CASE STUDY: IMPLEMENTATION OF THE IEC61508 STANDARD ON A CHEMICAL PLANT UPGRADE PROJECT

Christopher J. Beale (MIChemE) and Shaun Dunford, Ciba Specialty Chemicals, Additives Division, PO Box 38, Bradford, West Yorkshire. BD12 OJZ. UK

Many chemical plants now rely on automated control and protection systems. Great care must be taken when designing, operating and maintaining these systems to ensure that potential common mode failures are minimised and system reliability is optimised. The new international standard IEC61508 provides a framework for systematically managing the risks associated with these automated systems. In many ways, the standard is a framework which binds existing safety and risk engineering techniques together rather than being a completely new technique. Emphasis is placed on using systematic approaches, compiling comprehensive documentation, making use of multi-disciplinary teams and taking a lifecycle approach for the project. The IEC61508 standard has been used successfully on several recent projects at the Bradford site which have major accident hazard potential. This paper explains how the standard has been applied to real projects and highlights the areas of the standard which were difficult to implement.

IEC61508, risk assessment, plant automation.

1. INTRODUCTION

1.1 OVERVIEW OF STANDARD

IEC61508 is an international standard for managing the life cycle safety requirements of E / E / PES (Electrical / Electronic / Programmable Electronic System) for Safety Related Systems (IEC, 1998). The standard has been developed for use across a wide range of industries. Once the standard has been finalised, there are plans to produce related standards for specific industry segments. Some parts of the standard have been issued while other parts are still in draft form.

Major hazard chemical plants often rely on a range of Safety Related Systems (SRS) to ensure that their risk levels are acceptable. Many of these systems use E / E / PES technology. IEC61508 therefore provides an approach to assist with the systematic management of these systems in the chemical industry.

The standard is based on a lifecycle safety model. This model is made up of three broad areas :

(i) Scope definition, hazard identification and development of the plant basis of safety using SRS's where required.

(ii) Design, validation and specification of SRS requirements.

(iii) System installation, commissioning, maintenance, operation and final decommissioning.

Underpinning the standard are four key concepts :

(i) **Equipment under control (EUC)** : the plant and it's control systems in which hazards can occur if the control systems allow the plant to operate outside key parameters. An example would be a storage tank holding hazardous materials which was controlled by a DCS (Distributed Control System).

(ii) **Safety Related Systems (SRS)** : which protect the plant if it reaches a state which is outside these key parameters. An example would be a hard-wired overfill protection interlock for the storage tank.

(iii) **Safety Functions (SF)** : which define the precise operating requirements for the Safety Related System. An example would be 'close feed valve V126 if level switch LS237 detects that the tank contents have reached the 95% full level'.

(iv) **Safety Integrity Level (SIL)** : which defines the required reliability level for the Safety related System. An example would be specifying a SIL1 reliability level for the overfill protection system, which means that the probability of failure on demand for the system must be shown to lie within the range 0.01 to 0.1.

The Safety Related Systems may use different technologies : E / E / PES, 'other technology' such as mechanical pressure relief devices and 'external risk reduction facilities' such as bund containment systems which limit the consequences of any accidents which occur.

