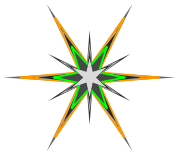


S T S A R C E S

Standards for Safety Related Complex Electronic Systems

Annex 11

Applicability of IEC 61508 & EN 954

Task 1: A study of the links & divergences between draft IEC 61508 and EN 954

Final Report of WP4

S J Brown & S Frost

HEALTH & SAFETY EXECUTIVE

HSE

European Project STSARCES
Contract SMT 4CT97-2191

CONTENTS

1. INTRODUCTION

This report compares the methodologies and requirements of two standards: Draft IEC 61508 (Functional safety of electrical/electronic/programmable electronic safety-related systems)[1] and EN 954 (Safety of machinery - Safety related parts of control system)[1]. The report discusses whether these two standards are likely to set the same or differing requirements when applied to machinery control systems.

Both standards propose a structured approach towards the design of safety-related control systems but differ in that EN 954 is designed to address all types of control system technologies whilst Draft IEC 61508 has been primarily (but not exclusively) designed to apply to electrical/electronic/programmable electronic (E/E/PE) based control systems. The standards require that the safety-related functions of the control system are classified; Draft IEC 61508 requires that the control system be allocated a safety integrity level whilst EN 954 uses the concept of safety performance and places the system into one of five categories. There is a significant difference in the way that the safety integrity levels and categories are derived and defined; it is the problems that this difference causes that are discussed in this report especially when the two classifications are compared with a view to developing a strategy to link them.

Draft IEC 61508 uses a safety lifecycle approach to ensure that the design of a safety-related control system is systematically carried out. This lifecycle is examined to establish whether it would be suitable for the design of machinery control systems.

The report begins with an examination of the two standards with regard to their scope, strategies for the design process and the methodology of their respective safety integrity classification systems.

2. OVERVIEW OF STANDARDS

2.1 EN 954 (Safety of machinery - Safety related parts of control systems)

2.1.1 EN 954-1 (Safety of machinery - Safety related parts of control systems: General principles for design).

[1] Note 1. This report is based upon the following versions of the standards: Draft IEC 61508 Version 4.0 05/12/97; EN 954-1 December 1996; and Draft EN 954-2 Revision 11 November 1997.

2.1.1.1 Introduction

EN 954-1 is intended to be used during the design of machinery control systems. It applies only to the safety-related parts of that control system but does encompass all technologies; programmable electronic systems are specifically stated as being within its scope.

The standard describes a design strategy, a list of characteristics and requirements of safety functions, and a categorising system for the safety related parts together with a section describing the validation requirements. A scheme of five categories of safety-related systems is proposed but these categories are not structured hierarchically in terms of their resistance to faults or their reliability. A category is defined in respect of its resistance to faults and its subsequent behaviour in fault conditions, and it is recommended that they should be used as reference points.

Draft IEC 61508 is not called up as a normative standard by EN 954, although it is referred to as guidance in the clause dealing with validation requirements. Also, it is listed at Table 1 amongst standards giving requirements for characteristics of safety functions implemented by programmable electronic systems.

2.1.1.2 Design strategy

The standard assumes that a risk assessment has been carried out in accordance with the principles of EN 1050: 1996 'Safety of machinery - Principles of risk assessment', which determines the contribution to risk reduction that each safety related part of the control system shall make. This contribution may be only a subset of the overall risk from the equipment under control. The machinery design lifecycle begins with EN 292-1: 1991 'Safety of machinery - Basic concepts, general principles for design. Part 1. Basic terminology, methodology' where the requirement is to identify the hazards and assess the risk (*EN 292-1 clause 5.2)* then remove the hazards or limit the risks as much as possible (*EN 292-1 clause 5.3),* by the suitable choice of design features (*EN 292-2 clause 3),* such as applying safety principles when designing control systems (*EN 292-2 clause 3.7).* This leads to EN 954, although it quoted as a normative reference in EN 292-2: 1991 as 'Safety of machinery - Principles for the design of safety-related control systems'.

The design strategy proposed by EN 954 is as follows:

Step 1 Hazard analysis and risk assess at the machine (as required in EN 292-1 and using EN 1050);

Step 2 Decide the measures for risk reduction by design and/or the provision of safeguards (as required in EN 292-1 and EN 292-2);

Step 3 Specify the safety requirements for the safety-related parts of the control system in terms of the characteristics of the safety functions, measures to achieve risk reduction and the selection of category(ies) for each of the safety functions;

Step 4 Design the safety-related parts of the control system in accordance with the specification developed in Step 3 following a general strategy where emphasis is placed upon fault resistance and verification of the safety-related parts in the context of the specified safety function(s) and category(ies); and

Step 5 Validate the achieved safety function(s) and category(ies) against the specification developed in Step 3 with re-design as necessary. The validation requirements for programmable electronic safety-related parts of control systems are subject to detailed procedures for tests of fault behaviour - guidance on the assessment of programmable electronic systems includes a reference to Draft IEC 61508.

Having decided the measures to reduce risk, the selection of a category for a particular safety-related part of a machinery control system depends upon:

(i) the reduction in risk to be achieved by safety function to which the part applies;

(ii) the probability of occurrence of a fault in that part;

(iii) the risk arising in the case of a fault in that part;

(iv) the measures taken to avoid, tolerate or detect a fault in that part.

In general EN 954-1's design strategy correlates with Draft IEC 61508 lifecycle phases 3 (Hazard and risk analysis) to 13 (Overall safety validation).

2.1.1.3 Categories

This section describes the categories and their scope. The authors' comments on the requirements are in italics.

2.1.1.3.1 Category B

As a minimum the safety related parts of the control system shall use basic safety principles that are relevant to the specific application so those parts are able to withstand:

(i) expected operating stresses;
(ii) influence of processed material;
(iii) other relevant external influences.

No special measures for safety are applied to parts complying with this category (*implies that any component may be used in the safety related system provided it is "suitable for use*").

When a fault occurs it can lead to loss of the safety function.

2.1.1.3.2 Category 1

Category B applies (*components suitable for use*). In addition the system shall be designed using well-tried components (see Note 1) and well-tried safety principles (see Note 2).

NOTE 1: A well-tried component for a safety-related application is defined as a component which has been:

- widely used in the past with successful results in similar applications; or
- made and verified using principles which demonstrates its suitability and reliability for safety-related applications.

NOTE 2: Well-tried safety principles include:

- avoidance of certain faults, eg. avoidance of short-circuit by separation;
- reducing the probability of faults, eg. over/underrating of components;
- by pre-determining the failure mode, eg. components which fail open- circuit when power should be removed in the event of a fault;
- detect faults at an early stage; and
- restrict the consequences of a fault, eg. earthing of equipment.

This category permits certain assessed faults to be excluded because the fault rate is known to be very low.

Experience of a part's operation in one application (ie "well tried") may not be suitable for another application.

The probability of failure in category 1 is lower than in category B and therefore the loss of safety function is less likely. When a fault occurs it can lead to the loss of the safety function and additional measures which are not provided by the safety related parts of the machine control system may be necessary to satisfy the Essential Health and Safety Requirements of the Machinery Directive (see Annex A of EN 292-2).

It is noted that single electronic components alone are not normally able to realise category 1 (*This is assumed to apply individual electronic components such as transistors, triacs etc)*.

Also, newly developed components and safety principles are considered equivalent to 'well tried' if they satisfy the conditions in Notes 1 and 2 above. *(This implies that it is only possible to justify a newly developed component as 'well tried' by verifying that the principles underlying its design and construction are relevant to the safety-related application*).

2.1.1.3.3 Category 2

Category B (*components suitable for use*) and the use of well-tried safety principles apply.

In addition, the safety functions of the safety related parts of the control system shall be checked at suitable intervals by the machine control system:-

(i) at the machine start-up; and
(ii) prior to the initiation of any hazardous situation; and
(iii) periodically during operation if the risk assessment and the kind of operation indicates that it is necessary.

