STANDARDS FOR COMPUTER CONTROL IN THE PROCESS SECTOR

John Brazendale

Health and Safety Executive, Bootle L20 3QZ

An outline of draft international standard IEC 1508 is given with particular application to protection systems used in the process industries. The paper details how the standard treats random hardware faults, common cause faults and systematic faults in both hardware and software.

STANDARDS PES COMPUTER SOFTWARE SAFETY RELIABILITY

INTRODUCTION

Process plant, machinery and other equipment can, if they malfunction, present risks to persons from hazardous events such as fires, explosions, radiation overdoses, machinery traps ...etc. One of the ways such plant and machinery can malfunction is from failures of electro-mechanical, electronic, and programmable electronic (E/E/PES) devices. Failures can arise either from physical faults in the device eg. from wear and tear occurring randomly in time (random hardware faults) ; or from systematic faults eg. errors made in the specification and design of a system that cause it to fail under some particular combination of inputs under some environmental condition. As well as inputs from sensors this includes data entry by operators and associated with this are potential systematic faults due to poor interface design.

Computer-based systems offer many advantages not only economic, but also the potential for improving safety. However, the attention to detail required to realise this potential is significantly greater than is the case using conventional system components.

Some of the benefits include:

- the ability to automatically perform proof checks on critical components at a frequency significantly higher than would be possible with manual approaches;
- the potential to provide sophisticated safety interlocks;

- the ability to provide diagnostic functions and condition monitoring which can be used to analyse and report on the performance of plant and machinery, in real time;

- the potential to provide better information to operators and hence improve decision making affecting safety.

The use of computer-based systems in safety related applications does however raise a number of problems which need to be adequately addressed. In particular, these include:

- Complexity leads to design errors that are not easily identified;

- the failure modes are complex, very large in number, and not always predictable;

- it follows that is impossible to fully test a computer-based system and therefore there may be a set of inputs that occurs when the system is in actual use that the designer has not tested. If you are lucky the result may be just a minor inconvenience; if you are not the computer may fail to carry out some critical task or it may do something different altogether that is dangerous e.g. opening a valve at the wrong time;

- the traditional engineering approach of testing a system at the end of development is not therefore sufficient - attention has to be paid to the procedures used in its design, implementation and maintenance. The emphasis is on preventing mistakes rather than on finding them by testing.

TYPICAL APPLICATIONS.

Computers have been used extensively in the process industries for many years, e.g. in refineries. Because of concerns over their reliability they have until recently not been used in a direct safety role. Protection was provided by mechanical devices (e.g. vents and relief valves) and by electrical relay-based trip systems e.g. for overfill protection on storage tanks. This is now changing. Increasing experience of successful operation and the codification of good engineering practices has led to this technology becoming more widely accepted for safety roles. Typical applications include burner management systems, emergency shut down systems, and fire and gas systems.

PROPOSED IEC INTERNATIONAL STANDARD

HSE recognised that there was a need for guidelines on computer safety as long ago as 1981 and issued a small booklet called "Microprocessors in Industry", which pointed up the changes in traditional approaches to industrial safety that would be necessary in dealing with computer-controlled plant and machinery. It followed this up in 1987 with the well known PES Guidelines (see reference 5). Feedback on that document indicated a demand for a generic standard on this topic and this has led to the work described in this paper.

The International Standard is being developed under the auspices of the International Electrotechnical Commission (IEC) entitled **" Draft IEC 1508 - Functional safety: Safety-related systems"**. The proposed Parts of this standard are:

- **Part 1: General Requirements;**
- **Part 2: Requirements for Electrical/ Electronic / Programmable Electronic Systems;**
- **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**

When finalised, this generically based International Standard will constitute an IEC **basic safety publication** covering functional safety for electrical/electronic/programmable electronic safety-related systems and will have implications for all IEC standards, covering all application-sectors. for the future design and use of safety-related control systems. It will set the framework to facilitate the development of sector standards (eg. medical, transport, process control).

