EMERGING INTERNATIONAL STANDARDS FOR INSTRUMENT PROTECTION SYSTEMS USED IN SAFETY APPLICATIONS

M Wilson, Health and Safety Executive, W M Black, BP International

This paper provides an overview of two draft standards, IEC 1508 and IEC1511. The first draft international standard is IEC 1508 Functional safety of E/E/PE safety-related systems which is being developed by the International Electrotechnical Commission (IEC). The second is IEC1511 Functional Safety:Safety Instrumented Systems for the Process Industry which is the process sector interpretation of IEC 1508. This paper identifies key features of the two standards and there current progress.

INTRODUCTION

A draft international standard IEC 1508 on the functional safety of safety-related systems has been developed by the International Electrotechnical Commission (IEC). The proposed standard is a generic standard which can be used in any industrial sector concerned with safety-related protection systems. Work has also started on IEC1511which is the process sector interpretation of this standard Both standards have their roots in concerns about using programmable electronic systems, and software in particular. However they apply to all electrotechnical technologies, from the humble relay through solid-state electronics and onto programmable electronic systems.

The structure of IEC 1508[1] is shown in table 1 below. IEC1511 is not sufficiently advanced to have a defined structure as yet, although it is believed it will comprise a number of parts, mirroring the parts of IEC 1508.

IEC1508 has been designated a basic safety publication by the IEC and as such other IEC standards must adopt its principles and approach.

Table 1 - Structure of IEC 1508

IEC1508	Title of section
Part 1	General requirements
Part 2	Requirements for electrical/electronic/programmable electronic systems (E/E/PES).
Part 3	Software requirements
Part 4	Definitions
Part 5	Guidelines on the application of part 1
Part 6	Guidelines on the application of parts 2 and 3
Part 7	Bibliography of techniques

AIM OF THESE STANDARDS

The overall goal of these standards is to ensure that plant and equipment are safely automated. The standard is concerned with :

- ensuring an adequately designed, installed and maintained protection system
- preventing failures of control systems triggering other events which in turn could lead to danger (eg fire, release of toxic materials, repeat stroke of a machine etc)
- preventing undetected facilities in protection systems making them unavailable when needed for a safety action, eg in an emergency shutdown system.

This should be contrasted with so-called primary causes of danger such as electric shock which although important are well covered by existing standards and are not therefore within the scope of these standards.

The term *functional* safety has been used to define this aspect of safety and is 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.

Failures in control systems can be categorised into two types:

- Random failure: where components can fail due to the action of wear and tear mechanisms at any point throughout their design life.
- Systematic failure: these generally result from some form of human error and are often inherent within the system eg inadequate specification. One of the features of a systematic error is that it will not be revealed by testing.

Random failures can be detected and prevented from becoming dangerous by the use of fault tolerant design techniques, diagnostics and regular proof checking. Systematic failures can be prevented by the management of safety, use of competent personnel and providing suitable systems and procedures.

Most control system failures are as a result of systematic failure rather than random failure.

SYSTEMATIC FAILURES

These standards are being produced to minimise both systematic and random failures. They emphasise three key elements to combat systematic failures. These are

- safety management
- safety lifecycle
- functional safety assessment.

These three elements are discussed in greater detail below.

Safety Management

Safety management concerns planning, organisation, monitoring and review of preventive and protective measures. Of particular importance is the competence of the persons involved in managing and developing safety-related control systems.

Most incidents involving control systems (of all technologies) are caused by a combination of technical and managerial failures. A typical incident, taken from a recent HSE publication,[3] which illustrates the importance of safety management is described below. The incident is taken from the chemical industry and illustrates a systematic failure:

In a computer controlled batch-reactor plant, the specification for the computer program for handling alarms contained a fundamental error. The computer was programmed so that if a fault occurred in the plant all controlled variables, eg cooling water flowrate, would be left as they were and an alarm would go off.

The computer had also been programmed to increase the flow of cooling water to the reflux condenser immediately after a catalyst had been added to the reactor.

