify the related hazard that would result from failure of the IPS to function on demand.

When we produce final edited HAZOP worksheets typically at the end of each Unit study we are able to assign risk ranking (frequency and consequence) to the relevant IPS hazard scenarios, based on generic incident type (e.g. vessel rupture, major gas release).

These rankings can be calibrated to correspond to the IEC risk graph frequency and consequence parameters to provide a preliminary assignment of SIL ratings for the related IPS.

Following completion of all units, it is necessary to have some consolidation of SIL ratings. This is to ensure consistent interpretation for similar instrument types and hazard scenarios, within the context of overall process risk levels. When several groups are involved in the assessment, there are likely to be some inconsistencies in initial SIL ratings, particularly since the assessment reflects the judgement and opinion of team members.

LIST OF ACRONYMS/ABBREVIATIONS

ALARP	As Low As Reasonably Practicable (principle)
BPCS	Basic Process Control System
C	Consequence Parameter (in risk graph method)
ESD	Emergency Shut-Down (system)
F	Exposure Parameter (in risk graph method)
FALL	Flow Alarm Low Low
HAZOP	Hazard and Operability Study
IEC	International Electrotechnical Commission
IPS	Instrumented Protection System
LALL	Level Alarm Low Low
LI	Level Indicator
LCV	Level Control Valve
LC/LAL	Level Control/Level Alarm Low
LS	Level Switch
MOV	Motor Operated Valve
P	Avoidance Parameter (in risk graph method)
P&ID	Piping and Instrumentation Diagram
PCV	Pressure Control Valve
PI	Pressure Indicator
PS	Pressure Switch
PSV	Pressure Safety Valve
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SV	Safety Valve
TAH	Temperature Alarm High

TAHH	Temperature Alarm High High
TCV	Temperature Control Valve
TI	Temperature Indicator
TS	Temperature Switch
UA	Unacceptable (level of risk)
W	Frequency Parameter (in risk graph method)