The initiation of the check may be automatic or manual. If the check detects a fault a safe state shall be maintained until that fault is cleared. The occurrence of a fault may lead to the loss of the safety function between checks but its loss shall be detected at the next check. (*This implies that if the check is carried out prior to the hazard being initiated there is a probability that the safety function could then fail during the hazardous event (leading to danger). The failure of the safety function must then be detected at the next check; this may be quite onerous because it requires that any failure or sequence of (accumulated) failures within the safety function shall be detected).*

2.1.1.3.4 Category 3

Category B (*components suitable for use)* and the use of well-tried safety principles apply. In addition, the control system shall be designed so that a single fault does not lead to the loss of the safety functions, taking into account common mode failures.

Safety will be maintained in the presence of a single (*detected)* fault. Whenever reasonably practicable the single fault shall be detected at or before the next demand upon the safety function.

The category allows for some faults not to be detected and that an accumulation of faults may lead to a hazard situation at the machine *(The standard implies not just loss of the safety function but that the control system could initiate an output that could lead to a hazardous situation).*

2.1.1.3.5 Category 4

Category B (*components suitable for use)* and the use of well-tried safety principles apply. In addition, the control system shall be designed so that:-

(i) a single fault doe not lead to a loss of the safety functions; and

(ii) the single fault is detected at or before the next demand upon the safety functions. If this detection is not possible, then an accumulation of faults shall not lead to a loss of safety functions.

Common mode failures are taken into account. The system behaviour is that when faults occur the safety function is always performed and the faults will be detected in time to prevent the loss of the safety function. *(This implies that the control system will never fail to danger and, consequently, must be considered to have a high level of safety integrity).*

2.1.1.3.6 Summary of category requirements.

Table 1 lists the requirements for each of the categories.

One or more safety related parts may be used to perform one or more safety functions. If combinations of parts are used which have different categories, the category that may be assigned to the complete system must be established by a new overall analysis of the combination of parts and their fault behaviour. For example, the combined category of a system that used a category 1 part and a category 3 part could be equivalent to category 1, 2 or 3 and may be 4 depending upon their structural configuration at the machine.

2.1.1.4 Validation

The standard requires a validation plan and refers the reader to Draft IEC 61508 for guidance (*It is not clear whether this refers to all technologies or just E/E/PE).* A safety validation report is also required. Generally the same requirements are required from both standards but Draft IEC 61508 is more specific with regard to the information and processes required from this phase.

Draft EN 954-2 provides a more comprehensive commentary on the validation process for safety-related parts of control systems which is intended to determine compliance for each part with a safety requirements specification derived from EN 954-1.

2.1.1.5 Maintenance

There is a difference in the approaches taken by EN 954 and Draft IEC 61508 in this phase. EN 954-1 refers to EN 292-2 which calls for maintenance to be documented whilst Draft IEC 61508 calls for a procedure to be developed.

Table 1 Summary of requirements

Cat.	Basic Safety Principles	Well Tried Components	Well Tried Safety Principles	Fault Detection	Comments
B	❼			none	
1	❼	❼	❼	none	Category 1 has a lower failure to danger than category B.
2	❼		❼	• at machine start up • prior to initiation of hazard • periodically (if required)	• The check may be manual or automatic • The occurrence of a fault may lead to the loss of the safety function between the checking intervals, the loss of the safety function shall be detected by the check. It is assumed that the requirement is specified as the check undertaken prior to the initiation of the hazard it is possible for the safety function to be lost whilst the hazard exists.
3	❼		❼	• at or before the next demand upon the safety functions	• The safety function is maintained in the presence of a single fault. • Not all faults will be detected and accumulation of faults may cause the loss of the safety function • Under fault conditions the system may issue an unintended output which may lead to a hazardous situation
4	❼		❼	• at or before the next demand upon the safety function	• The safety function is maintained in the presence of a single fault. • Not all faults will be capable of detection but the accumulation of faults shall not cause the loss of the safety function.

2.1.2 Draft 954-2 (Safety of machinery - Safety-related parts of control systems: Validation).

2.1.2.1 Introduction

Draft 954-2 specifies the validation process, including analysis and testing techniques, which may be applied to the safety functions and categories for the safety-related parts of control systems given in EN 954-1. The introductory notes make it clear that the safety requirements can be validated by any combination of analysis and testing, but advises that analysis should be performed in parallel with the design process.

The draft standard describes a validation process, planning and documentation requirements, and methods applicable to the validation of categories specified in EN 954-1. The requirements and conditions for a range of control system technologies are provided in five informative annexes - annex E deals with electronic/programmable electronic systems. Validation techniques for environmental and maintenance provisions are also described.

Draft IEC 61508 is not called up as a normative reference by Draft 954-2, although it is referred to in guidance notes dealing with documentation relating to software and the validation requirements for categories wherever programmable electronic systems may need to be considered. Also, indirect reference is made to the quantitative analysis techniques described in Draft IEC 61508 through guidance provided on this subject in annex E of EN 954-1.

2.1.2.2 Validation Process

Draft 954-2 defines validation as a means by which the safety related parts of a control system can be determined to conform (*or not conform)* to their specification. In particular, it is assumed that validation should demonstrate that each safety-related part meets the requirements of EN 954-1 with respect to the specified safety characteristics for that part (in accordance with the design rationale) and the selected category.

The draft standard calls for the validation process to be executed against a pre-defined plan which identifies and describes the analysis/tests involved for the specified safety functions and categories. It also requires the process to be documented and records to be kept which indicate the extent of compliance achieved.

The validation process proposed by Draft 954-2 is as follows:

Step 1. Validation plan
Prior to starting the validation process a 'plan' shall be produced which outlines the strategy and describes the requirements for specified safety functions and their categories.

Step 2. Analysis (see Notes 1 and 2)

Validation by analysis requires examination of documentation which fully describes the design considerations, including specified safety functions in terms of their assigned performance category, arising from the general strategy for design. This may include details of 'well-tried' components, 'well-tried' safety principles, checking procedures, etc. using the informative guidance provided in annexes A to E, as necessary. The standard accepts that analysis of the deterministic arguments to support the use of complex safety-related control systems requires use of the information from other sources, including Draft IEC 61508 for PE safety-related systems.

Step 3. Testing (see Notes 3 and 4)

The draft standard states that when validation by analysis is not sufficient to demonstrate that the safety functions satisfy their safety requirements then testing should be carried out in order to complete the validation exercise. These tests should be performed in a systematic manner by producing a test plan and implementing the tests either manually or automatically.

Step 4. Validation record (see Note 5)

The draft standard requires that validation by analysis and testing should be recorded so that the overall validation process for a machine's safety-related control system is both fully traceable and auditable. This final validation record should cross-reference to all other forms of documentation which, therefore, need to be properly identified.

Note: 1. The guidance for electronic/programmable electronic systems at annex E is incomplete and does not include information on 'well-tried' components which may exclude the use of this technology in category 1 applications.

2. Clause 8.3 of Draft 954-2 describes the validation of category specifications and correlates these to Draft IEC 61508 as:

Category B not applicable
Category 1 not applicable
Category 2 equivalent to SIL 1
Category 3 equivalent to SIL 2
Category 4 equivalent to SIL 3

This guidance is not supplemented by criteria which supports the assignment of these relationships and, in practice, it is unlikely that any such scheme can be fully justified without taking the risk reduction factors associated with a safety function into account as required by Draft IEC 61508. *(Therefore, in the authors opinion, this information is not useful for machinery designers, manufacturers, etc. since it may be misinterpreted with regard to the overall safety of a machine's E/PE control system.)*

3. Draft 954-2 does not assist users of the standard in determining when validation by analysis is insufficient to demonstrate that the safety functions satisfy their safety requirements and that testing should be carried out to complete the validation exercise.