When a fault arose just after the catalyst had been added, the computer failed to increase the flow of cooling water, the reactor overheated, pressure increased, and caused the contents to be discharged to atmosphere when the relief valve lifted.

(Please refer to An engineers view of human error[6] for a more detailed description of this incident)

This incident happened even though a hazard analysis had been carried out. Either this analysis was not thorough enough, or those carrying out the analysis made wrong assumptions about how the programmer would interpret the requirements of the design at the detailed design stage.

Whatever the reason, those concerned with both the design of the control system, and the programming of the computer, were presented with an inadequate specification of the required safety functions of the plant. The primary purpose of a specification is to provide an unambiguous way of communicating user requirements.

The effect of this particular combination of events would probably have been revealed if the specification had been analysed with respect to the particular failure modes of the control system, as opposed to adopting a general principle of "freeze on fault".

As the above example shows, technical criteria for safety are not enough - paying attention to detail and to properly manage the technical issues are just as important - hence the need for safety management.

Safety Management also encompasses risk analysis which attempts to answer some basic questions:

- Firstly, what can go wrong, how often will this happen and what are the consequences

- Secondly, determining the most appropriate combination of measures and systems for preventing and controlling this

The standards require a risk analysis to be carried out and that the installed system(s) meet the original targets set. It does not set risk targets because the determination of such targets and the form they take (eg numerical or detailed proscribed measures) are determined by social, legal and policy issues which vary from country to country. However the results of risk analysis are used to determine the required safety integrity level for the safety-related protection system.

Safety integrity is defined as 'the likelihood of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time'

Table 2 - Safety Integrity Levels

SAFETY INTEGRITY LEVEL	TARGET FAILURE MEASURES FOR A SAFETY-RELATED SYSTEM	
	DEMAND MODE OF OPERATION PROB OF FAILURE / DEMAND	CONTINUOUS - HIGH DEMAND MODE OF OPERATION PROB OF FAILURE / YEAR
4	$>=10^{-5}$ to $<10^{-4}$	$>=10^{-5}$ to $<10^{-4}$
3	$>=10^{-4}$ to $<10^{-3}$	$>=10^{-4}$ to $<10^{-3}$
2	$>=10^{-3}$ to $<10^{-2}$	$>=10^{-3}$ to $<10^{-2}$
1	$>=10^{-2}$ to $<10^{-1}$	$>=10^{-2}$ to $<10^{-1}$

Four levels of safety integrity are defined in IEC 1508, see table 2 above. These levels relate to single systems only.

The standards use this table as a baseline against which performance can be assessed.

It is these safety integrity levels which determine what equipment should be used and what techniques and measures should be adopted during the design, installation, commissioning, maintenance and modification of the equipment.

Safety Lifecycle

The concept of a 'lifecycle' is well established and is increasingly being used as a 'model' to focus attention on the importance of functional safety as a discrete function in every phase of this lifecycle. Figure 1 below shows the overall safety lifecycle model used in the proposed international standard.

The *'safety lifecycle'* is defined as*: The necessary activities involving safety-related systems, occurring during a period of time that starts at the concept phase of a project, and finishes when any safety-related systems are no longer available for use.*

The safety lifecycle phases are shown as rectangular boxes in figure 1 below.

Each phase has an input, an objective, a set of associated safety activities, and an output, or 'deliverable'. The deliverables of one phase provide the inputs to the next. Running across all the lifecycle phases are verification and assessment activities. The safety lifecycle model is essentially a 'top-down' approach. Iteration will occur eg hazard and risk analysis is shown only once, but in reality this activity can only be of a preliminary nature at this point in the safety lifecycle. Hazard and risk analysis is used continually throughout the safety lifecycle, and particularly during the 'realisation' phase (the phase in which the design and implementation is undertaken).

