A CASE HISTORY OF THE APPLICATION OF DRAFT INTERNATIONAL STANDARDS IEC 1508 TO THE NEEDS OF THE PROCESS INDUSTRIES

G C Tuff - Eutech Engineering Solutions Limited
C J Beale - Allied Colloids Limited

This paper provides an overview of the contents of IEC 1508, and illustrates the practical application of its principles to a major plant upgrade by Allied Colloids, working with consultants Eutech Engineering Solutions (a wholly owned subsidiary of ICI plc). In particular, the paper focuses on how critical Safety, Health and Environmental hazards were identified by the ICI Process Hazard Review tool, and how the hazard prevention and protection systems were subsequently developed and validated as part of a safety life-cycle programme.

IEC 1508 safety-related systems
life-cycle process hazard review

INTRODUCTION

Until the early part of the 20th century improvements in industrial safety were made primarily by learning from incidents and accidents as they occurred. Most effort was aimed at consolidating existing experience and anticipating only the most obvious hazards posed by the introduction of new methods of working or new technology. Regulation tended to be developed independently for different sectors of activity. In today's industrial world, we recognise the need to anticipate and evaluate risks before we engage in any new activity, and there is an expectation that lessons learned in one sector will be adapted to the needs of work in other sectors.

The rapid development of digital electronics and information technology has brought massive changes to every walk of life and has brought an additional dimension to our quest for consistent and acceptable levels of safety. Our world is increasingly dependent on Programmable Electronic Systems (PES) for controlling and monitoring the equipment, processes and systems on which we depend for so many aspects of our lives. We expect these systems to respond "intelligently" to failures in the equipment or process under their control, and even to react benignly to their own failure.

Recognising the need for detailed guidance on how to incorporate PES technology safely into the workplace, the International Electrotechnical Commission (IEC) initiated the development of a new international standard [1] which has provisionally been entitled:- **IEC 1508 : Functional safety : safety-related systems.**

For the purposes of this document, functional safety has been defined as:-

- the ability of a safety-related system to carry out the actions necessary to achieve a safe state for the equipment under control (EUC) or to maintain a safe state for the EUC.

whilst a safety-related system has been defined as one which:-

- implements the required safety functions necessary to achieve a safe state for the EUC or to maintain a safe state for the EUC.

and

- is intended to achieve, on its own or with other safety-related systems, the necessary level of safety integrity for the implementation of the required safety functions.

Not surprisingly, this document, dealing with complex issues, has taken some years to complete. However its key provisions were voted on and accepted last year and formal publication of the total document is scheduled for 1998.

It will be appreciated that, owing to the extensive use of electrical and electronic based safety systems in the process industries, it is likely that the standard will find wide application in this sector once it has been published, although, even in its draft form, the concepts and guidance it contains are beginning to be applied to good effect. Indeed, the main subject of this paper is an account of how the principles contained within the draft standard were applied to an upgrade project, and the lessons that were learned from this experience.

One potential drawback of the standard, however, is that it has been written as a generic document, which, so far as the uninitiated is concerned, renders it difficult to follow and apply in practice. To overcome this obstacle, versions for transport, medical and process industries are already in preparation, but it will be some time before these are made available in the open literature. The version for the process industries has been designated IEC 1511.

Recognising that the approach advocated by IEC 1508 deserves a wide audience, and that some demystification may be required, the authors have, in consequence, set out to offer a subjective overview of the contents of the draft standard, to offer an interpretation of some of the jargon in the context of the chemical and process industries, and to illustrate the practical application of the principles contained within the standard (as it existed in mid 1996) by reference to a chemical industry upgrade project.

It should be noted, however, that neither the authors nor their employers can accept any liability for losses etc.... arising from the use of the information provided. Reference should also be made to the current versions of IEC 1508 and IEC 1511.

OVERVIEW OF DRAFT STANDARD IEC 1508

To gain a clear understanding of this Standard, one must recognise that it encompasses three strands, namely:

- the need for a generic document on which subsequent sector-specific standards may be based consistently;
- the need to place safety-related systems in the broader context of the nature of the equipment they control, and also the context of many aspects in their life-cycle from definition to implementation;
- the need for specific guidance on designing systems to achieve defined functionality and integrity.