APPLICATION SPECIFIC STANDARD ON PROCESS CONTROL

Work on this standard has recently started in order to provide an interpretation of IEC 1508 for the process sector. The terms of reference for this new task are as follows:-

- "To develop an International Standard that specifies the functional safety requirements for electrical/electronic/programmable electronic safety-related systems for the process industries. The standard shall conform to the International Standard "Functional Safety: Safety-Related Systems" Parts 1, 2 and 3 being prepared by Working Groups 9 and 10. The proposed International Standard shall take into account current and emerging standards and documents relevant to the process industries.....";
- "To develop associated guidance to aid the understanding of the International Standard proposed above";
- "To develop guidance for specific safety-related system architectural configurations appropriate to the process industries that will aid the designer in meeting specific target Safety Integrity Levels."

The countries agreeing to participate in this task are as follows:-

Canada, China, Czech Republic. Finland. France. Germany, Italy. Japan. Netherlands. Poland, United Kingdom, Sweden and the USA.

As well as IEC 1508 this standard will utilise information from existing standards and guidelines relevant to the process sector. Of particular note here is an ISA standard (see reference 6) and a German Namur Guideline (see reference 7). The ISA standard - " Application of Safety Instrumented Systems for the Process Industries" is nearing the final stages in the USA. It is closely aligned with IEC1508, but places less emphasis on safety management because of the nature of the standard. The Namur guideline " Safety of Process Plants using Measurement and Control Equipment " is similar to the German VDE 0801 standard (see reference 8) which although still a draft is being used by TUV to give "certification" to safety PLCs. Part 2 of IEC 1508 is similar in concept to the hardware parts of VDE 0801 and therefore it can be seen that there is a convergence of standards taking place.

DRAFT IEC 1508: FUNCTIONAL SAFETY: SAFETY-RELATED SYSTEMS

The standard combines safety management with technical criteria. This makes it different to many traditional standards which are either procedural eg. ISO 9001; 1994 "Quality Systems - Model for quality assurance in design, development, production, installation and servicing "; or technical (eg. the set of tests to meet IEC 801-3 - " Electromagnetic compatibility for industrial process measurement and control equipment").

The rationale for this is due to the nature of failures causing danger in control equipment.

An analysis of 34 incidents for a forthcoming HSE publication (1) suggests that most control system failures may have their root cause in an inadequate specification. (see figure 1). In some cases this was because insufficient hazard analysis of the Equipment Under Control (EUC) had been carried out: in others it was because the impact on the specification of a critical failure mode of the control system had not been assessed. Many of these failings ultimately can be traced back to a lack of Safety Management.

It is acknowledged that because of the small sample size the results of this analysis are not statistically significant, and therefore care needs to be taken in using these results to generalise for all control system failures. However other studies provide support for these conclusions, in particular in the area of software development a number of studies have shown that errors made during specification account for most software faults and failures. See for example (2).

The only way to prevent this type of error is by good safety management procedures - if the specification is wrong or the design intent is not properly followed through no amount of "testing" at the end will find the problem. A good example of this is illustrated in the incident described in figure 2.

Safety Management.

Safety management concerns planning, procedures, organisation, monitoring and review of the technical activities. The scheme adopted in IEC1508 is similar in concept to ISO 9001, but with the necessary emphasis on safety activities such as hazard and risk analysis, verification and validation, and safety assessment. In order to structure the safety management requirements a lifecycle approach has been adopted - the safety lifecycle - shown in figure 3. 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 overall goal is to encourage a systematic approach that fosters collaboration and good communication between engineering disciplines and between users, vendors and contractors.

Technical Criteria.

