

PRACTICAL GUIDELINES AND PROCEDURE FOR SIL RANKING UNDER IEC 61508/61511

Mike Wass
Consultant, AK EHS & Risk, Aker Kvaerner Engineering Services Ltd,
1410 Centre Park Square, Warrington, Cheshire, WA1 1QG, UK; +44 (0) 1925 892509;
mike.wass@akerkvaerner.com; www.akerkvaerner.com/AKEHSandRisk

INTRODUCTION

The international standards IEC 61508, Functional Safety of Electrical/Electronic/Programmable Electronic (E/E/PE) Safety-Related Systems (SRS) and IEC 61511, the daughter standard for the process industry sector, provide meticulous requirements and guidance whose implications can be daunting to the user. Many parts of the process industries are still getting to grips with what is required for compliance, in an environment where regulators increasingly seek compliance with the standards as a means of demonstrating that process hazards are adequately controlled. Practical ways forward to implement and comply with the standards are not immediately evident. Significant proportions of the standards are informative and leave the user to resolve the detail, such as calibration of 'Risk Graphs'.

This paper summarises the principles, content and experience of implementing a procedure for the first 5 steps of the safety life cycle in IEC 61508 that has been developed by AK EHS & Risk in association with its clients. The principles used in the procedure for calibration of risk graphs will be discussed. The output of the procedure is a methodically defined and substantiated allocation of safety requirements and Safety Integrity Levels (SIL) for E/E/PE SRS (i.e. trips, emergency shutdown systems). Options for further refining the procedure will be highlighted.

PRINCIPLES AND CONTENT OF THE PROCEDURE

The procedure that has been developed covers the first 5 steps of the safety life cycle of IEC 61508 from 'Concept Development' through to 'Safety Allocation'. The procedure also covers the 'Hazard and Risk Assessment' and 'Allocation of Safety Functions' phases of the simplified safety life cycle in IEC 61511. The procedure is segmented as follows:

- Common Requirements of IEC 61508 for Safety Lifecycle Phase 1 to 5
- Concept Development (Safety Lifecycle Phase 1)
- Overall Scope Definition (Safety Lifecycle Phase 2)
- Process Hazard and Risk Analysis and Protection Layer Identification (Safety Lifecycle Phase 3)
- Overall Safety Requirements Allocation (Safety Lifecycle Phases 4 and 5)

- Iteration (Layer of Protection Analysis (LOPA)/Fault Tree Analysis)
- Appendices

The 'Common Requirements' section gives requirements for project managers to establish and implement a 'Safety Lifecycle Safety Plan', to then monitor and verify implementation of the plan and finally to instigate a 'Functional Safety Assessment' once implementation of the rest of the procedure is complete. A form from the procedure for recording the safety plan, together with the subsequent monitoring and verification is shown as Figure 1.

The 'Functional Safety Assessment' is required to evaluate the assessments made for Safety Lifecycle Phases 1 to 5 against the following criteria:

- Have all hazards of the process or equipment under control been considered?
- Are the assessments based on sufficient and firm information?
- Are the assessments neither unduly pessimistic nor optimistic?

<table>
<tr><td colspan="5">Project Reference:</td></tr>
<tr><td colspan="2">Safety Lifecycle Phase 3</td><td colspan="3">Title: Hazard and Risk Analysis</td></tr>
<tr><td colspan="5">Task Description:

Confirm the following Safety Lifecycle Phase 3 objectives have been met.