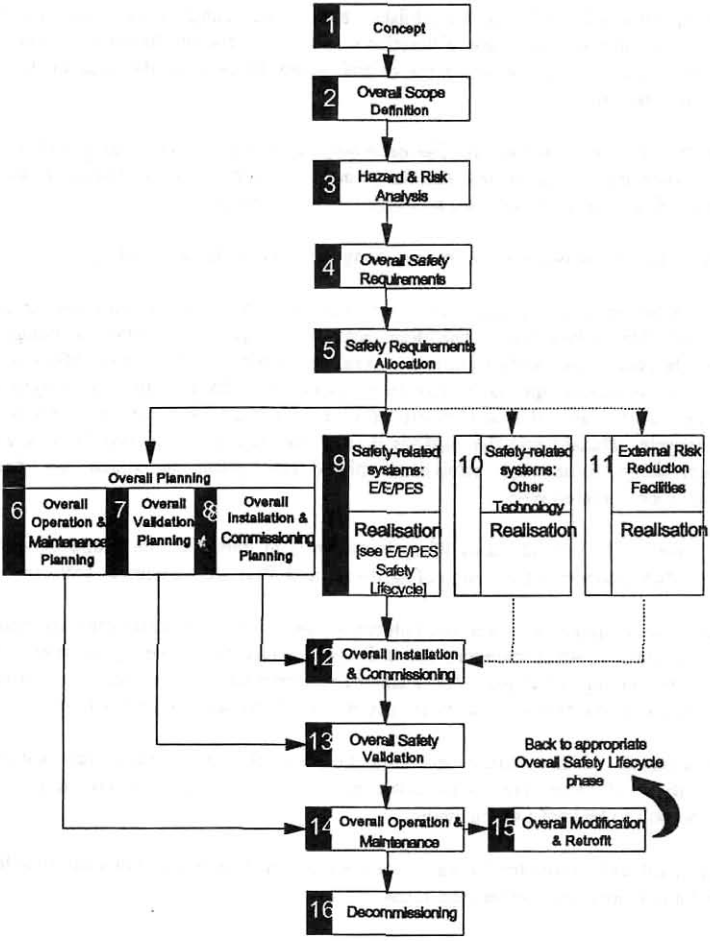
Figure 1 shows the overall safety lifecycle which is in Part 1 of the proposed international standard. Part 2 concerns the design of hardware and Part 3 the design of software.

Software is only subject to systematic failures. Of particular note is the software design safety lifecycle in Part 3 which provides for software quality assurance eg version control and software engineering techniques. The standard recommends various measures and techniques to prevent systematic failures in software depending on the safety integrity level.

The structuring of the safety lifecycles between the three parts has allowed good harmonisation of what are often different discipline areas and provides a way for documentation to be kept to a minimum.

The Safety Lifecycle provides the framework within which activities important to safety can be managed and systematic failures minimised.

Figure 1 - Overall Safety Lifecycle



Functional Safety Assessment

The third measure to prevent systematic failures is functional safety assessment which is defined as:

The undertaking of an investigation in order to arrive at a judgement of the functional safety achieved by one or more safety-related systems and/or external risk reduction facilities.

Whilst the project team may well have verified their design there may a need for an independent safety review, particularly for complex systems. This second opinion will in most cases come from within the same organisation. However, for the highest levels of safety integrity, or very serious consequences in the event of safety-related system failure, independent third-party assessment may be required.

RANDOM HARDWARE FAILURES

To overcome random hardware failures the standard requires that a safety-related control system :

- Possesses a specified level of fault tolerance.
- Achieves the required safety integrity target.

In order to demonstrate the safety integrity target above, designers can either use a reliability model or they can use an equivalent set of criteria which are developed within the standard.

MAINTENANCE AND MODIFICATION

One of the benefits of a lifecycle approach is that the standards require consideration of maintenance and operational requirements during the design phase. They also describes the measures and systems which have to be implemented to ensure that the protection systems safety integrity is maintained until it is no longer required.

The key issues associated with this are

1. The need to proof test to discover dangerous unrevealed failures (the test interval will be determined by a number of factors including, equipment used, safety integrity level required and diagnostics facilities inherent within the system)

2. Control of **all** modifications to the system. Modifications are the second highest cause of failures in protection systems usually because they were implemented without the full safety implications being considered. The standard requires that the safety significance of a modification is assessed and that the appropriate phase in the lifecycle is returned to.