4. Automatically applied tests may be made using computer-aided test (CAT) equipment, computer-aided software engineering (CASE) tools, etc. However, there is no guidance on what measures should be taken to

ensure that this test equipment does not become the cause of apparent defects due to inherent faults in the design of its hardware or software elements.

5. The validation process described in the draft standard is considered to have a significant normative requirement for documentation to be produced by the 'designer' of the safety-related control system so that the extent of compliance to EN 954-1 can be properly evaluated. The documentation aspects of Draft IEC 61508 have, in the past, received criticism because of concern that this may be a significant burden upon dutyholders and, consequently, it may be necessary to review this aspect of the validation scheme recommended by draft 954-2.

2.2 Draft IEC 61508 (Functional safety of electrical/electronic/ programmable electronic safety-related systems).

Draft IEC 61508 is primarily concerned with safety-related control systems which incorporate electrical/electronic/programmable electronic (E/E/PE) devices. It does, however, lay down a framework which may be applicable to safety-related systems irrespective of the technology on which those systems are based. It is intended for application across a wide range of industries (eg. process, manufacturing, transportation and medical).

The standard is aimed at the achievement of functional safety (that is the ability to carry out safety-related functions correctly) rather than primary safety (such as protection against electric shock). The starting point for the standard is that there is, at least, an outline design for a process or machine and that there is a need to reduce the risks associated with the operation of the process or machine to a tolerable level. This risk reduction is achieved by employing safety-related systems which are seen as being added to the basic equipment or process (which is referred to as the “Equipment Under Control” (EUC)).

The methodology is first to identify the hazards and risks associated with the EUC (without the safety-related systems in place). If any of the risks are considered to be intolerable then the risk reduction necessary to achieve an acceptable level of safety must be evaluated. The safety-related functions intended to achieve the necessary risk reduction are then specified. Associated with each safety-related function is a “Safety Integrity Level” (SIL). This is a quantitative measure of the probability of failure to carry out the safety-function as required. 4 SILs are defined in the standard, each level covering a decade range of probability.

Having specified the safety functions it is then necessary to decide which functions will be implemented by systems using E/E/PE technology, which will use other (eg. hydraulic) technology and which functions will be implemented by “external risk reduction facilities”.
Those functions which are to be implemented using E/E/PE technology are then allocated to specific E/E/PE based safety related systems. Each of these systems is allocated a SIL target based on the highest safety integrity requirement of the safety functions allocated to that system.

The SIL target for each E/E/PE safety-related system leads to a set of recommendations, both for hardware and software elements of the system. The recommendations address both the avoidance of failures (by the adoption of certain

procedures and methods) and the control of failures (by the use of certain design techniques). The premise of the standard is that adoption of the recommended measures and techniques will lead to failure probabilities commensurate with the specified SIL.

The above process is illustrated in Figure 1. Examples of hazards, safety functions and safety-related systems which may be applicable to machinery are given in Table 2.

The requirements of the standard are specified in a framework termed the “safety lifecycle”. This divides the activities considered necessary for the achievement of functional safety into a number of phases. Each phase has specified requirements and defined sets of inputs and outputs. The safety lifecycle encompasses the entire life of the system, from initial concept through to de-commissioning. Much emphasis is placed on the provision of documentation. In all, a total of some 49 different documents are required (in the case of a PE-based safety-related system). The documents are intended to transfer information through the phases of the lifecycle and also to provide information for verification, validation and assessment activities.

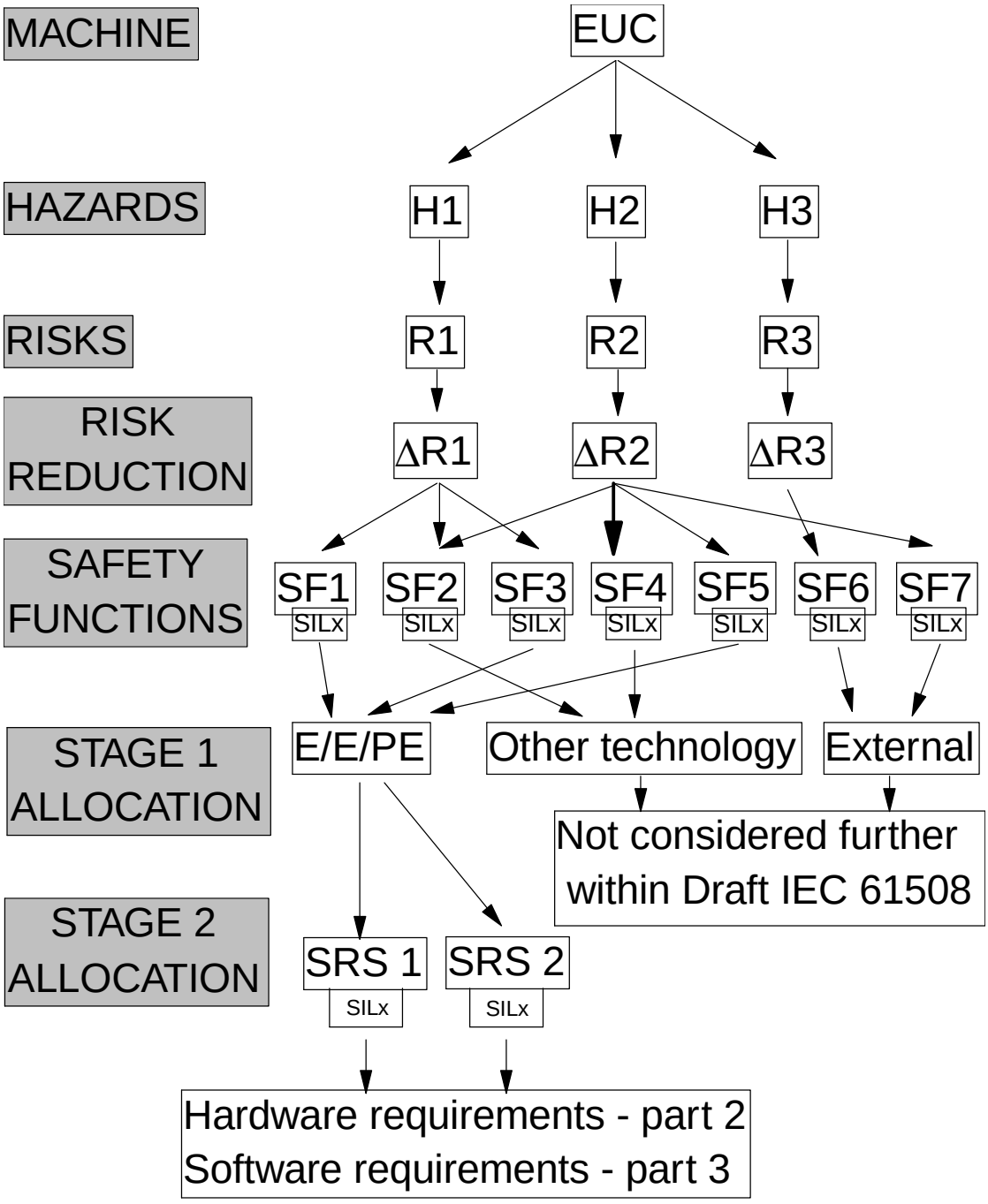


Figure 1 Draft IEC 61508

Hazards

- Contact with dangerous moving parts
- Electric shock
- Physical stability
- Break-up of machine
- Falling or ejected objects
- Surfaces, edges & angles
- Extreme surface temperatures
- Fire/explosion
- Noise/vibration
- Emissions of radiation, dust, gases, etc.
- others

Overall safety functions

- Prevent contact with dangerous moving parts during normal operation
- Prevent contact with dangerous moving parts during set up
- Prevent contact with dangerous moving parts during maintenance
- Prevent contact with live electrical conductors
- Prevention of unexpected start-up
- Emergency stop
- others

E/E/PES safety-related systems

- PLC control of guard interlocks
- PLC control of crawl speed
- Hard-wire control of interlocks
- Crawl speed monitor
- Light curtain control
- Control of motor drives
- others

Other technology safety-related systems

- Fixed guard
- Mechanical braking
- others

External risk reduction factors

- Instructions/training
- Limitation of access
- others ...