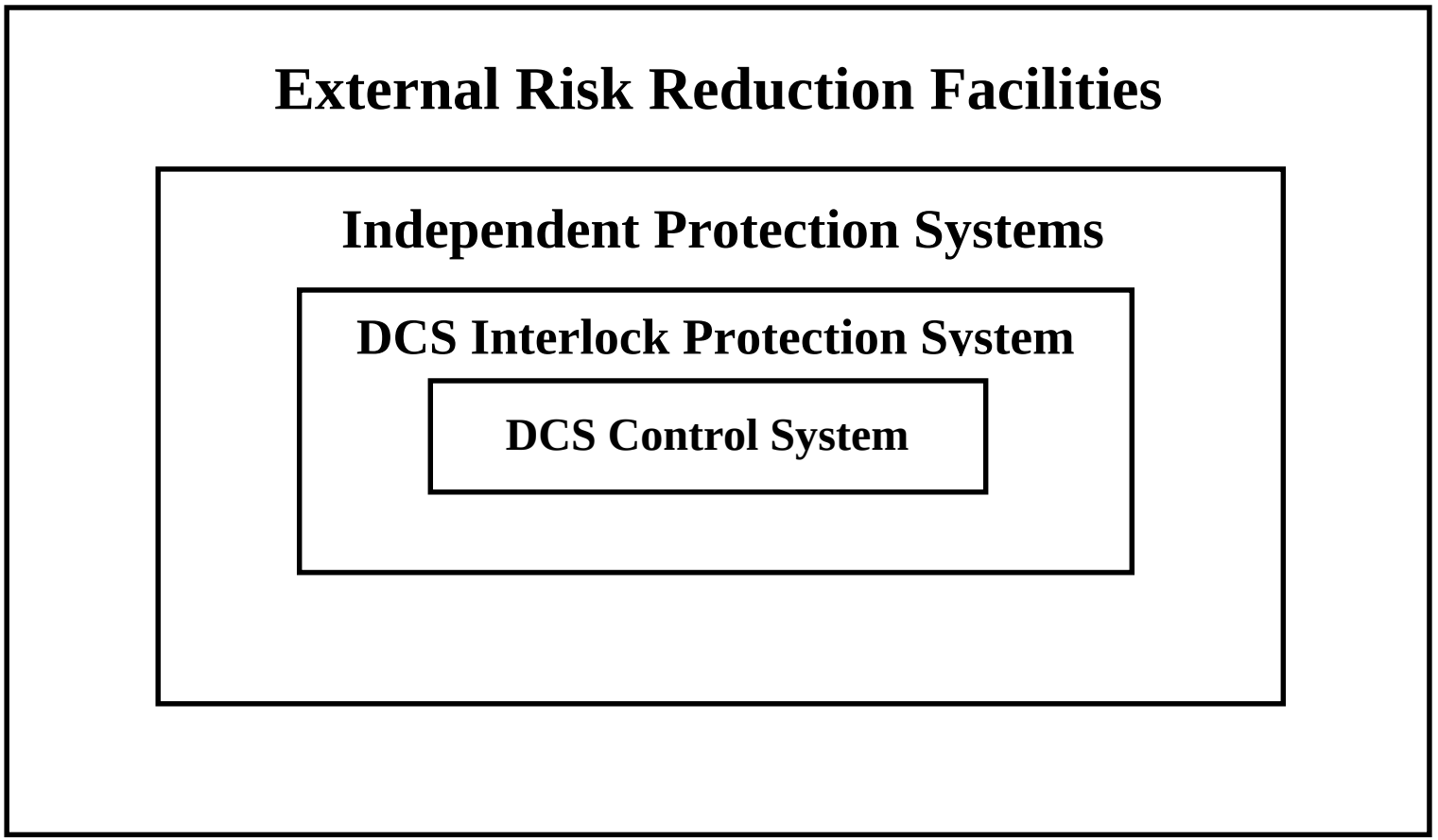
The plant will therefore have a basis of safety which relies on an appropriate mix of these individual features and can be viewed as an 'onion model' with diverse protection and emergency systems protecting the plant like rings around an onion (see **Figure 1**).

1.2 DECISION TO USE IEC61508

There are a large number of chemical processing and storage activities on the Ciba Specialty Chemicals Bradford site. Many of these operations involve potentially hazardous materials. New Process Safety Management (PSM) systems have recently been introduced to manage these operations to ensure that each operation has a documented and acceptable basis of safety. The basis of safety will often rely on key protection systems. These systems can be E / E / PES, mechanical or procedural and their performance is critical to the safety of individual plants and the site as a whole.

A systematic approach was therefore needed to manage these critical systems. Existing systems were in place but were often difficult to audit and did not effectively cover life cycle safety requirements. IEC61508 offered a structured framework for managing the life cycle safety requirements of these systems. The standard was therefore adopted on a trial project which later proved to be successful. IEC61508 is now being used on all relevant new projects on the site.

Figure 1 The ‘Onion Model’ Of Plant Safety.



1.3 APPLICATION OF IEC61508 ON REAL PROJECTS

IEC61508 has now been used by Ciba Specialty Chemicals on a range of chemical plant projects covering chemical production plants, tank farm storage facilities and powder handling facilities. E / E / PES protection systems have been required for a number of applications including :

(i) overfill protection systems for tanks and vessels which handle hazardous materials,

(ii) high temperature protection systems for reactions which are subject to potential violent thermal runaways or fires,

(iii) overpressure protection systems for vessels.

(iv) plant shutdown systems to protect against incorrect chemical compositions.

This paper is based on experience which has been gained on these projects. E / E / PES requirements have not exceeded SIL1 on projects completed to date.

2. PROJECT TEAM SELECTION AND STAFF TRAINING

2.1 THE TEAM BASED APPROACH

Effective teamwork and co-operation is critical to the successful completion of projects within the framework of IEC61508. Rather than allowing projects to become a series of unconnected activities with handover from department to department, emphasis is placed on close co-operation between disciplines throughout the project lifecycle. This helps to ensure that optimal decisions are made which reflect the needs of the project rather than those of individual disciplines. The following benefits have been gained on projects by using this team based approach :

(i) early identification of hazards allowing some to be eliminated.

(ii) rapid identification of impractical design constraints.

(iii) design changes to improve plant operability.

(iv) design changes to simplify maintenance requirements.

(v) speedier project progress.