The main technical criteria in Part 1 of IEC 1508 are given below in the context of protection systems eg. Emergency shut down systems as these are the main interest in the process industry :-

Risk Assuming that we are at the outline design stage of the Equipment under Control (EUC), that design is required to be subject to a hazard and risk analysis. (It should be emphasised that as detailed design proceeds

hazard and risk analysis may have to be repeated). For each hazardous event (eg. explosion) possible from the EUC a hazard and risk analysis has to be carried out and the following specified:-

- The consequences of the hazardous event.
- The likelihood of it happening
- The event sequence involved
- The level of safety required

The standard allows risk to be specified qualitatively or numerically. Part 5 of IEC 1508 gives guidance on a number of ways of specifying this information. However it does not preclude other ways. For example in the process industries the Fatal Accident Rate (FAR) is quite common (at least for major hazard sites) and this would be "acceptable" to IEC 1508.

The overall approach to risk reduction is shown in Figure 4. The standard does not say what level of safety is appropriate, because this a legal issue outside the scope of the standard.

If risk is specified qualitatively then there has to be a link to the safety integrity level - because this is the *driver* for the design criteria. Hence schemes like the Hazardous Event Severity Matrix (see Figure 5 below) which have been developed by the Centre for Process Safety in the USA (see reference 3). The safety integrity level (SIL) is a measure of the safety performance of the protection system - see Table 1 below

TABLE 1 - SAFETY INTEGRITY LEVELS: TARGET FAILURE MEASURES

SAFETY INTEGRITY LEVEL	DEMAND MODE OF OPERATION (Probability of failure to perform its design function on demand)	CONTINUOUS/HIGH DEMAND MODE OF OPERATION (Probability of a dangerous failure per 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 $<10^{-1}$

Safety Requirements Specification. Having specified the target level of safety, the standard requires that a specification is drawn up which defines the process conditions which require safety actions. The specification will define the safe state and the process inputs and outputs including the various modes of the system eg. start-up, maintenance ..etc. Although the focus of IEC 1508 in on instrumented systems the standard recognises that safety will be achieved by a package of instrument, mechanical (eg. relief valves) and procedural means and requires that their role be defined, but it does not go into the detail of how the safety integrity of these other measures is assured.

For each function the specification details the required target safety integrity level. At this stage equipment is only being considered in outline. The following gives the criteria for assessing the design solution to the Safety Requirements Specification.

Claim Limits for Protection systems. The standard recognises that there is a great danger in "the numbers game" and that common mode and other systematic causes of failure will limit the achievable levels of safety integrity (equivalent to availability) in a protection system. Care also needs to be taken with failure data.

The standard limits the safety integrity that can be claimed for a single safety-related system which contains an E/E/PES device to level 4 ie. no lower than 10^{-5} failure per demand .

For SIL 3 and 4, (see Table 1) a theoretical prediction of safety integrity (eg. by part count) is not considered adequate. You can only claim SIL 3 and 4 if the components forming part of the proposed protection system have been used many times before in a wide range of systems and applications including a similar environment to the one proposed in a system of comparable complexity ; and there has to be relevant and accurate failure data (generic data is not adequate).

Particularly in protection systems based on a PES there are likely to be many safety functions in the same system. In these circumstances the SIL for the system has to be based on the highest SIL of the safety functions allocated to that system.

Demand Rates from control systems Particularly in the process industries. it is good practice to separate control and protection. If one does that there is then the need to calculate the demand rate from the process control system so that the safety integrity level of the protection system can be calculated. This is usually done by field or vendor supplied data, but the standard places a limit as to what can be claimed.

A control system that is placing demands on a protection system cannot claim a safety integrity level (demand rate) lower than 1in 10 years, unless it is qualified by the IEC 1508 process. The failure rate (used to calculate the demand rate) of a control system has to be quantified by analysis or operational experience.

Defences against Common Cause Failures (CCF) in mixed technology systems. We want ensure that CCFs do not negate the benefits of redundancy in mixed technology systems. for example between an instrumented system and a pneumatic logic system.

If a mixed safety architecture of say 3 safety-related systems in parallel (eg hydraulic ,electronic, and mechanical) is suggested as the solution to an overall SIL level requirement, then the SIL levels can only be "added" if they are functionally diverse. (This is a stricter requirement than statistical independence and generally means measuring a different state variable and controlling a different manipulated variable).