• Identify hazard scenarios and the hazards associated with the equipment under control.
• Eliminate or reduce risks arising from the equipment under control where possible (i.e. inherent SHE).
• Identify hazard scenarios requiring risk reduction by Safety Related Systems.
• Identify the necessary risk reduction to be achieved by Safety Related Systems.</td></tr>
<tr><td colspan="5">Resources</td></tr>
<tr><td colspan="2" rowspan="2">Nominated Responsible Person(s):</td><td colspan="3">Competency</td></tr>
<tr><td>Applicable Training and Experience</td><td colspan="2">Qualifications</td></tr>
<tr><td colspan="2">Name:
Title:
Department:
Company:
Responsibility:</td><td></td><td colspan="2"></td></tr>
<tr><td colspan="5">Documentation</td></tr>
<tr><td>Description</td><td>Input Received</td><td>Verification Date</td><td>Output Complete</td><td>Verification Date</td></tr>
<tr><td>Document No:
Revision:
Title:</td><td></td><td></td><td></td><td></td></tr>
</table>

Figure 1. Example form recording the safety lifecycle safety plan, monitoring and verification

- Are the assessments technically correct?
- Have realistic SIL values been allocated to E/E/PE SRS?

The 'Concept Development' section sets down the data gathering requirements to ensure that equipment under control and its environment are sufficiently understood before detailed assessment commences. The procedure sets down the information requirements under the following headings:

- Process definition
- Chemicals and services
- Physical and hazardous property data
- Plant location and local environment
- Legislative, consultation and risk requirements

The 'Overall Scope Definition' section requires the definition of the boundary of the process and equipment under control being assessed, together with its control system. The output is a defined and documented basic design, operating philosophy, control system and alarm response, together with a preliminary Piping and Instrumentation Diagram (P&ID) showing controls and alarms.

The 'Process Hazard and Risk Analysis and Protection Layer Identification' section is based on the output from 'Concept Development' and 'Overall Scope Definition'. The stated objectives are to:

- To identify hazards and hazard scenarios associated with the equipment under control.
- To eliminate or reduce risks arising from the equipment under control where possible prior to further assessment. Note that IEC 61508/61511 require that inherent safety of the equipment under control is optimised before the requirement for Safety Related Systems is considered.
- To identify hazard scenarios requiring risk reduction by Safety Related Systems.
- To identify the necessary level of risk reduction to be achieved by Safety Related Systems.

The focus of this section of the procedure is screening all hazard scenarios associated with the process and equipment under control using a risk graph approach. The rapid risk graph screening approach enables compliance with the requirement of IEC 61508 that 'all hazard scenarios arising from the equipment under control, under all modes of operation are considered' within a reasonable timescale.

Figure 2 shows the ranking categories for human harm that are used by the procedure. The procedure also addresses environmental and financial loss but the corresponding information is omitted for brevity in this paper. The broad range of human harm categories enables all hazards to be considered and also enables society's aversion to incidents affecting large numbers of people at one time to be taken into account i.e. Societal Risk. Seven categories of frequency of harm are used in the risk graph to cover the full range of hazard frequencies relevant to the process industries. The frequency bands are skewed, as in the informative example in IEC 61511, so that typical order of

Harm to people

Code	People Harm Description
Cp1	Single person on-site suffering minor Injury
Cp2	Ten people on-site suffering minor Injury
Cp3	Hundred people on-site suffering minor Injury
Cp4	Single person on-site suffering Major Injury
Cp5	Ten people on-site suffering Major Injury
Cp6	Hundred people on-site suffering Major Injury
Cp7	Single person on site dying
Cp8	Ten on-site personnel dying
Cp9	Hundred on-site personnel dying
Cp10	Single member of public dying
Cp11	Ten members of public dying
Cp12	Hundred members of public dying

(Annual) Frequency of Occurrence of the Undesired Event

Code	Frequency Description
W1	Less than once in 33,333 years to once in 333,333 years
W2	Less than once in 3,333 years to once in 33,333 years
W3	Less than once in 333 years to once in 3,333 years
W4	Less than once in 33 years to once in 333 years
W5	Less than once in 3.3 years to once in 33 years
W6	Less than once in 4 months to once in 3.3 years
W7	Less than once in 2 weeks to once in 4 months

Probability that Personnel Are Present In The Zone Of Hazard

Code	Probability Description
F1	Average presence of less than 2.5 hours in every 24 hours
F2	Average presence of more than 2.5 hours in every 24 hours