Table 2: Draft IEC 61508 concepts that may be applied to machinery

3. **IDEALISED REQUIREMENTS**

A quantifiable measure of determining a control system's safety integrity is desirable because it allows direct comparisons to be made between systems, assuming a common set of assumptions. Unfortunately such a measure can be difficult to estimate so it would be preferable to be able to move from a qualitative assessment of the safety requirements for a control system to a quantitative value of safety integrity. A risk graph or look-up table would be the ideal way of carrying out this process but it could only work if:

(i) control system products were specified in terms of their safety integrity (both complete and modular based solutions), see Note 1.

(ii) examples of "well-tried" or traditional (usually electromechanical based) circuits were available that were specified in terms of safety integrity.

(iii) examples were given on how to calculate safety integrity for new (modular) designs.

(iv) a mechanism was developed for calculating the overall safety integrity level from component parts operating in series and/or parallel.

Note 1: It is assumed that complete control systems could be obtained from one supplier, in which case it would be the responsibility of that supplier to specify the safety integrity. Alternatively, the control system could be a combination of modules (a module here includes a hardwired circuit) where the safety integrity would be specified by each of the module suppliers.

The specification for the safety integrity would describe the limitations of any in-built diagnostic system and include any requirements for proof checking/maintenance intervals. This specification would also recommend configurations or operational parameters that would enable it to achieve a particular safety integrity level.

The system designer would then analyze the combination of modules that comprise the system and using the mechanism mentioned in (iv) above, calculate the overall safety integrity level for the safety function.

4. DEFICIENCIES/DIFFICULTIES WITH EXISTING STANDARDS

4.1 EN954-1

4.1.1 Selection of category

The development of the category definitions within EN 954-1 would appear to have been driven by the underlying presumption that safety integrity could be linked to the fault behaviour of the system. This is reflected in the risk graph (EN 954-1, Annex B) which indicates that those categories with greater fault detection and fault tolerance

are preferred for application where the consequences (severity of injury) are greater and exposure times are greater. The difficulty with this concept is that other factors, such as component reliability, can play a large, perhaps major, part in determining safety integrity with the result that fault handling characteristics alone may not be a suitable indicator of safety integrity. For example, a system which achieves its safety integrity by the use of simple, but highly reliable mechanical linkages may have no inherent fault detection or fault tolerance and as such may be thought of as belonging to category B or category 1. However, the likely failure rate of the system may be so low, owing to its inherent reliability, that it achieves a high level of safety integrity and it is suitable for application where high levels of risk reduction are required (e.g. a linkage in a power press mechanical guard).

This has been recognized in EN 954-1 where it is stated (Annex B) that “component reliability, the technology used in the particular application can indicate a deviation from the expected choice of category”.

This has lead to the rather confusing situation that whilst the theoretical choice of category may be related to risk, the most appropriate category, taking all factors into account, may be different. The EN 954-1 category selection process would appear to be to first identify the theoretical, or “reference” category on the basis of risk (by use of the risk graph), then to modify the selection of category according to component reliability, technology used, etc. The second stage of this process is largely empirical; and little guidance is given within the standard. As a result category selection is likely to suffer from either blind adoption of the risk graph, without reference to the modifying factors, or be so subjective in nature that any link with safety integrity is at best tenuous.

4.1.2 Application of the standard

On a point of presentation, it is considered difficult to extract the normative requirements of EN 954-1. For example, some of the requirements are hidden within lengthy clauses (e.g. the requirement to state reasons for deviating from preferred category which is contained within Annex B.1). With specific regard to programmable electronic systems there is an informative reference (within Table 1) to Draft IEC 61508. If taken at face value, this implies that all Draft IEC 61508 requirements may be informative to
EN 954-1.

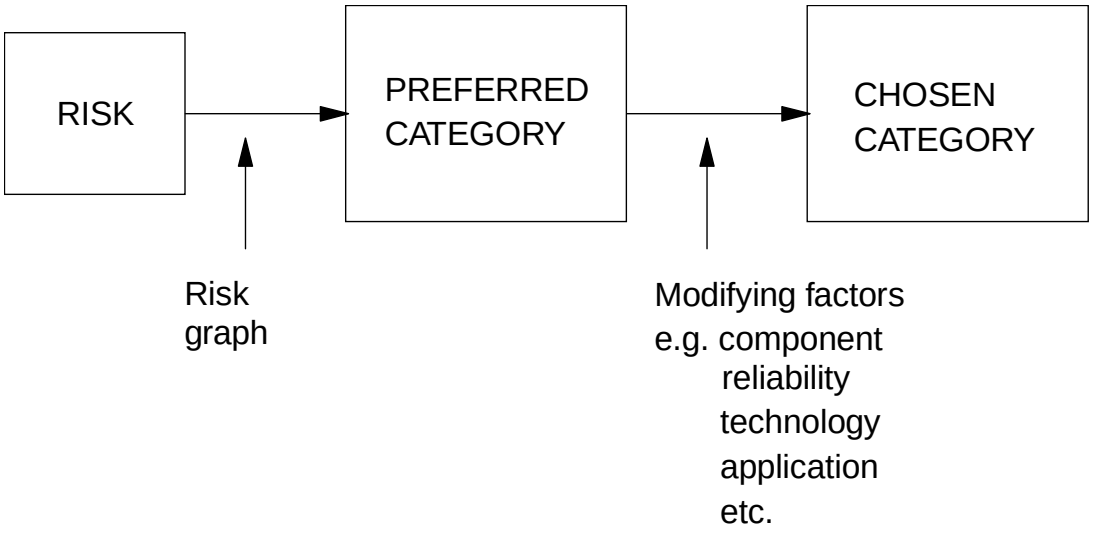


Figure 2: EN 954-1 Category selection process

4.2 Draft IEC 61508

4.2.1 Complexity

The comprehensive nature of Draft IEC 61508 has resulted in what is seen by the machinery sector as an extremely complex and difficult to understand standard.

4.2.2 Terminology & culture

Much of the terminology relates more closely to the process sector which has had significant influence in the development of Draft IEC 61508. In particular, it is considered that the following terms are not fully understood by the machinery sector:

- Proof checking/testing
- External risk reduction facilities
- Safety Integrity Level
- Safety Lifecycle
- Level of safety
- Demand mode/continuous mode of operation
- Total combination of systems
- Verification
- Equipment under control (EUC) risk
- Safety requirements allocation

4.2.3 System considerations (allocation of responsibilities)

The overall safety lifecycle described by Draft 61508 covers all phases of an equipment's life from concept through to decommissioning. Very rarely would one party have responsibility across the entire lifecycle. It is considered that there is a need to delineate responsibilities. This is particularly so in the case of manufacturers who are producing machines or safety components for use in a variety of applications where it may not be practical for the manufacturer to undertake a complete hazard and risk analysis and identify suitable safety functions for all applications at an early stage in the safety lifecycle. In such cases the emphasis must be on the manufacturers to supply sufficient and suitable information (including the Safety Integrity Level) so that users can take proper account of the equipment's performance characteristics in the final application.

4.2.4 Documentation

The extensive documentation requirements of Draft IEC 61508 are seen by the machinery sector to be excessively burdensome.

4.2.5 Architectures

The existing draft of IEC 61508, part 2 does not fully address control system architectures appropriate for application to machinery.

4.2.6 Measures and techniques

Many of the traditionally accepted measures and techniques used in the machinery sector are not included within the present draft of IEC 61508. Many of these measures and techniques have been developed to protect against failures resulting from intentional mis-use or defeat. It is considered that these elements of systematic safety integrity are not adequately addressed by the current draft of IEC 61508.