If they are not Functionally Diverse then the standard requires the designer to justify the claimed SIL, taking into account common cause failure.

Defences against Common Cause Failures in Protection Systems. We want ensure that CCFs do not negate the benefits of redundancy between instrumented systems. A qualitative " by inspection" set of criteria" are given or an analytical (quantitative method) can be used.

If two or more protection systems are in parallel and are based on electromechanical, electronic or programmable electronic devices then their individual SILs can only be "added" if they are:-

- Functionally diverse.
- Implemented in diverse technologies.
- Not share common parts or services whose failure could initiate a CCF.
- Have a predominant failure mode for common support systems that is in a safe direction.
- Procedurally diverse ie. they do not share common operational, maintenance, or test procedures.
- Physically separated.

Otherwise a dependent failure analysis has to be undertaken which shows that the probability of dependent failure is very much less than the required safety integrity level.

Criteria for the design of a single protection system The design of the safety-related system should, commensurate with the safety integrity level, provide protection against random hardware faults by an appropriate combination of fault tolerance, on-line diagnostic coverage and manual proof checking . (see Table 2 below). Justification that you have achieved these requirements is either by reference to Tables in the standard that link SIL with these features (see Table 3 below); or by a quantitative analysis.

The Architecture should commensurate with the SIL provide protection against systematic faults. Justification that you have achieved this requirement is by "demonstration" that certain techniques and engineering practices have been used eg separation of power from signal lines. Tables in the standard rank the techniques against the SIL. If techniques other than those used in the standard are used then a detailed justification is required.

TABLE 2: EXTRACT FROM IEC 1508 PART 2 : FAULT REQUIREMENTS: PROTECTION SYSTEMS

SIL	FAULT REQUIREMENTS FOR TYPE A COMPONENTS	FAULT REQUIREMENTS FOR TYPE B COMPONENTS
1	• Safety-related undetected faults shall be detected by the proof check.	• Safety-related undetected faults shall be detected by the proof check.
2	• Safety-related undetected faults shall be detected by the proof check.	• For components without on-line medium diagnostic coverage, the system shall be able to perform the safety function in the presence of a single fault. • Safety-related undetected faults shall be detected by the proof check.
3	• For components without on-line high diagnostic coverage, the system shall be able to perform the safety function in the presence of a single fault. • Safety-related undetected faults shall be detected by the proof check.	• For components with on-line high diagnostic coverage, the system shall be able to perform the safety function in the presence of a single fault. • For components without on-line high diagnostic coverage, the system shall be able to perform the safety function in the presence of two faults. • Safety-related undetected faults shall be detected by the proof check.
4	• For components with on-line high diagnostic coverage, the system shall be able to perform the safety function in the presence of a single fault. • For components without on-line high diagnostic coverage, the system shall be able to perform the safety function in the presence of two faults. • Safety-related undetected faults shall be detected by the proof check. • Quantitative hardware analysis shall be based on worst-case assumptions.	• The components shall be able to perform the safety function in the presence of two faults. • Faults shall be detected with on-line high diagnostic coverage. • Safety-related undetected faults shall be detected by the proof check. • Quantitative hardware analysis shall be based on worst-case assumptions.
Type A components have predictable failure modes and there is good failure data. Type B components are the opposite eg. microprocessors.		