Possibility of Personnel Protecting Themselves When The Hazard Occurs

Code	Probability Description
P1	Possible under certain conditions (10% probability of being harmed)
P2	Not Possible

Figure 2. Ranking categories for human harm

magnitude estimates, i.e. 'once every 10 years', fall clearly into a category. Figure 3 shows extracts from a typical risk graph used in the procedure. The risk graph gives the necessary risk reduction, in terms of probability of failure on demand, for the selected ranking categories. The calibration of this risk graph is discussed later in the paper. Figure 4 shows a form from the procedure for recording the identification of necessary risk reduction.

The 'Overall Safety Requirements Allocation' section defines how to take the necessary risk reduction and allocate it to other safety technologies and external risk reduction facilities before allocating the residual risk reduction to E/E/PE SRS. The procedure only permits risk reduction requirements to be expressed in terms of the Safety Integrity Level for safety requirements that have been allocated to E/E/PE SRS. Figure 5 shows a form from the procedure for recording safety requirements allocation.

For Harm to people										
Harm categories		Probability of being present categories	Probability of avoiding harm categories	Frequency Categories						
				W7	W6	W5	W4	W3	W2	W1
				Less than once in 2 weeks to once in 4 months	Less than once in 4 months to once in 3.3 years	Less than once in 3.3 years to once in 33 years	Less than once in 33 years to once in 333 years	Less than once in 333 years to once in 3333 years	Less than once in 3,333 years to once in 33,333 years	Less than once in 33,333 years to once in 333,333 yrs
Cp5	Ten people on-site suffering major injury	F1 (0.1)	P1	0.0001	0.001	0.01	a	-	-	-
			P2	0.00001	0.0001	0.001	0.01	a	-	-
		F2	P1	0.00001	0.0001	0.001	0.01	a	-	-
			P2	Unacceptable	0.00001	0.0001	0.001	0.01	a	-
Cp6	One hundred people on-site suffering major injury	F1 (0.1)	P1	0.0001	0.001	0.01	a	-	-	-
			P2	0.00001	0.0001	0.001	0.01	a	-	-
		F2	P1	0.00001	0.0001	0.001	0.01	a	-	-
			P2	Unacceptable	0.00001	0.0001	0.001	0.01	a	-
Cp7	Single person on site dying	F1 (0.1)	P1	0.00001	0.0001	0.001	0.01	a	-	-
			P2	Unacceptable	0.00001	0.0001	0.001	0.01	a	-
		F2	P1	Unacceptable	0.00001	0.0001	0.001	0.01	a	-
			P2	Unacceptable	Unacceptable	0.00001	0.0001	0.001	0.01	a
Cp8	Ten on-site personnel dying	F1 (0.1)	P1	0.00001	0.0001	0.001	0.01	a	-	-
			P2	Unacceptable	0.00001	0.0001	0.001	0.01	a	-
		F2	P1	Unacceptable	0.00001	0.0001	0.001	0.01	a	-
			P2	Unacceptable	Unacceptable	0.00001	0.0001	0.001	0.01	a
Cp9	One hundred on-site personnel dying	F1 (0.1)	P1	Unacceptable	0.00001	0.0001	0.001	0.01	a	-
			P2	Unacceptable	Unacceptable	0.00001	0.0001	0.001	0.01	a
		F2	P1	Unacceptable	Unacceptable	0.00001	0.0001	0.001	0.01	a
			P2	Unacceptable	Unacceptable	Unacceptable	0.00001	0.0001	0.001	0.01
Cp10	Single member of public dying	N/a	P1	Unacceptable	Unacceptable	0.00001	0.0001	0.001	0.01	a
			P2	Unacceptable	Unacceptable	Unacceptable	0.00001	0.0001	0.001	0.01
Cp11	Ten members of public dying	N/a	P1	Unacceptable	Unacceptable	0.00001	0.0001	0.001	0.01	a
			P2	Unacceptable	Unacceptable	Unacceptable	0.00001	0.0001	0.001	0.01