We will now describe the standard from each of these three aspects.

Firstly, it should be appreciated that suppliers of programmable electronic systems sell into all sectors (the Internet has shown that digital electronics is no respecter of traditional boundaries!). The standard therefore aims to lay a consistent foundation for all sectors and is necessarily generic in its approach.

A further illustration of the generic nature of the document is that it recognises that the purpose of Electrical, Electronic and Programmable Electronic Systems (E/E/PES) may also be addressed by the use of systems employing other technology, such as hydraulics or fluidics, or even by procedural arrangements for human intervention (External Risk Reduction Facilities). With such a broad scope, it is inevitable that some of the terminology used lacks the familiarity of accepted terminology already established in the process sector.

Secondly, but crucially, the standard establishes a **life-cycle** of interlinking phases. An outline of the IEC 1508 safety life-cycle is presented in figure 1 (by permission of HSE).

The key parameters for the design of a safety-related system are identified as accurately defined **functionality** (what is the system supposed to do in response to defined events?) and quantitative targets of **integrity** (the probability of the safety-related system performing as intended).

The standard recognises that, if the functionality and integrity are to be set correctly, then a thorough identification of all the possible hazards will be required, followed by a careful analysis of the potential risks weighed against what is considered to be tolerable.

There will also be a need for explicit consideration of how the functionality and integrity is to be shared between different protective systems, namely:

- Electrical/Electronic/Programmable Electronic Systems (E/E/PES).
- Systems of other technology.
- External Risk Reduction Facilities.

So far as the process industries are concerned, E/E/PES protective systems might include instrumented protective systems (via a Distributed Control System, Programmable Logic Controller or hard-wired relays). Other technology protective systems might include pressure relief or fire protection systems, and External Risk Reduction Facilities might include human intervention or passive facilities such as bunding.

The key is to obtain an appropriate mix of technologies which, in combination, provide a number of layers of protection to achieve an acceptable level of Safety, Health and Environmental (SHE) performance (or integrity). This process is depicted in figure 2, (by permission of the HSE) which shows how an acceptable level of safety is achieved by assigning risk reduction factors to each of the technologies employed.

The life-cycle describes five phases leading to the proper specification of a safety-related system. The document also deals, however, with a further six phases stretching from installation of the system, through its operation and maintenance, and, eventually, to its decommissioning. At each phase the effectiveness of the systems functionality or integrity can be impaired.

The life-cycle sets the conceptual framework for correct design and operation of the safety-related system, but the standard goes on to explain the procedural measures which need to be established in order to ensure that each phase is correctly executed. Managing the safety life-cycle requires clarity of responsibility, careful planning of each phase, and continual verification that one phase has been properly executed before addressing the next.

Competence of those doing the work and regular on-going assessments of the safety achieved are other important themes covered.

Before describing the third and final subject of the standard - the design of the safety-related systems themselves - some comments on computers are appropriate.

Society has a somewhat ambivalent attitude to the use of computers. We generally accept that we can rely on computers to calculate our salary payments, yet live in growing fear of the "millennium effect".

PES technology impresses us with its ability to perform repeatably - always giving an identical response in a specific situation. However, it horrifies us with its unpredictable response to circumstances not anticipated by the program (at the time of writing, British Gas is being severely criticised for sending out enormous, erroneous bills as a result of switching to a new computerised billing system).

It is important, then, to recognise two quite different types of hazard which can be associated with a PES, and it is helpful to consider a situation where the equipment control function is in a separate PES from a safety protection function.

Malfunctions in the control system may have dangerous consequences - especially where many controls are integrated within a single control PES. However, such malfunctions are likely to be very rare. The reliability of a PES is very high, especially when compared with other elements in a process control loop such as the measurement device and the valve.

Malfunctions in the control system, if anticipated correctly, can also be countered by the appropriate function of a separate protective system. Malfunctions in the protective system itself, however, are less easily comprehended. The protective system is required to function only rarely and, in all but the simplest cases, the combination of events leading to failure may be difficult to predict, and hence to test.