4.3 Mapping of Category to Safety Integrity Level

Safety Integrity (from Draft IEC 61508) is defined as:
"Probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time".

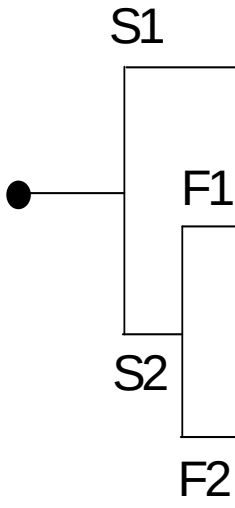
A Category (from EN954-1) is defined as:
"Classification of the safety-related parts of a control system in respect of their resistance to faults and their subsequent behaviour in the fault condition, and which is achieved by the structural arrangements of the parts and/or by their reliability".

Safety integrity is a measure of a system's ability to perform the required safety function within a stated period of time. The safety integrity calculation (probability of failure on demand) is a function of:

(I) failure rate of the components that comprise the system
(ii) proof test interval
(iii) diagnostic coverage
(iv) common cause failure
(v) structure

Draft IEC 61508 also applies requirements to safety components which are detailed in Annex A (normative) of Part 2. This Annex includes a series of tables, which list requirements of the components for hardware and systematic safety integrity, analogous to the definitions of the categories but include the concepts of proof check interval and diagnostic coverage which do not appear explicitly in EN954-1.

It is important to note that there is an assumption in the probability of failure on demand calculation that having carried out a proof test the system is returned to its original "as new", state. In the machinery sector a machine is often run until the control system breaks or stops functioning; reliance is almost totally based upon the control system's self diagnostics.



Safety Integrity Levels			
Safety Function	Safety related system		
	Contribution of s-r-s to safety function		
	Key	Significant	Low
1	1	-	-
1	1	1	-
2	2	1	-
3	3	2	1
3	3	3	2

S Severity of injury

S1 slight (normally reversible)

S2 serious (normally irreversible) injury including death

F Frequency and/or exposure time to hazard

F1 seldom to quite often and/or exposure time is short

F2 frequent to continuous and/or exposure time is long

P Possibility of avoiding the hazard

P1 possible under specific conditions

P2 scarcely possible

Figure 3 Risk graph for selection of safety integrity levels

The categories of EN954-1 are a function of:

(I) reliability of the components
(ii) structure

where the contribution of these two elements varies with the technology used; it is stated that a single channel of safety-related parts of high reliability in one technology could provide the same or higher resistance to faults as a fault tolerant structure of lower reliability in a different technology.

Generally, the difference between safety integrity levels and the categories is that safety integrity is the probability that the system will fail to provide the safety function within a certain time. It is a quantitative measure of a system's performance. The categories are a statement upon the systems resistance to faults and its behaviour once one or more faults have occurred and it is a qualitative measure of a system's behaviour.

Attempts made to map safety integrity levels to categories have found that this is not possible without fundamental changes to the definitions of those categories. A number of mapping techniques that have been tried are described in Appendix 1. This inability to define a map between integrity levels and categories mainly floundered because the categories do not provide an hierarchical structure to their fault resistance.

5. PROPOSED APPLICATION OF DRAFT IEC 61508 TO MACHINERY SECTOR

5.1 Determination of Safety Integrity Level

It is proposed that a development of the risk graph currently included within EN954-1 (Annex B) could be used for the determination of Safety Integrity Levels. An example of such an approach is given in Figure 3.

With reference to Figure 3, the following observations can be made:

- It is considered that SIL 3 is appropriate for the highest risk applications in machinery. This corresponds to a 10^{-3} probability of dangerous failure per year and therefore aligns with what is commonly regarded (at least within the UK) as the maximum tolerable risk for workers.
- The Safety Integrity Level of the safety function is first determined. It is then necessary to consider the contribution of the particular safety-related system under consideration to the overall SIL of the safety function. For systems which play a key part in implementing the safety function, then the system SIL may be considered to be the same as the function SIL. For systems which fulfill a lesser role it may be possible to relax the SIL requirements. This reflects the apportionment of risk associated with the Draft IEC 61508.

5.2 Architecture design

Draft IEC 61508-6 describes a number of examples of system architectures but only the single controller with single processor and single I/O (1oo1) is likely to be applicable to the machinery sector. Figures 4 and 5 depict typical arrangements for machinery systems; basically a single PE system with a hardwired/electromechanical circuit or electronic guard/monitor in parallel.

For machinery systems it is important that electromechanical examples and tables are produced. Also a mechanism which allows the overall safety integrity level to be calculated from a series and/or parallel combination of components of different safety integrity levels needs to be developed. Finally, example architectures for machinery control systems need to be created.

5.3 Safety Lifecycle

The safety lifecycle (Overall, E/E/PE and Software) as defined by Draft IEC 61508 are considered to be sound and it is not thought that they can be simplified significantly in the general case without danger of omitting key phases. In principle, the lifecycle is thought to be appropriate for the machinery sector.

5.4 Documentation

The documentation requirements of Draft IEC 61508 are extensive and thorough; it addresses complete system designs and encompasses the full lifecycle from conception to de-commissioning. However, a machine usually comprises just one system, the end use of which may not be known by the machine designer and, once sold, control (maintenance) of the machine is often handed over to another party. In addition the manufacturer may have in-house procedures (to ISO 9000) for project management, coding standards, fault reporting and fixing, etc.; some of the documents required by the standard may repeat this work.

The designers and manufacturers of safety components, safety systems or sub-systems (eg. CNC controller, drive controller, etc.) may face an even greater problem because they may not know all the end uses for their equipment.