Figure 3. Extracts from a typical risk graph

Hazard Scenario Number	Equipment Affected	Hazard Description	Event Sequence	Potential Human Harm	Potential Environmental Harm

Summary of Relevant Non-Safety Related Systems			
Plant Design	Operating Philosophy	Control System	Abnormal Situation Management

Selection of Frequency/Consequence Categories				
Human Harm Cp	Environmental Harm Ce	Frequency W	People Present ? F	Can people avoid harm? P
Justification	Justification	Justification	Justification	Justification

Personnel Safety Necessary Risk Reduction Factor	
Environment Necessary Risk Reduction Factor	

Figure 4. Form for recording selection of necessary risk reduction

Scenario No.	Equipment Affected	Hazard Description	Event Sequence	Potential Human Harm	Potential Enviro Harm

Personnel Safety Necessary Risk Reduction Factor					
Environment Necessary Risk Reduction Factor					
Allocation of Safety Requirements					
Other Technology Safety Related Systems	Description of Type, Location and Function		Risk Reduction Achieved		Justification
			For People:		
			For Environment:		
External Risk Reduction Facilities	Description of Type, Location and Function		Risk Reduction Achieved		Justification
			For People:		
			For Environment:		
Potential for Common Cause Failure between Other Technology and External Safety Related Systems (High, Medium or Low)					
Potential for Common Cause Failure between E/E/PE and other Safety Related Systems (High, Medium or Low)					

E/E/PE Systems	Description of the Function	Input Parameter/s, Type and Origin	Output Devices and Location	SIL Ranking	
				For People:	Overall
				For Environment:	

Figure 5. Form for recording safety requirements allocation

The 'Iteration' section requires that the operational and financial acceptability of the allocated safety integrity levels be reviewed. This is a second chance to optimize the inherent safety of the equipment under control by revising the operation and design of the process to reduce the inherent risks. This section also requires E/E/PE SRS ranked SIL 2 or more to be reassessed by layer of protection or fault tree analysis to confirm the validity of the allocation. Finally this section requires that the costs of installing a safety related system to further reduce risk by an order of magnitude, to be established to see if this is reasonable. Decision criteria are given.

The 'Appendices' section contains the forms, risk graphs and other job aids such as generic likelihood and consequence modeling data to enable implementation of the procedure with minimal reference to external sources.

PRINCIPLES ADOPTED FOR CALIBRATION OF RISK GRAPHS

The risk graph shown in Figure 3 has been calibrated based on tolerability data established for the UK by the Health and Safety Executive[1,2]. The unacceptable boundary of societal risk is given as 50 people dying every 5,000 years from a single industrial activity and the broadly acceptable boundary is two orders of magnitude less frequent than this and that the slope of the Log-Log plot is -1.

The risk graph is calibrated on the principle that a site's residual societal risk should lie in the middle of the tolerable region. This equates to 50 fatalities every 50,000 years and extrapolates back to a single fatality, from amongst all the personnel at a single industrial site, being tolerable once every 1000 years. A single fatality every 100 years is taken as the single point of reference of acceptable residual risk for calibration of the risk graph. This residual risk must take account of all hazard scenarios. In order to determine the acceptable residual risk for a single hazard scenario an estimate must be made of the number of process hazard scenarios at a site that have the potential to kill a single person. The risk graph in Figure 3 is calibrated on the basis that the site has 100 single fatality process hazard scenarios. This is believed to be typical of many industrial sites. Hence the acceptable residual risk from a single hazard scenario is once every 100,000 years. The necessary risk reduction for each box of the risk graph is established by dividing the target residual risk by the combination of event frequency (mid range value), probability of personnel being present (1.0 or 0.1) and probability of personnel avoiding harm (1.0 or 0.1).

When calibrating for other levels of harm, further assumptions have to be made. For example, when considering hazards scenarios with the potential to cause 10 fatalities it is assumed that the acceptable frequency is ten times less than for single fatalities. However, it is also assumed that the total number of such hazard scenarios is only an appropriate percentage of that for single fatalities.