TABLE 3 - EXTRACT FROM IEC 1508 PART 2-ARCHITECTURE

Safety Integrity Level (SIL)	PE logic system Configuration	Diagnostic Coverage per channel	Off-line Proof Test Interval (TI)	Mean Time to Spurious Trip (MTTFspurious) On -line Repair
1	Single PE, Single I/O, Ext. Watchdog (WD)	Low	1 Month	1.9 Years
	Single PE, Single I/O, Ext. WD	Medium	6 Months	1.7 Years
	Single PE, Single I/O, Ext. WD	High	48+ Months	1.6 Years
	Dual PE,Dual I/O,1oo2	None	6 Months	1.4 Years
	Dual PE,Dual I/O,1oo2	Low	16 Months	1.0 Years
	Dual PE,Dual I/O,1oo2	Medium	36 Months	0.8 Years
	Dual PE,Dual I/O,1oo2	High	36 Months	0.8 Years
2	Single PE, Single I/O, Ext. WD	High	6 Months	1.6 Years
	Dual PE, Single I/O	High	6 Months	10 Years
	Dual PE,Dual I/O,1oo2	None	2 Months	1.4 Years
	Dual PE,Dual I/O,1oo2	Low	5 Months	1.0 Years
	Dual PE,Dual I/O,1oo2	Medium	18 Months	0.8 Years
	Dual PE,Dual I/O,1oo2	High	36 Months	0.8 Years
In the full table similar entries are given for dual systems with diagnostics and for dual 2002 and TMR systems.				

Software A safety-related computer application should be developed and maintained under a Quality Management system which complies with ISO 9001 and ISO 9000-3. The procedures of the quality system should be set out in document form and made known to all personnel connected with the development.

A Software Requirements Specification should set out completely and unambiguously the software safety functions in a way that permits traceability from the software to the Safety Requirements Specification. The quality system should ensure that throughout the development process, the software is adequately documented at an appropriate level of detail, both to assist the lifetime maintenance of the application, and to provide the audit trail necessary for subsequent assessment of the safety-related application.

Safety-related software should be developed within a lifecycle which clearly identifies the development stages eg. software requirements specification, design specification, implementation, verification and validation, etc. . A documented Quality Plan should set out the acceptance criteria to be satisfied at each stage.

A comprehensive test plan should be devised and documented which demonstrates that the working software is a correct implementation of the required safety functions. The successful test results of every issued version of software should be documented as evidence that the Safety Requirements Specification was satisfied.

Effective configuration management and change control during development should ensure that changes in requirements, specifications, design, etc. are adequately documented, and that the impact of all changes is analysed to ensure that the Safety Requirements Specification is satisfied. After commissioning, the working software should

be protected from unauthorised change, and its precise configuration (eg. list of modules, version number, etc.) should be recorded accurately.

From the above it can be seen that the approach is to control the factors that influence the achievement of safety integrity in software. These include:-

- Rigour of software quality assurance approach.
- Choice of software engineering technique.
- Software architecture

This is the approach taken by Part 3 of the standard which indexes these factors against the required safety integrity level. An example table from the standard is included below (Table 4) .

TABLE 4 - EXTRACT FROM IEC 1508 PART 3-SOFTWARE

Software Design and Development				
TECHNIQUE / MEASURE	SIL 1	SIL 2	SIL 3	SIL 4
Formal Methods including for example, CCS, CSP, HOL, LOTOS, OBL, Temporal Logic, VDM and Z	----------	R	R	HR
Semi - Formal methods	R	HR	HR	HR
Strut. Methodology including for example, JSD, MASCOT, SADT, SSADM and Yourdon	HR	HR	HR	HR
Modular Approach	HR	HR	HR	HR
Design and Coding Standards	R	HR	HR	HR

CONCLUSIONS

An outline of draft international standard IEC 1508 has been given with particular application to protection systems based on programmable devices used in the process industries. The paper details how the standard treats random hardware faults, common cause faults and systematic faults (eg. design errors) in both hardware and software.

Parts 1 - 7 of IEC 1508 will be issued in July 1995 to all National Committees as part of a major consultation exercise. Parts 1, 3, 4, and 5 will be issued as Committee Draft for Vote (CDV). Parts 2, 6, and 7 as Committee Drafts (CD). Comments are required back to the IEC by November 15th 1995. Final publication of Parts 1, 3, 4, and 5 is expected in late 1996. Final publication of Parts 2, 6, and 7 is expected in late 1997.

The systematic approach and technical principles used in the standard are increasingly being used in new projects and is being adopted in other standards initiatives (for example in medical applications - see reference 4).