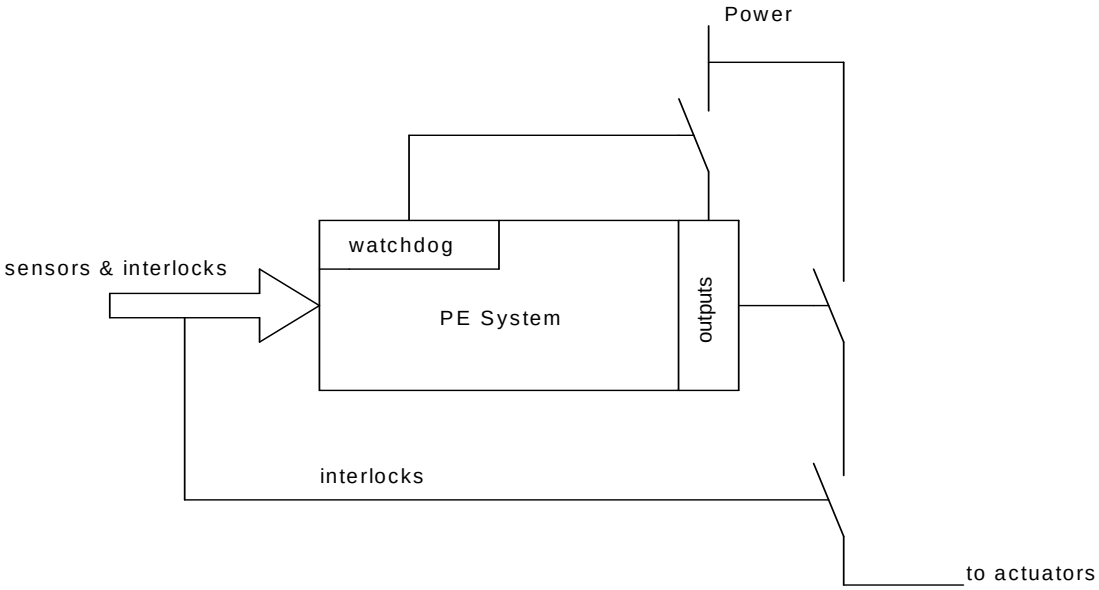


Figure 4: Typical PE system/interlock arrangement

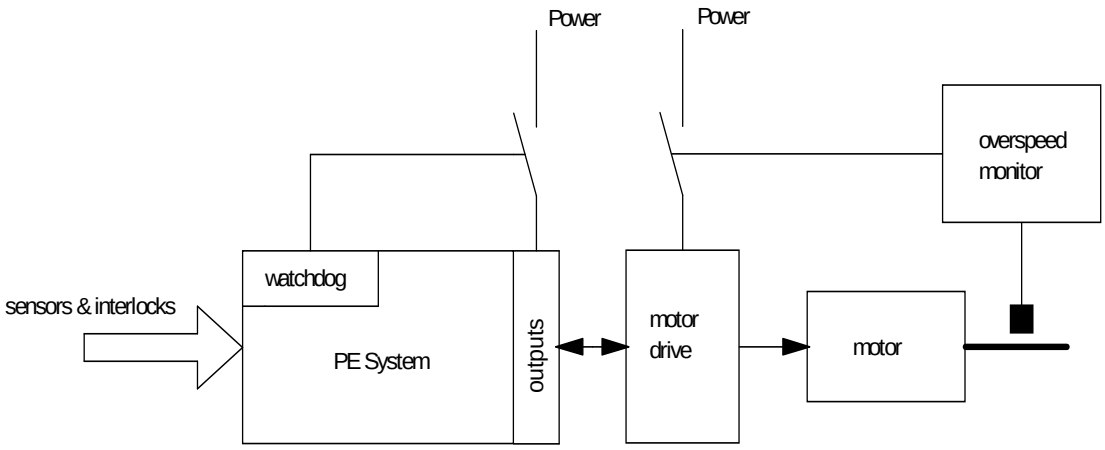


Figure 5: Typical overspeed arrangement

The basic documentation objectives of Draft IEC 61508 could be complied with by machine control system manufacturers but individual documents listed in Part 1 (Annex A) of the standard may not need to be produced because:

(i) only a single E/E/PE controller being developed and not a system.

(ii) usually a product is being produced and in-house procedures should exist to deal with issues such as project management, coding standards, etc.

(iii) maintenance and de-commissioning may not be the responsibility of the control system or machine manufacturers and designers of machinery control systems.

Appendix 4 suggests which documents listed by draft IEC 61508-1 Annex A (informative) should be required of the manufacturers and designers of machinery control systems.

6. **CONCLUSIONS**

1. A linear mapping of the safety integrity levels of Draft IEC 61508 to the categories of EN954-1 could not be established. This was due to the category definitions in EN954-1 not placing any quantifiable requirements regarding the rate of failure of the safety functions.

However, it can be stated that, in a given technology, category 1 is likely to have a higher safety integrity level than category B and category 4 will have the highest safety integrity level.

2. The qualitative approach of EN 954-1 is a desirable one from the machinery sector point of view and could be usefully developed and linked to Draft IEC 61508.

3. The principles of Draft IEC 61508 (safety lifecycle and safety integrity levels) can be applied to E/E/PE control systems in machinery. Draft IEC 61508 could replace EN 954-1 for E/E/PE systems but a qualitative approach leading to a safety integrity level would have to be developed.

If such an approach was developed, there would no longer be the requirement for E/E/PE safety systems to be defined in terms of categories.

4. The non-hierarchical structure of EN 954-1's categories is often misinterpreted into an hierarchical one. This is because the category definitions have to be carefully analysed to understand their full meaning. An informative annex interpreting the categories for different technologies may be useful.

5. Although the categories are difficult to relate to risk, EN954-1, as a document, does provides much useful information into the design strategies for safety and the requirements for safety functions.

6. Draft IEC 61508 covers all phases of an equipment's life from concept through to decommissioning. In the machinery sector, very rarely would one party have responsibility across the entire lifecycle. It is considered that there is a need to delineate responsibilities. This is particularly so in the case of manufacturers who are producing machines or safety components for use in a variety of applications where it may not be practical for the manufacturer to undertake a complete hazard and risk analysis and identify suitable safety functions for all applications at an early stage in the Safety Lifecycle. In such cases the emphasis must be on the manufacturers to supply sufficient and suitable information (including the Safety Integrity Level) so that users can take proper account of the equipment's performance characteristics in the final application.

7. **RECOMMENDATIONS**

We recommend that:

1. The category definitions in EN954-1 be reviewed taking into account the principles for E/E/PE safety-related control systems of Draft IEC 61508. We would suggest that the category definitions should clearly identify the safety performance (or safety integrity) requirements of the safety-related parts of machinery control systems and that such a review should be focused upon reducing the analysis which has to be performed by machinery designers.

2. The qualitative methodology of EN 954-1 should be revised in the proposed amendment so that the design strategy properly considers <u>all</u> the factors which affect risk reduction.

Appendix 1 Mapping schemes

This appendix lists some of the various strategies considered to try and obtain some correlation between EN 954-1's categories and Draft IEC 61508's safety integrity levels. A brief description is given for each approach followed by the main reasons why it was rejected.

1. Examination of EN 954-1's Categories for implied Safety Integrity Levels.

The descriptions of the categories were assessed to determine whether they inferred a particular safety integrity level or levels.

Reason(s) for failure:

(i) Category 4 states that no loss of the safety function can occur, therefore this could equate to safety integrity level 4. However, for categories B to 3 no such assumption could be made.

(ii) Categories B to 3 assume that the system will fail but the category definitions do no state the expected frequency of those failures. Thus it is feasible that a category B system could achieve safety integrity level 4 (when considering all technologies, eg. mechanical links).

2. Fault Resistance

Safety integrity uses component failure rate as a variable within its algorithm and categories use component reliability as a determining factor.

Reason(s) for failure:

(i) The contribution that component reliability provides towards the safety function could vary considerably without affecting the category because EN 954-1 allows it to be offset by the system's structure.

(ii) A safety integrity level assumes a proof check interval.

3. Safety Integrity level achieved though choice of category and application of a set of techniques.

Any category of safety system could be used for a particular safety integrity level provided that some defined set of additional measures were also implemented. These additional measures would be similar to (and would include) those that appear in Draft IEC 61508 parts 2 and 3.

Reason(s) for failure:

(i) Difficulty in deriving these additional measures.
(ii) Masks the underlying problem that categories cannot be easily linked to risk; this approach is effectively re-defining EN 954-1's categories.

4. Risk Graphs

Link the categories of EN 954-1 to a risk level and then link the risk level obtained to a safety integrity level.

Reason(s) for failure:

(i) The definitions for the categories do not address risk.

(ii) These is no hierarchical structure to the categories.

5. E/E/PES Technology Only Approach

EN954-1 id designed to cover a range of technologies. It was investigated whether applying the categories only in terms of E/E/PE technologies could form a structure that could be mapped to safety integrity levels.

Reasons for failure:

(i) Limited in analysis is just E/E/PE technologies did not fundamentally change the way the categories were structured.

6. Descriptive/Quantitative Approach

This approach accepted that categories and safety integrity levels were different and examined the viability that a safety system could be marketed in terms of its reliability (SIL) and its fault behaviour (category).

Reason(s) for failure:

(i) It still required the calculation of safety integrity levels by machine manufacturers and system builders. It did not simplify the process of designing a machinery control system. It did not remove the problem that, theoretically, any category could achieve any safety integrity level.

Appendix 2 - Common requirements & differences

The following are considered to be factors in the comparison of EN 954-1 and Draft IEC 61508.

General

- EN 954-1 does not take the hierarchical system oriented view which is a strong feature of Draft IEC 61508.
- Draft IEC 61508 refers to safety-related systems, which are seen as being wrapped around the “equipment under control” (EUC) to provide a “level of safety”. EN 954-1 refers to “safety related parts of control systems”.
- Draft IEC 61508 requires the production of documentation at each phase of the Safety Lifecycle. The only specific documents required by EN 954-1 are the validation plan and validation report.
- Draft IEC 61508 has a strong formal structure with clearly defined objectives and requirements specified for each phase of the safety lifecycle. EN 954-1 is much less structured and careful examination is necessary to extract the key requirements.