3. On an ongoing basis the system is reviewed and assessed to ensure that the safety integrity levels which the system was designed to achieve are still appropriate and are being achieved.

MAJOR ISSUES DEBATED DURING STANDARDS DEVELOPMENT

During the development of IEC1508 and IEC1511 there have been a number of important issues which have been difficult to resolve. In many cases agreement has been reached on what changes are necessary, in somecases the issues are still under debate. The difficulties in most cases have not been technical but have been caused by the following:

- Legal requirements in each country are different with respect to risk
- Relationships with Regulatory Authorities vary considerably
- The practice in each industry sector is different
- Concern that existing facilities may be expected to meet the new standards

The difficulties have been resolved in most cases by careful selection of words which enable the essential requirements to be realised in a number of ways. In a number of cases the alternatives have been presented in an informative annex which then allows different industries and different countries to adopt methods appropriate to the application. Care is therefore needed before concluding that all options available in the standard are equal and meet in all respects legal requirements of all Countries.

Details of some of the areas discussed during the development of the two standards are described below.

MAJOR ISSUES WITH IEC1508

When safety is achieved using protective instrument systems it needs to be recognised that the level of complexity is generally significantly greater the with other means of risk reduction such as relief valves or passive protection. Competency and effective planning of work at all lifecycle stages are therefore key to reducing failures due to systematic causes. IEC 1508 sets out what needs to be considered at each stage of the implementation relating to these issues. The standard also recognises the importance of good maintenance, operations and modification procedures. Failures or demands due to systematic causes need to be recognised and modifications initiated to ensure the probability of repeat occurence is minimised. Requirements are also included for the collection of data on fialures and demands and analysis of this data to ensure assumptions made during design were valid.

To be effective all of the above activities need to be within the framework of a safety management system. It needs to be appreciated that many of the requirements are already included within the normal quality and safety processes within projects. Where Contractors and Vendors work in accordance with ISO9000 the guidance within the standard shows how quality principles should be applied within a functional safety context.

To ensure these aspects were fully covered, Iec 1508 stated requirements for Safety Management. There was a concern from some Countries that Safety Management was outside the intended scope of the workgroup. It will now be made clear within the standard that what is being stated are requirements to ensure the technology is properly managed. It was considered vital that Management are properly advised on these issues. A number of paragraphs have been reworded and the section retitled as 'Managment of Functional Safety'.

ENVIRONMENTAL PROTECTION

The risk based approach is equally suited to protection of the environment and the current version of IEC1508 recommends its use for such applications. Emerging regulations in Europe and the USA relating to the environment has led the working group to consider if more detailed guidance would be of benefit. There are a number of difficulties in applying the risk based approach to the environment and the working group are still considering the options. One of the difficulties is likely to be the range of environmental consequences which must be considered. There will also be difficulty in reaching agreement on methods to determine the environmental integrity levels (EIL?) for a range of applications. In many cases it will be difficult to evaluate the long term effects of environmental consequences. A further question arises as to how to determine integrity levels in the case where a single failure leads to both safety and environmental consequences. The simple approach of using a system with the highest required integrity level is probably the most effective but this will need agreement.

ASSET PROTECTION

The risk based approach when applied to asset protection should result in minimum whole life cost and hence maximum value for the stakeholders. There is little doubt within the working group that the approach when applied to asset protection will lead to benefits. However some members of the working group have taken the view that these issues should be the subject of internal procedures within individual companies rather than the subject of an international standard. Agreement on the inclusion of asset protection has yet to be reached.

The implication of including environmental and asset protection into the scope of the IEC1511 standard are summarised as follows:

1. The standard will provide a "one stop" guide for instrument engineers for all categories of protection.

2. The standard will establish the most effective protection taking into account all the consequences of a hazard.

3. The extension of the integrity level definitions to environment and asset protection will develop a larger market for equipment with defined integrity levels and lead to lower costs.

4. There would be a need to introduce the concept of environmental integrity levels and asset integrity levels. It is suggested that these are linked to the instrumented function. The system would have a specified integrity level only. This would be an advantage for vendors and any independent body undertaking a conformity assessment since they are not usually in control of where equipment is applied.