A PES is vulnerable to systematic failure rather than random failure, and so different precautions have to be taken. The emphasis in this instance is on the use of prescribed techniques rather than proof testing.

The third subject of the standard, which lies at its core, is the specification and design of the PES-based safety related system. The process of design is broken down in the standard into a series of activities. The specification of safety functional requirements and safety integrity requirements has already been covered in the early phases of the life-cycle.

Design now requires the development of a suitable architecture, the selection of suitable components and sub-components, and the specification of software tailored to the architecture. After design, the components and the software have to be integrated into a working system.

The standard gives a graded series of methods and techniques which should be applied to the system design process. Selection of the appropriate method or technique is governed by the integrity band specified for the duty (or Safety Integrity Level (SIL) in IEC 1508 parlance).

Given the ambitious scope of this standard, it is hardly surprising that it has taken some time to reach its publication, nor that there has been much debate over its detailed contents. However, the use of this standard as a tool for bringing better management of safety is now becoming evident. One such application is illustrated in the remainder of this paper.

THE PROCESS

Allied Colloids Limited (ACL) is a manufacturer of speciality or "effect" chemicals which are largely based around acrylic polymers. The vast majority of the company's products, which find applications in sectors as diverse as water treatment, the textile and paper manufacturing industries and the oil and mineral extraction industries, are manufactured on a batch or semi-batch basis, although a number of key intermediate products are produced in continuous plant.

Anticipating future growth, the company recently identified the need to increase output from one of the aforementioned continuous plants. This plant comprised a reaction section, two stages of vacuum stripping, a final product purification (distillation) stage and a catalyst regeneration (reactive distillation) stage. The plant was, therefore, fairly representative of the type of process and unit operations commonly found throughout the process industries. A block diagram of the process is presented in figure 3.

Process studies indicated that the plant could readily be de-bottlenecked by the provision of additional heat exchange area and spray condenser capacity, and that the purity of the final product could be increased as part of the same project by the installation of an additional distillation column. Furthermore, it was recognised that significant productivity benefits could accrue from the installation of a distributed control system (DCS). In consequence, a project to carry out the aforementioned upgrades was commenced in January 1995.

As the raw materials and products of this process are toxic, malodorous, flammable and exothermically polymerisable, it is evident that the plant represents a major safety, health and environmental (SHE) hazard potential, necessitating careful management of the process risks which it poses. The need to ensure a high level of SHE performance is compounded by the strategic importance of the plant to the business.

In view of the foregoing considerations, and the fact that the upgrade constituted a major modification to the plant, it was considered appropriate to undertake a fundamental review of the process SHE hazards present in the plant, in order to satisfy both the company and the regulatory authorities that an adequate level of SHE performance was being delivered, and that an adequate level of SHE performance would continue to be delivered throughout the upgrade and beyond.

Following consultation with the Health and Safety Executive and the Environment Agency, it was agreed that the safety life-cycle approach embodied in draft standard IEC 1508 was appropriate to this project, and that the latter should be employed as a SHE assurance tool, since the installation of a DCS on the plant clearly brought the upgrade within the remit of the standard.

However, it was recognised that, due to its generic nature, the application of IEC 1508 would require specialist knowledge. Eutech Engineering Solutions Limited employees of which were familiar with the concepts of IEC 1508, were therefore instructed, with a view to providing the necessary competencies and resources to work alongside ACL on this project.

HOW THE CONCEPTS WERE APPLIED

Given that the plant was already in existence, the first activity was to benchmark the SHE performance of the plant prior to the upgrade. This was, however, not as straightforward as it may have been, since, as a result of a series of minor modifications and upgrades, the plant had undergone "creeping change" since it was built in the mid-eighties.

The approach adopted was to use the ICI/ Eutech Process Hazard Review (PHR) tool as part of a SHE assurance programme. This technique which, was developed to examine the SHE performance of existing facilities is a guideword-driven, what-if technique that is focused on accident initiating events, enabling the major SHE hazards on an existing facility to be identified more effectively than by the traditional HAZOP technique. The problems of using the traditional HAZOP techniques in such cases are described in Reference 2, and include the restriction of focus, the need for very large commitment of management time and the generation of a very broad range of actions. By contrast, PHR is very much a production tool (rather than a design tool), and the participation of key operations staff is crucial to its success.