Different projects will require different project team compositions. Care should be taken when creating the team to ensure that all relevant disciplines are included and that individual staff are competent to perform their role on the project. As IEC61508 is a new standard which introduces new technical jargon, it is essential that team members have either awareness training or specialist training on IEC61508 before they are involved in the project. Draft guidance on staff competency requirements has been published by the Institution of Electrical Engineers in conjunction with the British Computer Society and the United Kingdom Health and Safety Executive (IEE, 1999).

2.2 STAFF TRAINING REQUIREMENTS

Many of the techniques which are used within the standard are not new. The standard does, however, tie together many existing techniques and methodologies in a coherent and auditable framework. If high quality training is provided to key personnel, the learning curve for using the standard can be reasonably quick. Training needs will vary depending on the role of the individual within the project. The following hierarchy of training has been used for completed projects :

(i) Detailed training for safety engineers focusing on the activities at the front end of the project lifecycle such as hazard identification, identification of Safety Related Systems (SRS) and safety allocation.

(ii) Awareness training for all team members covering research chemists, design engineers, maintenance staff and production staff.

(iii) Detailed training for safety and control engineers in quantitative reliability assessment techniques.

(iv) Detailed training for control engineers covering the technical requirements of the middle section of the project lifecycle : designing, specifying, record - keeping, procuring, installing, formal handover and testing of Safety Related Systems.

(v) Training for maintenance staff on how to carry out lifecycle whole loop testing for individual E / E / PES loops.

(vi) Awareness training for senior managers so that they could understand the context of IEC61508 within the wider business.

Experience with IEC61508 will often not be available when the standard is first used in a company. It may therefore be necessary to use external specialist resources to prepare for and review the first few projects. Internal experience can then be developed and spread throughout the organisation.

When introducing a new standard, there will always be a learning curve to complete. Projects will only become truly efficient after experience has been gained on a number of projects within the organisation. Perseverance is required for these first few projects and effort will be required to overcome problems and create links with existing corporate systems or modify them where necessary..

2.3 TEAM SELECTION

It is important that key disciplines are represented on the project team. Some personnel will be core team members whereas others will only be required for some phases of the project. For chemical plant projects, most teams will require some combination of :

(i) safety engineers to identify hazards, assess risks, carry out reliability assessments and specify Safety Related Systems (SRS).

(ii) production staff and business managers to ensure that operability and safety requirements are satisfied.

(iii) engineering designers for chemical engineering, mechanical engineering, electrical engineering and project engineering.

(iv) control and instrumentation engineers to design, specify, install and commission E / E / PES systems.

(v) maintenance staff to ensure that systems are designed for maintenance.

(vi) other specialists such as environmental advisers and research chemists to assist in understanding chemical hazards.

(vii) suppliers and external specialists.