Scope

- EN 954-1 applies to safety related parts of control systems, Regardless of the type of energy used. Draft IEC 61508 is primarily concerned with E/E/PE systems.
- Draft IEC 61508 addresses the entire lifecycle from the concept phase through to decommissioning. EN 954 is restricted to the design phase.
- Draft IEC 61508 takes account of the entire system comprising EUC, safety-related system(s) and external risk reduction facilities. EN 954-1 is only concerned with the “safety related parts of control systems”.

Competence of persons

- Addressed by Draft IEC 61508, not by EN 954-1.

Safety management

- Addressed by Draft IEC 61508, not by EN 954-1.

Concept

- Addressed by Draft IEC 61508, not by EN 954-1.

Hazard & risk analysis

Both standards require:

- carry out a hazard and risk analysis.
- consider elimination of hazards.
- include fault conditions, reasonably foreseeable misuse and human factors
- identify events leading to hazards
- assess frequencies (or probabilities) of hazards events
- identify potential consequences
- assess risk associated with each hazardous event
- identify the necessary risk reduction, for each hazard.

Differences

- Draft IEC 61508 refers to “hazardous events of the EUC”. EN 954-1 refers to time/frequency of exposure to hazard.
- Draft IEC 61508 allows quantitative or qualitative techniques. EN 954-1 emphasis is on qualitative/empirical techniques.
- Draft IEC 61508 requires a “level of safety” (based on the tolerable risk) to be identified for each hazard. EN 954-1 simply refers to the “appropriate risk reduction”.
- Draft IEC 61508 requires details to be documented in “Hazard and Risk Management Description”. EN 954-1 has no documentation requirement.

Specification of safety functions

- Draft IEC 61508 requires specification of all safety functions included in the “total combination of safety-related systems and external risk reduction facilities”. EN 954-1 only requires specification of the safety functions “to be provided in the control system”.
- Draft IEC 61508 requires both a functional description and specification of Safety Integrity Level. EN 954-1 only requires a functional description.
- EN 954-1 lists common safety functions and associated characteristics applicable to machinery.
- Draft IEC 61508 allows for safety functions to be allocated between the safety-related system sand external risk reduction facilities. EN 954-1 only addresses those safety functions implemented by the “safety-related parts”.

Deviation and specification of performance requirements for control systems

- Draft IEC 61508 specifies a formal process whereby, for each hazard, the necessary risk reduction is derived from the EUC risk and the level of safety. It is then necessary to specify how the level of safety (and associated risk reduction)

will be achieved. This is done by describing what the safety-related systems will do (ie. the safety functions) and with what probability they will do it as required (ie. the safety integrity). At this stage the safety-related systems can take the form of external facilities or control systems (of any technology). Then the individual safety-related systems should be specified, both in terms of functionality and effectiveness (as relating to a specific technology) so that all the safety functions are implemented with the required level of safety integrity (taking into account the total effect of all the designated safety-related systems). It should be noted that the level of effectiveness of the individual safety-related systems is also measured by the parameter "safety integrity". Draft IEC 61508 requires that this process of deriving the performance requirements for individual safety related systems has to be documented in a "Safety Requirements Allocation Description".

- EN 954-1 requires that the measures for risk reduction by control means should be "decided" and specified in terms of functionality and category. the methodology to translate risk reduction (associated with particularly hazards) to performance requirements of safety related parts of control systems is not specified.

- Draft IEC 61508 requires that the "effectiveness" of the safety-related control systems be classified according to "safety integrity". Safety integrity is a quantified measure of the effectiveness of a safety-related control system and encompasses hardware reliability as well as control and avoidance of failures due to systematic faults.

- EN 954-1 requires that safety related parts of control system s be categorised according to resistance to faults. The performance measures associated with the categories are a description of measures taken to avoid or control failures and are not quantified.

- Draft IEC 61508 requires that overall safety functions and safety integrity requirements are documented in an "Overall Safety Requirements Specification". The corresponding requirements for individual E/E/PE safety-related systems are documented in the "E/E/PE Safety Requirements Specifications".

Design

- Both standards require that the design meets the specified safety requirements, but Draft IEC 61508 requires that the design documentation should identify and justify the techniques and measures chosen to achieve the Safety Integrity Level. With Draft IEC 61508, extensive tables of recommended techniques and measures (for both hardware and software) are provided. EN 954-1 simply requires a "list of the design features which provide the design rationale for the category achieved".

- Draft IEC 61508 recommends (under development) specific architectures, EN 954-1 does not address architecture (other than as may be necessary to achieve the fault behaviour according to category).

Behaviour under fault conditions

- Both standards require consideration of behaviour under fault conditions. In Draft IEC 61508, fault requirements depend on safety integrity level, extent of diagnostic coverage, knowledge of component failure modes, testability of components and knowledge of component reliability. In EN 954-1, fault requirements are dictated solely by choice of category.

Diagnostic coverage

- Draft IEC 61508 makes recommendations regarding the level of diagnostic coverage provided by the techniques and measures used to control failures. EN 954-1 similarly accepts that not all faults may be detected. In category 3, the required measures for fault detection are required to be graded according to consequence and probability of failure and technology used. In category 4, the inability to detect certain faults leads to the requirement to show that an accumulation of faults does not lead to loss of the safety function.

Proof checking

- Draft IEC 61508 requires that proof checks be undertaken so that the probability of failure on demand remains within the specified safety integrity level. Proof checking is not addressed by EN 954-1.

Integration

- Integration (software, hardware, modules, sensors, actuators) of E/E/PE systems is addressed by Draft IEC 61508, not by EN 954-1.

Operation & maintenance

- Both standards require information for operation and maintenance.

Validation

- Both standards require validation to demonstrate that the safety functions have been implemented according to specification.

Modification

- Addressed by Draft IEC 61508, not by EN954-1.

Verification

- Required by Draft IEC 61508, not by EN 954-1.

Functional safety assessment

- Required by Draft IEC 61508, not by EN 954-1.

Decommissioning

- Addressed by Draft IEC 61508, not by EN 954-1.

APPENDIX 3 REFERENCES

1. BS EN 954-1 Safety related parts of control systems. Part 1: General principles for design. (June 1997).

2. Draft 954-2 Safety-related parts of control systems. Part 2: Validation. CEN/TC114 - CLC/TC44X - JWG 6 N 544 Revision 11 (November 1997).

PART	REFERENCE	TITLE
Part 1	Version 4.0 (05/12/97)	Draft IEC 61508-1: Functional Safety - Safety-Related Systems - Part 1 General Requirements
Part 2	Version 4.0 (05/12/97)	Draft IEC 61508-2: Functional Safety - Safety-Related Systems - Part 2 Requirements for electrical/electronic/ programmable electronic systems.
Part 3	Version 4.0 (05/12/97)	Draft IEC 61508-3: Functional Safety - Safety-Related Systems - Part 3 Software requirements
Part 4	Version 4.0 (05/12/97)	Draft IEC 61508-4: Functional Safety - Safety-Related Systems - Part 4 Definitions and abbreviations.
Part 5	Version 4.0 (05/12/97)	Draft IEC 61508-5: Functional Safety - Safety-Related Systems - Part 5 Examples of methods for the determination of safety integrity levels.
Part 6	Version 4.0 (05/12/97)	Draft IEC 61508-6: Functional Safety - Safety-Related Systems - Part 6 Guidelines on the application of Parts 2 and 3
Part 7	Version 4 (05/12/97)	Draft IEC 61508-7: Functional Safety - Safety-Related Systems - Part 7 Overview of techniques and measures.