The PHR study provided a clear identification of the hazards associated with the operation of the plant and produced a list of key procedures for inclusion in a subsequent audit programme (essential to ensure adequate SHE performance throughout the life-cycle of the plant). In addition, potential weakness' in the pressure relief, fire protection and instrumented protective systems were identified.

The next stage was to assess the potential impact of each hazard in terms of its consequences, and thus identify those hazards with serious safety, health or environmental implications.

These relatively serious (SHE critical) hazards were then analysed further, firstly by developing a simple cause and effect logic to identify the chain of events leading from one or more initiating events to the undesired consequence. Secondly, the risks associated with each logical chain were estimated, using order of magnitude estimates to provide very approximate numeric estimates of the probable frequency of occurrence and likelihood of unacceptable consequences.

These crude estimates were nevertheless sufficient to enable a view to be taken on whether the risks were likely to be tolerable, and to identify the relatively few but important risks which needed to be attenuated. This procedure should not be confused with the much more rigorous Quantified Risk Assessment (QRA) analysis that might be appropriate when significant off-site consequences could occur or very high levels of reliability are being sought.

The next stage concerned the allocation of various protective measures (protective systems, control systems, fire protection system, pressure relief systems) to achieve an acceptable pattern of risk reduction, and the specification of the safety function and safety integrity level (crudely, the reliability) required of each protective measure. In practice this was an iterative process, the object being to avoid over-reliance on any one channel of protection and to avoid over-demanding targets of integrity.

The contribution to risk reduction which can realistically be achieved from the Distributed Control System was debated at length. Clearly, the normally correct operation of the DCS ensures that some potentially hazardous events are stifled at birth. However, as IEC 1508 makes clear, it would be unwise to over-value the contribution which the DCS can be counted upon to make, especially since failures in the control system itself may be one of the potential initiating events leading, ultimately, to the consequence which one is trying to protect against.

Discussions with the proprietary suppliers confirmed that they have designed and configured their system primarily as a process control device and that the detailed way in which the software has been developed and electronic hardware configured have not, as yet, been rigorously assessed against the criteria given in IEC 1508 for protective duties.

In order to achieve a balanced distribution of protection, a separate, dedicated protective system was therefore introduced to accommodate some of the risk reduction.

Programmable technology has been selected to provide flexibility and speed of configuration and follows the guidance given in IEC 1508.

The information generated during the Plant Study has been documented into two key reference documents: A Hazard and Risk Management Description, which records the analysis of risk and the assumptions involved, and a Maintenance and Operation Plan, which details the proof-testing and protective system maintenance procedures which must remain in force if the desired safety integrity is to be maintained.

LESSONS LEARNED

As a result of applying the new standard to a specific plant and situation, we made a number of observations based on this experience.

Different parts of the Standard are aimed at different people (Designers, installers, maintainers, operation managers, contractors). Before holding discussions about the application of any part of the Standard, it will always be important to ensure that all participants have a sound common understanding of the key underlying concepts.

Without such common ground, there are likely to be misunderstandings between individuals. In particular, we found difficulties in addressing the requirements for managing the functional safety of the control and protection systems of the plant, and the appropriate competencies of staff involved, before we had achieved a common and thorough appreciation of the details of each phase of the safety life-cycle. Against this, it has to be said that it was only through the process of applying the life-cycle to a real plant that we were able to develop a truly common interpretation of the document.

We found the concept of the life-cycle was very powerful, and served three separate key purposes:

1 Gaining an understanding of many of the provisions of IEC 1508 is made easier by relating them to the life-cycle process.

2 Clarifying Allied Colloid's own life-cycle processes, and gaining ownership of each of the phases.

3 By assigning a percentage completion against each phase, we were able to generate a "gap" analysis and this, in turn, led naturally to an action plan. By following the life-cycle approach, we could be confident that we had taken a comprehensive view on all the major areas for action.

We found that the content of each phase of the life-cycle had to be adapted to become relevant and helpful to the analysis of the specific plant and processes which we were studying.