3. SCOPE DEFINITION AND THE SAFETY PLAN

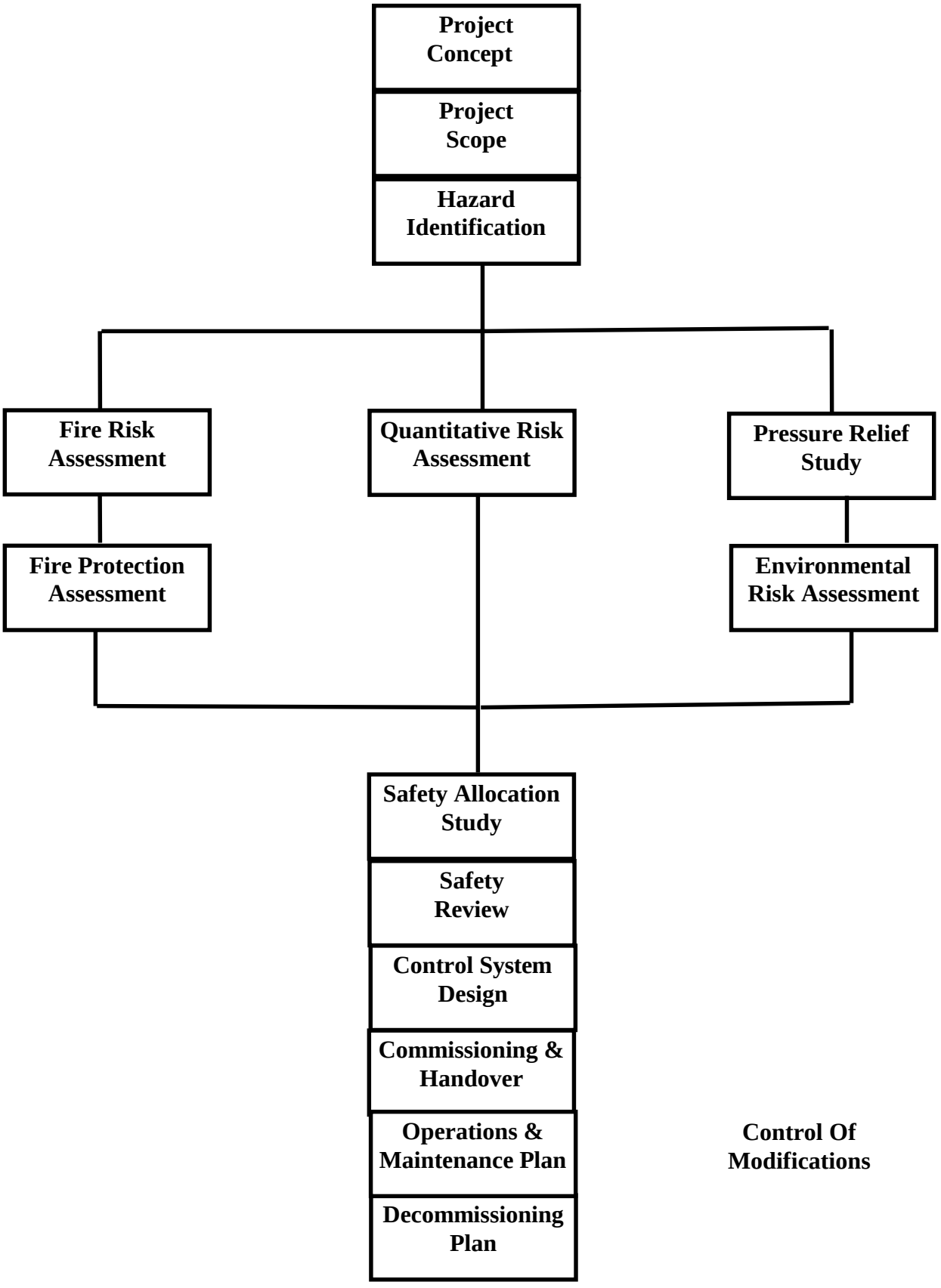
Project safety studies cannot be carried out effectively without a clear and unambiguous project scope. This should be in a written format supported by any appropriate drawings. Particular care should be taken to define the project boundaries and interactions with other plants. Interfaces which can cause ambiguity include : feed pipes from other plants, transfer pipes to other plants, road tanker loading and offloading, raw materials and product storage, container filling, services, effluent and links to other plant control systems. Clear scopes will lead to successful projects.

Once the scope has been agreed and defined, the safety plan needs to be produced. This defines key roles and responsibilities and the links between key stages in the project. A project schedule linking safety studies and protection system design activities to other engineering and procurement activities will provide a basis for monitoring and controlling project progress. Regular audits and reviews can then be made against the safety plan. Changes occur during most projects and some of these changes will affect the safety plan. Typical examples include personnel changes, scope changes and delays in completing some activities. In such cases, it will be necessary to treat the safety plan as a living document which is subject to regular updates.

The safety plan should address the whole project lifecycle from engineering design, through installation and commissioning to operation and then de-commissioning. It is particularly important to define points at which responsibilities are transferred between individuals or departments. Even though responsibilities may have been transferred, it is still important that a team based approach is followed through all stages of the project.

Figure 2 shows a typical framework for linking different safety and environmental studies for the initial stages of a project. This would form part of the safety plan. This framework will be different for different projects, reflecting the individual project structures and the nature of the hazards.

Figure 2 Typical Study Structure Within The Safety Plan..



4. HAZARD IDENTIFICATION

Hazards must be identified before any design or specification work can commence for Safety Related Systems. A wide range of techniques exist including brainstorming, what-if? Analysis, checklists and hazops. The most appropriate technique should be used for each project, using standard corporate techniques where possible. It is, however, important to use a technique which is designed to identify major hazards ie. those hazards which could cause serious harm to people or the environment.

The hazard identification exercise should produce a list of identified hazards for the plant. Rather than immediately starting to design protection systems for each hazard, the design team should thoroughly examine each hazard to identify methods of eliminating the hazard, reducing it's consequences and reducing it's frequency of occurrence using the principles of inherent SHE.

Any hazards which have minor consequences can be removed from the list to produce a residual list of major hazards which cannot be eliminated by design.

5. IDENTIFICATION OF SAFETY RELATED SYSTEMS (SRS)

Most hazard identification methodologies produce outputs in a matrix format, listing hazards, causes, assessed consequences, risk controls and actions. The risk controls should be highlighted and categorised for each hazard as they will be required for the subsequent stages of analysis.

The risk controls should be assessed using four categories :

(i) Electrical / Electronic / Programmable Electronic Systems (**E / E / PES**) comprising instruments, controllers and valves.

(ii) Other Technology (**OT**) such as mechanical safety systems.

(iii) External Risk Reduction Facilities (**ERRF**) which limit the consequences of an accident should it occur.

(iv) Plant Procedures (**PP**).