APPENDIX 4: DOCUMENTATION REQUIREMENTS FOR MACHINE CONTROL SYSTEMS

TABLE 4A: DOCUMENTS RELATED TO THE OVERALL SAFETY LIFECYCLE		Comments with regard to machinery based control systems
OVERALL SAFETY LIFECYCLE PHASE	**DOCUMENTS**	
Concept	• Description; {Overall Concept}	This depends upon whether the manufacturer of the control system is also responsible for producing the machine as a whole, including all safety aspects (ie. supplying a fully enclosed machine). Generally the manufacturer's knowledge of the overall concept of the machine may be severely limited and would not be able to produce this document
Overall Scope Definition	• Description; {Overall Scope Definition}	Same comments as for Concept
Hazard and Risk Analysis	• Description; {Hazard and Risk Management	Should be produced
Overall Safety Requirements	• Specification; {Overall Safety Requirements} comprising; {Overall Safety Functions & Overall Safety Integrity}	Should be produced
Safety Requirements Allocation	• Description {Safety Requirements Allocation}	Should be produced
Overall Operation and Maintenance Planning	• Plan; {Overall Operation and Maintenance}	The manufacturer may not be responsible for these two phases, the best that may be achievable is a "user manual" detailing the requirements. This document is unlikely to be required.
Overall Validation Planning	• Plan; {Overall Safety Validation}	Should be produced
Overall Installation and Commissioning Planning	• Plan; {Overall Installation}; • Plan; {Overall Commissioning}	The manufacturer may not be responsible for these phases This document is unlikely to be required
Realisation	• Realisation of E/E/PE safety-related systems	See tables 4B and 4C of this Appendix
Overall Installation and Commissioning	• Report; {Overall Installation} • Report; {Overall Commissioning}	Unlikely to be required
Overall Safety Validation	• Report; {Overall Safety Validation}	Should be produced
Overall Operation and Maintenance	• Log; {Overall Operation and Maintenance}	Unlikely to be required
Overall Modification and Retrofit	• Request; {Overall Modification}	These should be in-house procedures (eg. ISO 9000)

TABLE 4A: DOCUMENTS RELATED TO THE OVERALL SAFETY LIFECYCLE		Comments with regard to machinery based control systems
OVERALL SAFETY LIFECYCLE PHASE	**DOCUMENTS**	
	• Report; {Overall Modification & Retrofit Impact Analysis} • Log; {Overall Modification & Retrofit}	which apply across all products
Decommissioning	• Report; {Overall Decommissioning Impact Analysis} • Plan; {Overall Decommissioning} • Log; {Overall Decommissioning} • Report; {Overall Decommissioning}	Generally these will not be required.
Concerning all Phases	• Plan; {Safety} • Plan; {Verification} • Report; {Verification} • Plan; {Functional Safety Assessment} • Report; {Functional Safety Assessment}	These also should be in-house procedures

TABLE 4B: DOCUMENTS RELATED TO THE E/E/PE SAFETY LIFECYCLE		**Comments with regard to machinery based control systems**
E/E/PE SAFETY LIFECYCLE PHASE	**DOCUMENT**	
E/E/PE Safety Requirements	• Specification; {E/E/PE Safety Requirements} comprising; {E/E/PE Safety Functions & E/E/PE Safety Integrity	This is likely to have been completed as part of the overall safety requirements
E/E/PE Validation Planning	• Plan; {E/E/PE Safety Validation}	some comment as above

E/E/PE Design and Development
 	
E/E/PE Architecture
	• Description {E/E/PE Architecture Design} comprising
	  • Hardware Architecture
	  • Software Architecture
	• Specification {PE Integration Tests}
		should be produced

TABLE 4B: DOCUMENTS RELATED TO THE E/E/PE SAFETY LIFECYCLE		Comments with regard to machinery based control systems
E/E/PE SAFETY LIFECYCLE PHASE	**DOCUMENT**	
Hardware Architecture	• Specification {Integration Tests of PE and non PE Hardware} • Description; {Architecture Design Hardware} • Specification; {Hardware Architecture Integration Tests}	Unlikely to be required because the control system will usually be a single system and E/E/PE Architecture documents would have already detailed the information
Hardware Module Design	• Specification; {Hardware modules design} • Specifications; {Hardware modules Tests}	should be produced
Component Construction and/or Procurement	• Hardware Modules • Report; {Hardware Module Test}	should be produced
PE Integration	• Report; {Integration test of software onto PE hardware}	should be produced
E/E/PE Integration	• Report; {Integration test of PE and other hardware}	should be produced
E/E/PE Operation and Maintenance Procedures	• Instruction {User} • Instruction {Operation and Maintenance}	should be produced (within the context of the equipment being developed}
E/E/PE Safety Validation	• Report {E/E/PE Safety Validation}	should be produced
E/E/Modification	• Instruction; {E/E/PE Modification Procedures} • Request; {E/E/PE Modification} • Report; {E/E/PE Modification Impact Analysis} • Log; {E/E/PE Modification}	These should be in house-procedures (eg. ISO 9000) which apply across all products
Concerning all Phases	• Plan; {E/E/PE Safety} • Plan; {E/E/PE Verification} • Report; {E/E/PE Verification} • Plan; {E/E/PE Functional Safety Assessment}	These also should be in-house procedures

TABLE 4B: DOCUMENTS RELATED TO THE E/E/PE SAFETY LIFECYCLE		Comments with regard to machinery based control systems
E/E/PE SAFETY LIFECYCLE PHASE	**DOCUMENT**	
	• Report; {E/E/PE Functional Safety Assessment}	

TABLE 4C: DOCUMENTS RELATED TO THE SOFTWARE SAFETY LIFECYCLE		Comments with regard to machinery based control systems
SOFTWARE SAFETY LIFECYCLE PHASE	**DOCUMENT**	
Software Safety Requirements	• Specification; {Software Safety requirements} comprising; {Software Safety Functions & Software Safety Integrity	This is likely to have been completed as part of the overall safety requirements
Software Validation Planning	• Plan; {Software Safety Validation}	some comment as above
Software Design and Development Software Architecture Software System Design	• Description {Software Architecture Design} Specification; {Software Architecture Integration Tests} • Specification; (PE and Software Integration Tests} • Instruction; {Development Tools and Coding Manual}	Software architecture description should have already been completed. Software architecture tests unlikely to be required (assuming single system). Development tools and coding manual should be part of in-house procedures.
Module Design	• Specification; {Software System Design} • Specification; {Software System Integration Tests}	Unlikely to be required (assuming single system)

TABLE 4C: DOCUMENTS RELATED TO THE SOFTWARE SAFETY LIFECYCLE		Comments with regard to machinery based control systems
SOFTWARE SAFETY LIFECYCLE PHASE	**DOCUMENT**	
Coding	• Specification; {Software Module Design} • Specification; {Software Module Tests}	Should be produced
Module Testing	• List; {Source Code} • Report; {Software Module Test} • Report; {Code Review}	Should be produced
Software Integration	• Report; {Software Module Test}	Not required as already carried out
	• Report {Software module Integration Test} • Report; {Software System Integration Test} • Report; {Software Architecture Integration Test}	Only software module integration test should be required (assuming single system)
PE Integration	• Report; {PE & Software Integration Test}	should be produced
Software Operation and Maintenance Procedures	• Instruction {User} • Instruction {Operation and Maintenance}	should be produced
Software Safety Validation	• Report; {Software Safety Validation}	should be produced (within the context of the equipment being developed)
Software Modification	• Instruction; {Software Modification Procedures} • Request; {Software Modification} • Report; {Software Modification Impact • Analysis} • Log; {Software Modification}	These should be in-house procedures (eg. ISO 9000) which apply across all products.
Concerning all Phases	• Plan; {Software Safety}; • Plan; {Software Verification} • Report; {Software Verification} • Plan; {Software Functional Safety Assessment} • Report; {Software Functional Safety Assessment}	These also should be in-house procedures