For example, we found it difficult to distinguish between Phase 1 (Concept) and Phase 2 (Overall Scope Definition). The previous use of the PHR technique provided an ideal platform to enable us to undertake Phase 3 (Hazard and Risk Analysis).

The identification of potential hazards, the sequence of events which would precede them, and the likely consequences, were readily available from the PHR study. From these we developed order of magnitude estimates for the probable frequency of the events (in the absence of protection).

Phases 4 (Overall Safety Requirements) and 5 (Safety Requirements Allocation) proved more difficult to apply directly from the Standard.

The overall aim is clear: One is seeking to define one or more protective facilities or systems which will reduce the residual pattern of adverse consequences to a tolerable level. There were, however, several trade-offs to be made.

For example, the tolerability of one hazardous event is inevitably influenced by the number and severity of other possible hazardous events as one tries to define an acceptable overall result. Improvements in safety protective systems or external risk reduction facilities tended to yield quantum increments in integrity, so that the overall pattern of risk and distribution of protection had to be recycled to achieve a balanced and acceptable result.

The application of Phase 9 (Realisation of the E/E/PES System) required considerable clarification of the contribution allowable from the existing DCS System, and of the limitations which the Standard imposes. However, this clarification provided a sound starting point from which to begin the specification of an additional independent protective system .

The Standard was still in draft form at the time of this study, so there were significant gaps in the Annexes where, eventually, one would expect to find guidance and data in specifying and designing each element in the complete protective loop (Measurement / Logic / Final Actuator / Human Factors etc.,).

Finally, we note that Phases 6, 7, 8, and 11 through to 16 require and assume a high level of cross-organisational co-operation to achieve and maintain required integrity for functional safety over the entire life-cycle of the facility.

It is evident that significant work will be required to work through the implications of this generic standard in the context of any specific organisation, but the experience of Allied Colloids has been that the expenditure of such effort is ultimately worthwhile.

REFERENCES

1 The International Electrotechnical Commission " IEC 1508 : Functional Safety : Safety Related Systems."

2 Turney RD and Roff MF : "Improving Safety, Health and Environmental Protection on Existing Plants : Process Hazards Review." : 8th International Seminar on Loss Prevention and Safety Promotion in the Process Industries, Antwerp 1995.