These risk controls are the Safety Related Systems (SRS) for the plant. The safety function needs to be defined for each SRS. This is a clear definition of the performance requirement for the SRS. For example, for a tank overfill protection system, the safety function may be : *Feed isolation valve V135 should fully close if level switch LSW128 detects a level in excess of 90% in tank ST109.* At the start of the project, the safety function definition may be rather loose, but it must be refined as the project progresses so that a clear specification can be made for the SRS.

6. SAFETY ALLOCATION USING RISK MATRICES AND FAULT TREE ANALYSIS

6.1 SELECTING THE APPROPRIATE TECHNIQUE

The aim of the safety allocation exercise is to ensure that the risk associated with each hazard is acceptable. Risk is defined in a traditional way as the combination of the frequency and consequences of the hazard. The acceptability of the risk is defined by risk criteria. Individual organisations define their own risk criteria to meet their objectives. These criteria can be qualitative, using risk matrices, or quantitative.

IEC61508 views an accident frequency (F) as being composed of a demand rate (D) and the subsequent failures of Safety Related Systems (P). The demand rate is the frequency that the plant passes beyond it's safe control parameters and requires one or more protection systems to operate. In other words, it is the frequency at which accidents would occur if the plant had no protection systems.

$$Accident\ Frequency = Demand\ Rate \times P_1 \times P_2 \times P_3 \times ..... \times P_N$$

Where P_i is the failure rate on demand of each of the N SRS's.

IEC61508 part 5 proposes several approaches which can be used for safety allocation. There are pros and cons associated with each approach in terms of the need for data, time, subjectivity and auditability. Care must be exercised when choosing the technique which will be used in a study.

6.2 THE RISK MATRIX APPROACH

Hazards are assigned to defined consequence categories and defined frequency categories using a matrix format. Different regions of the matrix are then considered to have unacceptable, ALARP (As Low As Reasonably Practicable) or broadly acceptable risks. The way that these three regions are allocated to the matrix defines the corporate risk criteria.

IEC61508 part 5 Annex E proposes a 3 x 3 risk matrix using frequency categories of (low, medium, high) and consequence categories of (minor, serious, extensive). High risk regions of the matrix either require multiple independent protection systems or high SIL ratings for E / E / PES SRS's. This matrix will not necessarily correspond to the corporate risk criteria which are used by individual operating companies. It is also restrictive in that it only allows 9 combinations of frequency and consequence. For plants which have a wide range of diverse hazards, this categorisation is often overly restrictive and a revised matrix needs to be produced. 5 x 5 matrices linked to corporate criteria provide a much more balanced method of allocating SIL ratings and assuring compliance with risk criteria. An example of a 5 x 5 risk matrix is provided in **Appendix I**.

6.3 THE FAULT TREE APPROACH

Fault tree analysis can be used for assessing complex hazards. The technique is time consuming and therefore is not suitable for use with all hazards. The top of most fault trees is composed of a number of AND logic gates which combine a demand rate (D) with the probability (P_i) that a number of Safety Related Systems fail to operate correctly on demand. P_i for each SRS can then be directly linked to SIL levels for individual E / E / PES systems.

The fault tree analysis can then be used as a numerical tool for comparing predicted accident frequencies ($D \times P_1 \times ..... \times P_N$) with corporate risk tolerability targets.

6.4 THE RISK GRAPH APPROACH

This approach uses an event tree structure as a basis for allocating SIL levels to individual SRS's and has not been used on any of the projects which have been completed to date.

7. SAFETY INTEGRITY LEVEL (SIL) VALIDATION

7.1 DEFINITION OF SIL REQUIREMENTS

Once SIL requirements have been defined for each Safety Related System, a validation must be performed to ensure that the SIL requirement is actually met on real plant protection systems. Depending on the specific hazard, the following outcomes may be required from the Safety Allocation exercise :

(i) the hazard can be removed using inherent SHE principles (**IS**).

(ii) the hazard does not require SIL rated SRS's (**NR**).

(iii) SIL rated E / E / PES systems are required (**E / E / PES**).

(iv) SIL rated Other Technology systems are required (**OT**).

(v) SIL rated External Risk Reduction systems are required (**ERRF**).

(vi) SIL rated Plant Procedures are required (**PP**).

Some hazards will only require protection using one SIL rated protection system; others may have a more diverse requirement using different combinations of E / E / PES, OT, ERRF and PP. For example, a storage tank containing highly flammable liquid may require a SIL1 rated overfill protection system but a chemical reactor may require a SIL1 rated high temperature protection system and a SIL1 rated pressure relief system.

7.2 SIL RATINGS FOR NON E / E / PES SYSTEMS

This immediately causes a problem for the design team. The scope of IEC61508 covers E / E / PES systems but does not provide guidance on how to validate OT, ERRF and PP protection systems. The basis of safety for real plants often relies on a range of technologies so it is essential that a framework is developed for specifying and validating SIL requirements for the whole range of categories of protection systems.