The framework for dealing with this topic is now substantially in place, further work will be along two strands. Firstly to incorporate emerging technologies such as fuzzy logic, expert systems ...etc into the IEC 1508 framework. Secondly to gain feedback on the application of the standard to see where further advice may be needed and to generally refine its contents.

References

1. Out of Control - Control Systems - Why they went wrong, and how to prevent failure. HSE Books. PO Box 1999 Sudbury Suffolk CO 10 6FS. ISBN 0 7176 0847 6.

2. P Mellor, 1994 High Integrity Systems Volume 1 No 2. Page 101. CAD: Computer-Aided Disaster.

3. The Center for Chemical Process Safety (CCPS) - Guidelines for the safe automation of chemical processes. 1993. The American Institute of Chemical Engineers. 345 East 47th Street, New York, New York 100017. ISBN 0-8169-0554-1.

4. Medical Electrical Equipment. Part 1 : General requirements for safety. Collateral Standard: Programmable electrical medical systems. Draft IEC 601-1-4.

5. Programmable Electronic Systems in Safety-Related Applications. No.2 General Technical Guidelines. Available from HSE Books PO Box 1999 Sudbury Suffolk CO 10 6FS. ISBN 011 883906 3.

6. ISA -dS84.01. Draft Standard. Application of Safety Instrumented Systems for the Process Industries. ISA PO Box 12277, Research Triangle Park, NC 27709.USA.

7. Namur Guideline NE 31. Version 2.9 1994. Safety of Process Plants using Measurement and Control Equipment. Namur c/o Bayer AG, Gebaude K9, D-51368 Leverkusen. Germany.

8. DIN VDE 0801 "Principles for computers in safety-related systems."

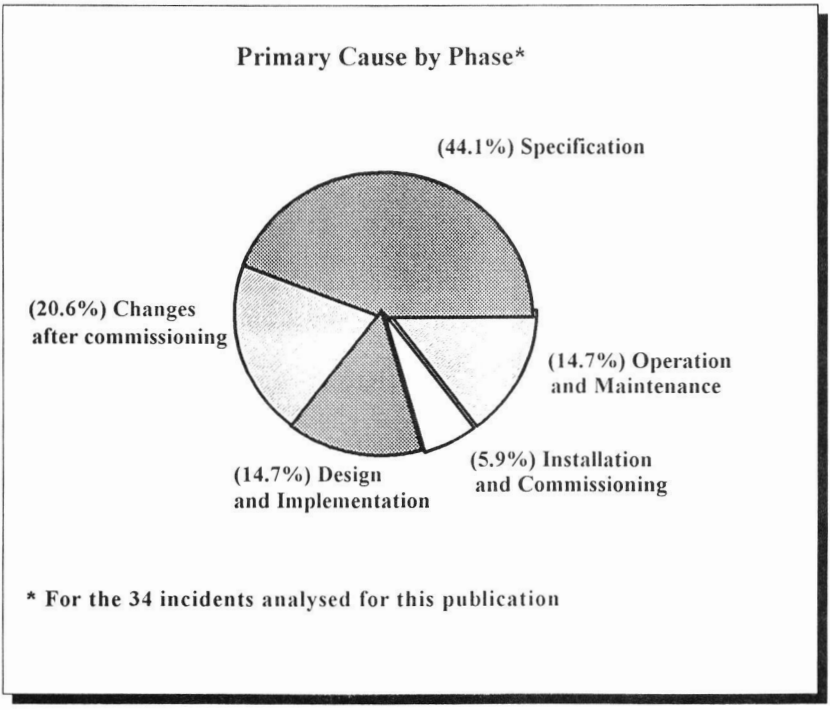


FIGURE 1: INCIDENCE OF CONTROL SYSTEM FAILURES

Inadequate Installation And Commissioning: Chemical Plant Gas Release

At a computer-controlled chemicals plant, a reactor gas valve opened unintentionally, causing the waste gas vent line to rupture and release noxious gases to atmosphere. Checks established that there had been no programmed or manual operation of the valve which was subsequently found to be working correctly. The investigation therefore turned to the control system and the output interface.