CONTROL SYSTEMS WITH SAFETY FUNCTIONS

The concept of safety instrumented control systems is not well recognised within the process control industry. Mainly because safety functions which require continuous control are rare. However most modern control systems have the capability to **functionally** carry out protection. Many of these control systems are highly reliable (although this does not necessarily extend to the sensors and actuators). Control systems (and their associated

sensors and actuators) are often the dominant demand on many protection systems. However if a very low demand rates from a control system can be claimed, safety instrumented protection systems become unnecessary. Where a very low demand rate is claimed from a control system the control system performance affects safety and it will be important to ensure that the entire system is designated a safety related system throughout its entire lifecycle. Currently IEC1508 places a number of constrains on the claimed reliability of control systems if they are not to be treated as safety systems.

Under certain circumstances it may be an advantage to designate a control system as a safety system even though this will place restrictions and costs on the process of implementing the system. The circumstances where it could be an advantage to designate a control system as a safety system could be as follows:

- where the majority of demands on the protection system arise because of failures of the control system;

- where the extra cost of implementing the control system as a safety system is lower than the extra cost if the protection system need to be implemented to a higher integrity level. This will need to take into account the costs of a having to implement the requirements for safety on a large scale (control system) as opposed to a small scale (protection system) application.

It should be noted that the performance of currently available control systems need to be high to face the expectations of production management. Quality and high availability are critical to business performance and commercially available control systems are designed to meet that need. There are likely to be benefits if performance capability of such systems can be utilised by allowing credit to be taken for low demand rates.

There is likely to be significant resistance to these ideas in the process sector. It woul however be unfortunate if a sector standard excluded the future use such an approach.

CURRENT STATUS AND EMERGING ISSUES

Parts 1 and 3,4 and 5 of IEC1508 are now at the Draft International Standard Stage whilst 2,6 and 7 are at the Committee Draft and Vote stage. We should see the Committee Draft version of part 1 of IEC1511 shortly.

There are a number of issues emerging which may influence the final version of both standards:

- A new standard for low complexity protection systems.
- A growing perception that the standards not only provide the basis for the design, installation, commissioning, maintenance and modification of protection systems designed to ensure the safety of people, but that this approach is equally applicable for those systems designed to protect the environment.

Conclusions

HAZARD AND RISK ANALYSIS

The perception of risk and the requirements relating to safety depend on the application sector and the country of intended use. in many cases open discussion of such issues becomes difficult and any standard trying to set requirements in this area is faced with considerable difficulties. Expectations vary between wanting the standard to set absolute levels of risk through to avoiding the issue altogether. Neither option is viable for an international standard on safety. Again there has been concern from some countries that hazard identification and risk assessment were outside the scope and competency of the working group. The approach adopted by the working group has been to require a hazard identification process to be carried out without being prescriptive about how it should be done. On the risk of risk reduction the approach has been to set out a framework of the issues to be considered, allowing both qualitative and quantitative methods to be used. Some changes will be made to the text to make it clear that for the purposes of the standard there is no requirement to assess absolute levels of risk. The only requirement of the standard is to determine the safety integrity level and by inference the range of risk reduction required from consideration of the parameters of the application. This can be done by calculation or using one of the risk graphs included in part 5. It should be noted where risk graphs are used to calculate safety integrity level they may only meet the minimum level of safety requirements. It will still be necessary to demonstrate that risk has been reduced to as low as reasonably practicable. Care is also needed when selecting and using risk graphs. Not all risk graphs set out in part 5 are equally suited to all sectors. One of the risk graphs was originally developed for the machinery sector and there may be some difficulty in applying the approach to the process sector. It is intended that sector specific standards produce risk graphs appropriate for that specific sector.