One solution to this problem is to revisit the fundamental philosophy behind SIL levels. The plant has a number of hazards : potential mechanisms for causing harm to people or the environment. Plant risk levels are defined as a combination of the severity of each hazard and the frequency of occurrence of the hazard. If no Safety Related Systems (SRS) were installed, the frequency of occurrence of the hazard is known as the demand rate : the frequency of requiring a Safety Related System to operate. Each SRS reduces the risk due to it's reliability : the probability that the SRS fails to function correctly when required. The reliability is defined by the SIL level. For example, a SIL1 reliability implies that the SRS failure

probability on demand will be between 0.01 and 0.1. The frequency associated with each hazard is therefore the product of the demand rate and the failure rate on demand of each SRS.

$$Accident\ Frequency = Demand\ Rate \times P_1 \times P_2 \times P_3 \times ..... \times P_N$$

Where P_i is the failure rate on demand of each of the N SRS's.

As an example, a reactor may be susceptible to a reaction runaway hazard. The demand rate has been assessed as 0.1 event per year based on a dominant cause of control system error. If no SRS's were installed, the accident frequency would be assessed as 1 runaway every 10 years. Two SRS's have been installed on the reactor : a SIL2 rated emergency cooling system and a SIL1 rated mechanical pressure relief system. Assuming (conservatively) that each SRS just meets the minimum SIL requirement :

$$Accident\ Frequency = 0.1 \times 0.01 \times 0.1 = 1 \times 10^{-4}\ per\ year.$$

The SIL rating is therefore a numerical target for the probability of failure on demand of the individual SRS. The higher the SIL rating, the more reliable the SRS must be.

The concept of SIL ratings could therefore be extended to cover OT, ERRF and PP as well as E / E / PES, but it must be recognised that this will go beyond the scope of the IEC61508 standard.

The reliability of an individual SRS is derived from the combination of the fundamental reliability of the equipment which constitutes the SRS and the test interval for the SRS. Rulesets can therefore be developed for each category of SRS to define SIL1, SIL2, SIL3 and SIL4 standards. As some categories will have a maximum credible reliability, An additional rule is recommended :

if the risk target can only be achieved using OT, ERRF or PP SRS's which have an assessed reliability requirement greater than SIL1, the plant design is not robust and a fundamental design change may be required.

The following three examples show how SIL1 reliability can be interpreted to develop a performance standard for OT, ERRF and PP SRS categories.

7.2.1 SIL RATINGS FOR OTHER TECHNOLOGY

Pressure relief systems are a mechanical form of SRS. A performance standard could be developed for such systems to ensure a SIL1 equivalent reliability based on :

(i) Documented specifications for the relief system.

(ii) Design of relief system by competent persons.

(iii) Independent design check.

(iv) Procurement of defined types of equipment from designated suppliers.

(v) Installation and testing by competent persons.

(vi) Regular independent testing and certification by qualified external bodies.

(vii) Verification that real failure rates for similar installed systems suggest that SIL1 reliability is being achieved in practice. Reference should be made to maintenance records and incident reports.

7.2.2 SIL RATINGS FOR EXTERNAL RISK REDUCTION FACILITIES

Bund containment systems fall within the ERRF category of SRS. A performance standard could be developed for such systems to ensure a SIL1 equivalent reliability based on :

(i) Clear specification of bund containment requirements.

(ii) Bund design by a competent civil engineer using defined standards and materials.

(iii) Independent design check.

(iv) Theoretical assessment of the likelihood of bund overtopping based on factors such as tank size, height of bund walls, proximity of bund walls to tanks, vulnerability of corner sections to high loads etc.

(v) Regular bund inspections and leak tests by a competent person.

7.2.3 SIL RATINGS FOR PLANT PROCEDURES

Manual inhibitor addition procedures are a procedural form of SRS. A performance standard could be developed for such systems to ensure a SIL1 equivalent reliability based on :

(i) Produce clear written procedures using a standard format.

(ii) Train operators and assure operator competence.

(iii) Regular refresher training for operators and simulated tests of procedure.

(iv) Regular independent audit to verify that procedures are working.

7.3 SIL RATINGS FOR E / E / PES SYSTEMS

Established reliability engineering techniques can be used to validate the system design for an individual SRS loop. This will involve :

(i) identifying the components which form the SRS loop. This normally involves an instrument or sensor, barriers, cables, control units, actuators and valves.

(ii) drawing a block diagram of the loop.

(iii) obtaining reliability data for each component in the loop.

(iv) calculating the inherent failure rate of the loop in failures per year, taking account of diversity where it exists (for example 1-out-of-2 instrument detection systems), system configuration and common mode failures (for example if two similar instruments are used for the 1-out-of -2 detection system).