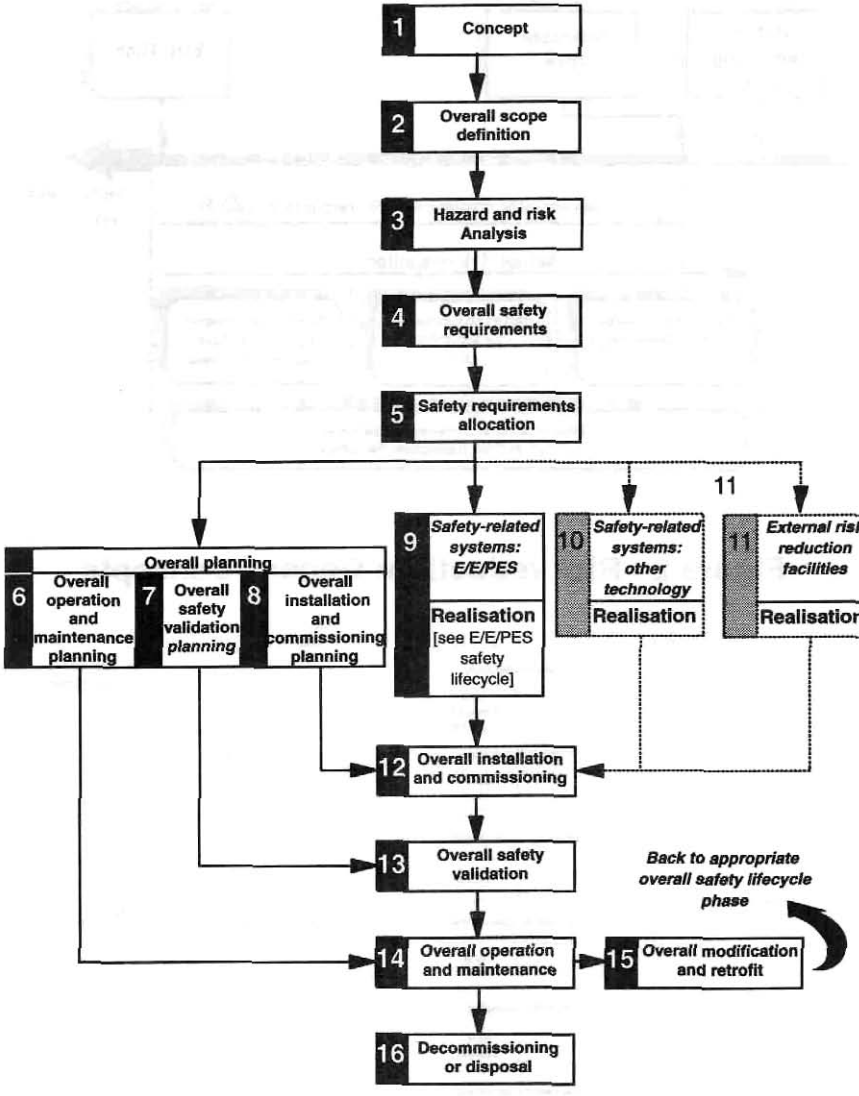

Figure 1 - Overall safety lifecycle

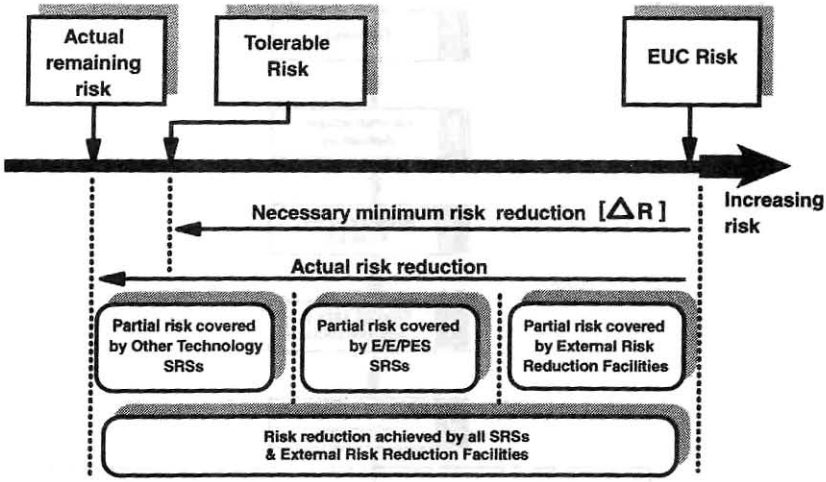

Figure 2 - Risk reduction: General concepts

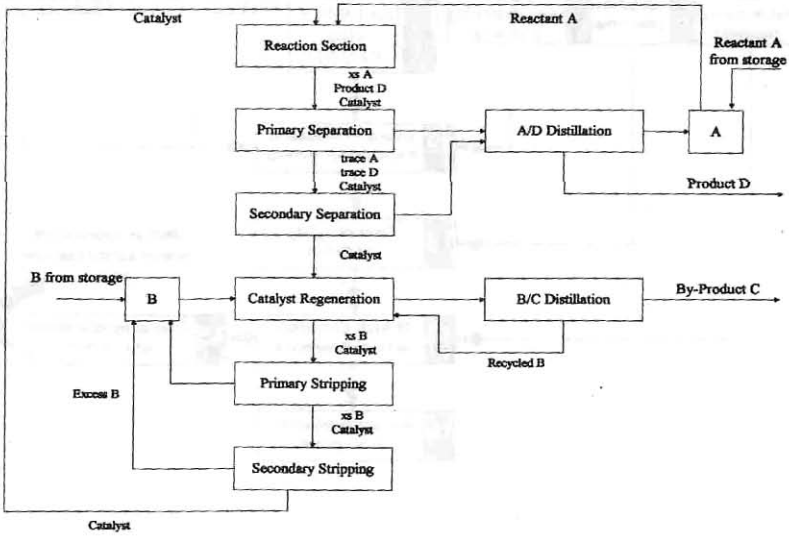

Figure 3 - Plant Block Diagram