SELECTION OF SYSTEM ARCHITECTURE AND TEST INTERVALS

Determination of architectures and test intervals is relatively straightforward providing reliable date is available for the application and appropriate models can be agreed. Unfortunately this is not always the case. The ISA Committee drafting SP84.02 has had considerable difficulty reaching agreement on these issues. The working group drafting IEC1508 has faced similar difficulties, but it is now believed that a feasible approach has been identified. Key to the approach has been the recognition that architectures and fault coverage for the logic functions are so diverse that agreement on the performance of such systems cannot be reached. The best that can be achieved is agreement on the methods that should be used to determine performance. To maintain a specified level of performance during the operating phase it is essential to carry out periodic proof checks. The interval between proof checks will depend on the reliability of the equipment and the diagnostic coverage. It is clear that in many industries that this information on reliability is not readily available and in some cases vendors are claiming very high levels of diagnostic coverage without any real evidence. Where there is uncertainty in performance it is clear that equipment or testing costs will need to be higher. It is hoped that the prospect of reduced costs through better information will stimulate more work in this area.

A particular problem in predicting the performance of redundant architectures has been how to account for common cause failures. If pessimistic predictions are made, common cause issues can easily dominate calculation to such an extent that additional spending to make system improvements becomes a waste of time. When the basis of existing models and available data were considered it became clear that much remained to be done in this area. A pragmatic

approach together with good judgement is probably the best way forward. There is likely to be significant debate about how much credit can be taken from the systematic approach required by standard when making judgements on the value of beta factors for different levels of diversity. There does however appear to be good agreement on what needs to be done to reduce the incidence of common cause failure and guidance will be given in next issue of the standard.

SIMPLE SYSTEMS

One of the essential requirements of the standard was that it should lead to the safe implementation of complex technology such as programmable electronic equipment. In the case of simple applications using simple technology many of the requirements will not be relevant. It will be made clear in future issues that not all the requirements will apply to simple systems providing this is justified during safety planning. It is also acknowledged that there is a need for an approach aimed at simple applications and new work is being considered in this area.

OTHER TECHNOLOGY AND EXTERNAL RISK REDUCTION

The lifecycle set down in IEC1508 included a requirement to determine safety functions and safety integrity levels for other technology safety systems and external risk reduction. The reason why this was considered necessary was to make sure that all safety functions and performance requirements were allocated in a systematic way before allowing credit to be taken for effective risk reduction. Some countries considered that this could be interpreted as instrument engineers telling other engineers how to do their job. It could also have been argued that this was needed. It is being made clearer that the standard provides a framework only with respect to risk assessment. The requirement will be that the safety function and performance of these other systems should be taken into account when determining safety functions and safety integrity of E/E/PES systems.

DOCUMENTATION

The general impression on its first reading the standard is that a large number of new documents are required if E/E/PES technology is used for safety applications. Some effort was made to make it clear in the documentation section that the essential requirement was for appropriate information to be made available. Unfortunately this was insufficient to remove the impression that the document set referenced in the main clauses was part of the requirements of the standard. The text has now been changed by removing all document titles and making it a requirement for information to be recorded and retained.

MAJOR ISSUES WITH 1511

The working group has taken as its starting point the current version of IEC1508. The terminology has been changed to be more immediately understandable to personnel in the process industry but the basic structure and concepts have remained unchanged. The following issues have been discussed in the working group:

This paper has provided the latest position concerning the emerging IEC International Standards on the 'Functional safety of safety-related systems'. The three key concepts of safety management, safety lifecycle and assessment are now firmly established. This together with technical requirements for software engineering techniques and design criteria for fault tolerance will provide a robust structure to accommodate, and harness safely, new technology as it emerges.

References

1 IEC 1508: Functional safety of E/E/PE safety-related systems: Parts 1 to 7 Available from BSI.

2 IEC 1511: Functional safety of instrument based protection systems for the process industry Part 1

3 'Out of Control - Why control systems go and how to prevent failure' HSE publication ISBN 0-7176-0847-6

4 'The tolerability of risk from nuclear power stations'. HSE publication. ISBN 0 11 886368 1.

5 BELL R and REINERT D 'Risk and system integrity concepts for safety-related control systems'.

6 KLETZ T 'An Engineers View Of Human Error' Institute of Chemical Engineers ISBN 085295265 1

7 Risk Analysis of Technological Systems - Application Guide. IEC56 (secretariat) 410