(v) assigning a sensible test interval for the whole loop (for example, the whole loop will be tested every three months). The test interval will only be practical if it fits in with production scheduling requirements. For example, if the plant shuts down every three months and the test is disruptive, a test interval of 3 months, 6 months or 1 year would be practical but 2 months would not. It is important that the maximum tolerable test interval is clearly defined. In some cases, on-line test routines may be feasible, thus reducing the frequency of disruptive plant shutdowns for maintenance.

(vi) calculating the fractional dead time (FDT) for the loop.

(vii) comparing the calculated FDT with the SIL requirement for the loop.

(viii) optimising the component reliability, component configuration and test interval to produce an FDT within the required range for the specified SIL level ie. an FDT of between 0.01 and 0.1 for a SIL1 rated loop.

7.3.1 DEFINING FAILURE RATE DATA

The validation of the SIL rating is only as reliable as the base failure rate data which is used for the FDT calculations. Data can be obtained from a number of sources including :

(i) historic experience on site.

(ii) data supplied by manufacturers.

(iii) generic databanks such as OREDA (DNV, 1998) or published sources of failure rate data such as Lees (Lees, 1996).

(iv) data synthesised from theoretical calculations.

Accurate failure rate data is difficult to obtain as it may be (i) generic and not applicable to the specific plant conditions, (ii) collected in a non-systematic manner, (iii) biased towards the commercial priorities of the organisation collecting the data, (iv) categorised inconsistently (fail to danger, fail safe, whole loop failure, individual component failure) or (v) out of date. Errors can be minimised by using agreed standardised data sets within an organisation. This ensures that all SIL rating validations are carried out on a consistent basis.

7.3.2 FRACTIONAL DEAD TIME CALCULATION

The Fractional Dead Time (FDT) represents the probability that the protection system will fail to operate successfully when a demand is placed on the system. It is related to the frequency of failure of the protection system and the test interval for the system. Assumptions are made that all tests are performed correctly, all errors are corrected immediately and loop failures follow a normal distribution ie. failures are randomly distributed over the test intervals. The

equation is only valid if F x T << 1 and D x T << 1 where D is the Demand Rate on the protection system (discussed in **Section 6.1**). The Fractional Dead Time is calculated as :

$$FDT = ½ \times F \times T$$

FDT = Fractional Dead Time. F = Loop failure rate per year. T = Test interval (years).

7.3.3 EXAMPLE SIL1 VALIDATION

Assuming that a simple SIL1 loop requires validation and making simplifications about the component failure rate data, the SIL1 rating can be validated using the following approach.

(i) inherent failure rate of loop calculated as 0.25 per year.

(ii) assume a whole loop test interval of once per year.

(iii) FDT = ½ x 0.25 x 1 = 0.125.

(iv) as the FDT lies outside the required SIL1 range, the loop test frequency will need to be increased.

(v) assuming a loop test frequency of every three months gives a revised FDT = ½ x 0.25 x 0.25 = 0.03.

(vi) this lies within the required SIL1 range (0.01 to 0.1) and SIL1 reliability will therefore be obtained as long as the test interval is adhered to and the correct components are used.

(vii) the maximum allowable test interval for this SIL1 loop would be 0.1 / (1/2 x 0.25) = 0.8 years ie. every 9 months. Using this test interval would just meet SIL1 requirements.

8. SYSTEM SPECIFICATION AND PROJECT COMMUNICATIONS

Full project documentation needs to be created and stored in a clear and auditable format. This will make it easier to communicate project requirements to team members and to third parties such as suppliers.

E / E / PES systems can range from simple hard wired control loop interlocks to complex computer controlled systems which manage multiple SRS's. External suppliers are therefore required whether the E / E / PES uses simple components or complex integrated systems. A clear means of communicating information about SRS requirements, detailed Safety Functions and SIL requirements is therefore required. Suppliers should be encouraged to understand the overall system requirements and may identify possible design errors such as incorrectly specified safety functions. Such issues should be investigated and rectified where necessary by the design team in consultation with the supplier. All changes should be fully documented.

9. LIFECYCLE TEST AND MAINTENANCE REQUIREMENTS

However well the system is designed and installed, it will fail to provide acceptable reliability if it is not correctly tested and maintained using the specified test intervals. IEC61508 therefore places great emphasis on lifecycle safety management to ensure that system performance is acceptable throughout the plant's life. This is best achieved by :

(i) defining clear responsibilities and handovers, including written system and responsibility acceptance documents.

(ii) clearly specifying test and maintenance requirements and procedures and training appropriate personnel.

(iii) ensuring that maintenance personnel fully understand the test procedures and confirm that they are practical. This can be carried out during system acceptance.

(iv) fully documenting test and maintenance records and auditing the maintenace system to verify that it is functioning correctly.