PRINCIPLES OF DEMONSTRATING THAT PROCESS HAZARDS ARE ADEQUATELY CONTROLLED

Using a calibrated risk graph alone will not be sufficient to demonstrate to regulatory bodies that process hazards are adequately controlled. The question from regulators

'Why shouldn't you install a more reliable trip?' is one that, increasingly, has to be answered. The procedure provides a framework for answering this. For example if a SIL 1 E/E/PE SRS is to be installed to protect against a single fatality on a high hazard process, then the residual risk using the risk graph in Figure 3, assuming a twenty year life span, is 0.0002 lives. In the UK, the HSE regard the minimum value to prevent a single fatality is £1,000,000 and that this should be increased to £10,000,000 for high hazard processes[1]. Therefore, this would equate to a capital expenditure of around £2,000 being reasonable to eliminate the majority of the residual risk by, say, increasing the E/E/PE SRS to SIL 2. This comparatively low level of justifiable additional expenditure is a consequence of the target residual risk for a single hazard scenario being set at a low value in the risk graph in Figure 3. However, if the same scenario was assessed for a site where the risk graph had been calibrated on the basis of just 10 single fatality scenarios, then the target residual risk for each scenario would be ten times higher. The justifiable additional capital expenditure to eliminate the residual risk would be correspondingly higher at £20,000.

EXPERIENCE OF IMPLEMENTING THE PROCEDURE

The form shown in Figure 4 drives the assessment team to understand and identify the non-safety related layers that control the hazard and prevent demands being made on safety related systems. However, design teams often identify a wealth of operational and design features that appear to prevent the hazard being considered from being realized. On close inspection it is not unusual to find that some of these features are not independent and that the design team is being over optimistic in estimating the frequency. It requires strong leadership from the chairman to sift out the genuine arguments and agree realistic choices for the frequency of harm category to be used with risk graphs.

The demand rates for some safety related systems are genuinely low because of the defenses offered by the non-safety related layers. When screening process hazards using a risk graph it frequently proves necessary to have an experienced risk assessor as part of the team so that realistic layers of protection calculations can be done to substantiate the assigning of low frequency categories. In the absence of this skill in the team, it is difficult to progress screening significant numbers of hazard scenarios because personnel will not be able to make realistic estimates of demand rates beyond the 3 to 33 year category.

The assessment teams in organizations in the early phases of adopting IEC 61508/61511 tend to think in terms of needing to SIL rank the 'trip' that has already been included on the preliminary designs, rather than assessing the necessary risk reduction of a hazard scenario. As a consequence meetings may be inefficient because they can get diverted into redesigning minute details of the trip rather than establishing the target reliabilities of safety related layers. This links to the other great challenge for the chairman of ensuring that the assessment team puts aside its knowledge of potential trip systems that they have already in mind and assess the consequences and likelihoods of incidents in the absence of safety related layers. This can prove difficult when safety related systems that people normally expect to be present as part of a basic design, such as bunds, are relevant.

CONCLUSIONS

The procedure provides a comprehensive approach to implementing all requirements of the first 5 stages of the IEC 61508 safety lifecycle and demonstrating that risks will be adequately controlled and meet regulatory expectations. It goes beyond SIL ranking, which is where many organisations focus their initial adoption of the standard. Despite the written procedure being straightforward and concise, significant risk assessment expertise and supporting information is needed for successful implementation. The procedure should be integrated into the early phases of existing process design practice to ensure that appropriate E/E/PE SRS are incorporated into process designs in a systematic and efficient manner.

REFERENCES

1. Health and Safety Executive, 2003, 'HIDs Approach to 'As Low As Reasonably Practicable' (ALARP)'; HID Web Site SPC/Permissioning/09
2. Health and Safety Executive, 2001 'Reducing Risks, Protecting People, HSE's decision-making process; HMSO