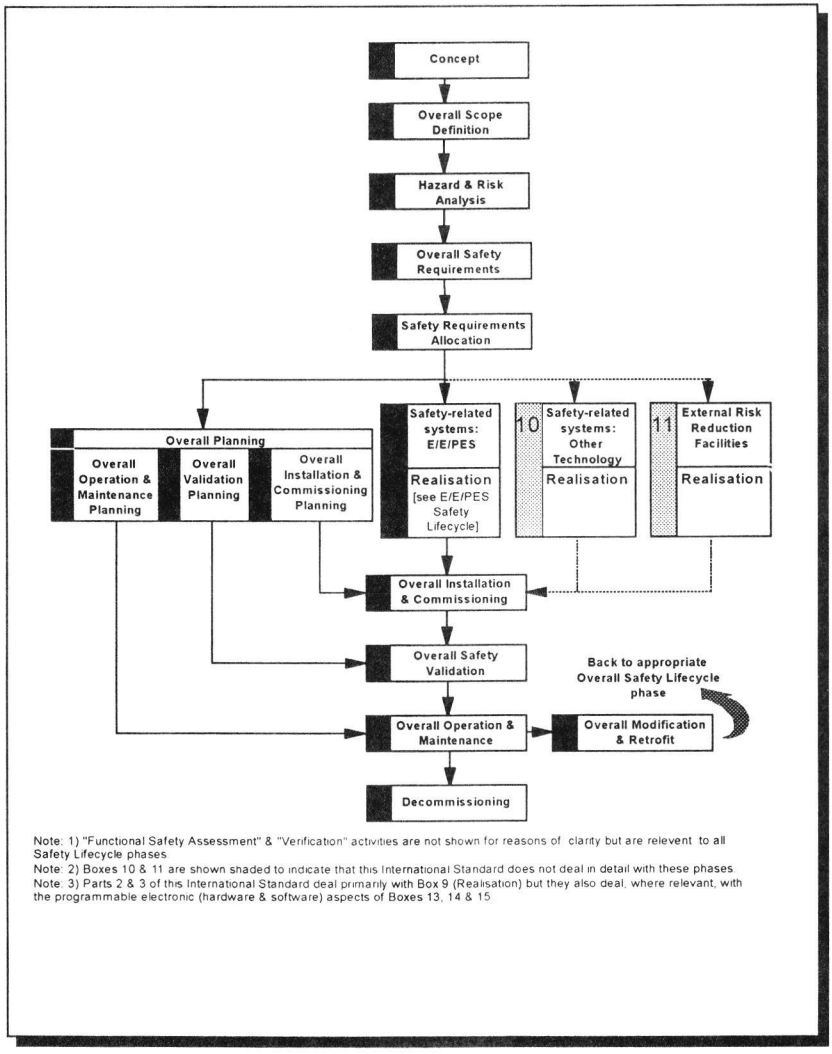
The output interface contained three types of interface card communication across common address and data highways to the main control system. Extensive investigation of the incident traced the cause to a fault on the 'driver' card which caused the gas valve to operate. The fault was identified as the omission of a ground connection for bit 15 on the data highway terminal which was being used as an additional address line. This meant that the card 'address' was not unique, and it was in fact responding to commands and data from the control system which were intended for a different card altogether.

It was discovered that this fault affected two such gas valves and had been present for the 6 years since the control system was commissioned. Its presence was revealed only by the particular combination of plant states prior to the incident. Since the reactor gas valve was required to 'freeze' on air failure, the valve was controlled from an output card which provided a train of pulses. These cards allowed for a choice of positive or negative going pulses by providing two input connections for bit 15 on the data highway, the unused input requiring to be connected to ground potential. It was the omission of this connection that caused the pulse output card to respond to messages intended for an on/off output card.