10. PROBLEM AREAS

Many problems need to be resolved when introducing any new standard into a company. Particular problems can occur with IEC61508 because the standard uses a lot of new technical jargon and definitions. This can lead to confusion. Three main problem areas have been identified :

(i) **Lack of commitment and leadership.** It is easy to become demoralised and confused when initially using the standard because of it's technical jargon and the fact that it uses lifecycle safety techniques. If these techniques are not currently used, a great deal of effort has to be put into creating links between different departments and corporate systems. These links can only be established if the team is dedicated and receives support from the company's senior management.

(ii) **Overlooking plant availability constraints.** The project team must balance the need to provide high safety reliability with the need to minimise the spurious trip rate on the plant. If this is not achieved, the plant may be extremely safe but very inefficient. Spurious trips cause plant downtime and may have associated safety hazards or environmental impacts. E / E / PES systems have to be designed carefully to achieve the desired balance. Building redundancy and voting logic into the E / E / PES can help to achieve the required balance but at a cost of making the system more complex and more expensive.

(iii) **Over-reliance on quantitative techniques.** Appropriate use should be made of quantitative and qualitative techniques. Numerical techniques (such as fault tree analysis) provide a thorough and detailed basis for decision making but require more time and effort than qualitative techniques. Furthermore, they may also convey a spurious sense of accuracy in the calculations, forcing the project team to accept impractical solutions to satisfy strict quantitative requirements. Some hazards are better suited to quantitative analysis than others.

11. CONCLUSIONS

IEC61508 is a useful standard for managing life cycle safety on chemical plants with major hazard potential. The standard contains jargon and places great emphasis on project teamwork and documentation. A learning curve therefore has to be climbed before the standard can be efficiently used within an organisation. Greatest benefit is derived from IEC61508 if it is linked into other elements of the organisation's Process Safety Management system. It is a useful tool in itself but it does not address all aspects of major hazard plant safety.

To introduce the standard into an organisation, the following approach is recommended :

(i) select a small project as a trial IEC61508 project.

(ii) assemble a project team and train the team using experienced external resources if they do not exist in-house.

(iii) complete the project and resolve problems as they arise.

(iv) review the trial project. Identify ways of avoiding and resolving problems.

(v) Create the links that are required between IEC61508 and corporate project management systems, Safety Management Systems and Process Safety Management systems.

(vi) start using IEC61508 on all new relevant projects, training new staff before they join the project team or using a mentoring system with experienced staff. In-house expertise will then rapidly develop.

12. REFERENCES AND ACRONYMS

ALARP	As Low As Reasonably Practicable
DCS	Distributed Control System
E / E / PES	Electrical / Electronic / Programmable Electronic System
ERRF	External Risk Reduction Facilities
EUC	Equipment Under Control
FDT	Fractional Dead Time
IS	Inherent Safety
NR	Not Required
OT	Other Technology
PP	Plant Procedures
PSM	Process Safety Management
SF	Safety Function
SHE	Safety, Health and Environment
SIL	Safety Integrity Level
SMS	Safety Management System
SRS	Safety Related System

The following references have been used :

OREDA (Offshore Reliability Data), Third Edition, distributed by DNV (DNV, 1998).

Draft international standard IEC61508, ‘Functional safety of Electrical / Electronic / Programmable Electronic Safety Related Systems’ (IEC, 1998).

‘Draft competency guidelines for Safety Related Systems practitioners’, Institution of Electrical Engineers / British Computer Society / Health and Safety Executive, June 1999 (IEE, 1999).

‘Loss prevention in the process industries’, Second Edition, (Lees, 1996).

Appendix I Example 5 x 5 Risk Matrix For IEC61508 Applications.

5 BY 5 RISK MATRIX

X	X	X	X	X	X	X	X	X	X	X	X	X	1	1	X	X	X	1	1	X	X	1	1	2	3 IND SYS
X	X	X	X	X	X	X	X	X	X	X	X	1	2	2	X	1	1	2	2	1	1	2	2	3	2 IND SYS
X	X	X	X	X	X	X	X	1	1	X	1	1	2	3	1	1	2	2	3	2	3	3	3	3+	1 IND SYS
10^{-4}	10^{-3}	10^{-2}	10^{-1}	1	10^{-4}	10^{-3}	10^{-2}	10^{-1}	1	10^{-4}	10^{-3}	10^{-2}	10^{-1}	1	10^{-4}	10^{-3}	10^{-2}	10^{-1}	1	10^{-4}	10^{-3}	10^{-2}	10^{-1}	1	
V Low	Low	Med	Mod	High	V Low	Low	Med	Mod	High	V Low	Low	Med	Mod	High	V Low	Low	Med	Mod	High	V Low	Low	Med	Mod	High	
EVENT FREQUENCY					EVENT FREQUENCY					EVENT FREQUENCY					EVENT FREQUENCY					EVENT FREQUENCY					
MINOR					SIGNIFICANT					SERIOUS					MAJOR					CATASTROPHIC					

EVENT CONSEQUENCES