Contributory factors include inadequate pre-delivery inspection which overlooked the missing connection, and the questionable decision to rely on the status of a single 'bit' in the design of a safety-related system.

This incident demonstrates the importance of detailed installation and commissioning procedures so as not to compromise the safety integrity built into the system. Installation and commissioning procedures should be specified as explicitly as practicable, with supporting documentation which required the signature of the installation technician on completion of thorough inspections and functional tests. Monitoring of such documentation, and recording resultant changes or temporary measures, plus participation in installation and commissioning activities by technical management, will then ensure adherence to these procedures.

FIGURE 2 : INCIDENT FROM "OUT OF CONTROL " (1)



Note: 1) "Functional Safety Assessment" & "Verification" activities are not shown for reasons of clarity but are relevent to all Safety Lifecycle phases.
Note: 2) Boxes 10 & 11 are shown shaded to indicate that this International Standard does not deal in detail with these phases.
Note: 3) Parts 2 & 3 of this International Standard deal primarily with Box 9 (Realisation) but they also deal, where relevant, with the programmable electronic (hardware & software) aspects of Boxes 13, 14 & 15.

FIGURE 3 - OVERALL SAFETY LIFECYCLE

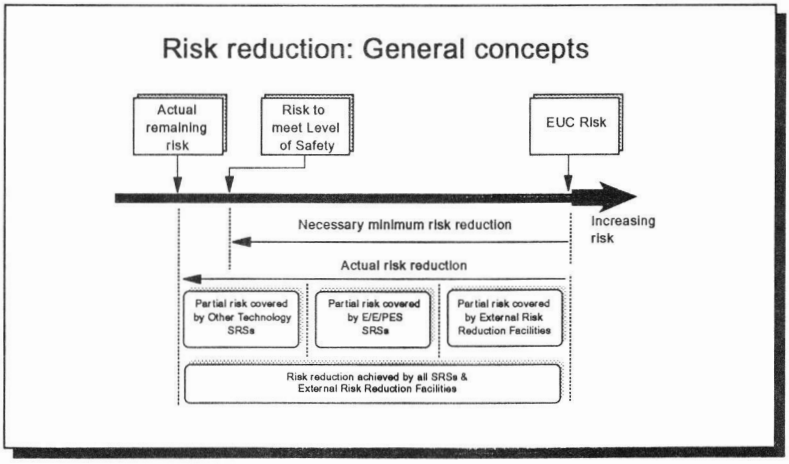


FIGURE 4 : RISK REDUCTION

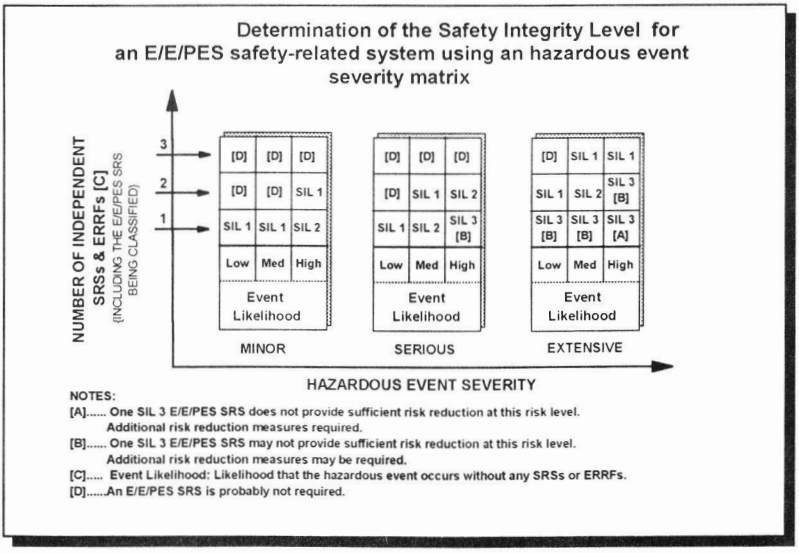


FIGURE 5: HAZARDOUS EVENT SEVERITY MATRIX