S T S A R C E S

Standards for Safety Related Complex Electronic Systems

Annex 13

Applicability of IEC 61508 & EN 954

Task 3: Design process Analysis

Final Report of WP4

S Frost

HEALTH & SAFETY EXECUTIVE

HSE

European Project STSARCES
Contract SMT 4CT97-2191

Introduction

Task 3 of the Divergences Study for Work-package 4 (WP4) of the STSARCES Project (STandards for SAfety-Related Complex Electronic Systems) was to establish whether the guidance on design contained in the EN 954[1] and IEC 61508[2] standards is representative of the approaches followed by designers and others in the machinery sector. This involved consultation with a limited number of UK machinery designers to review the machinery design and development process that have been evolved in their respective organisations.

This review of machinery design practice was conducted using a checklist/ questionnaire (see Annex 1) developed after analysis of the significant divergences noted in the WP4 Task 1 (Comparison of methodologies) report[3].

Objectives

The objectives assigned for Task 3 were as follows:

1) Examine existing design practices in the machinery sector;

2) Compare these design practices with the provisions of relevant EU Directives with respect to risk-based approaches in machinery design; and

3) Compare these design practices with the relevant requirements of the draft IEC 61508 and EN 954 standards which place responsibilities upon the role of machinery design and management.

Organisations consulted and information gathering

The following organisations, which comprise machinery manufacturers, control systems integrators and machinery users, were consulted during completion of this analysis either by site visit or telephone contact:

600 Lathe Co Ltd

Edwards Pearson Ltd

EJA Engineering Group plc

General Motors

GE Fanuc Automation (UK) Ltd

Giddings & Lewis Cross Hüller Ltd

Machine Tools Trade Association

Mersey Docks and Harbour Co Ltd

Pilz Automation Technology UK Ltd

RR Donnelley (UK) Ltd

At each contact the questionnaire at Annex 1 was used as the basis for assessment of their machinery and/or control system design process. The users contacted provided feedback on those aspects of the design and development lifecycle where they could contribute towards the overall effectiveness of the process.

It was originally envisaged that this questionnaire could be used as a means of receiving and recording feedback. This approach was adapted during initial contacts when it was apparent that it was better employed as a means for focusing the discussions on machinery design and safety-related control systems.

Main findings

1. Conceptual design activity was always performed during the development phases leading to the introduction of a new range of machinery. The extent to which this activity was carried out was dependent upon the level of new functions or characteristics to be performed by a machine design, new legislative provisions, or the introduction of new materials which are to be processed at the machine.

In a number of cases it was found that new machine designs were derived from existing machine types. This factor restricted the extent to which conceptual design, including fundamental changes to existing machine types, may be practicable whilst attempting to meet other constraints applied to the development such as project schedules, lead times for tooling, costs, etc.

2. Each machinery manufacturer contacted claimed that a hazard and risk analysis was carried out as part of a machines design and development lifecycle to satisfy current legislative requirements under the Supply of Machinery (Safety) Regulations 1992. However, the effectiveness of these analyses for all modes of operation, including foreseeable fault conditions and misuse, was unclear.

The criteria used to determine the risk reduction required was based on techniques and measures that had been used previously and had a satisfactory safety record in the view of the implementing organisation.

3. This approach that can be best described as ‘proven in use’ or ‘accepted practice’ followed by manufacturers had only limited support from the control systems integrators and safety component manufacturers contacted. These organisations tended to recommend a proactive approach whereby electrotechnical safety solutions should be selected in accordance with the application.

4. A machinery manufacturer contacted had established a reliability and maintainability (R&M) section to review component performance data in terms of either mean time to failure (MTTF) or mean time between failures (MTBF), as appropriate. This information was initially used to assist in component selection and subsequently by the R&M section for compilation of technical files.

This same organisation had attempted to collate feedback on control system defects from customers but claimed that the difficulties in extracting precise details for each incident outweighed any advantages accrued. Similar views were received from other organisations contacted.

5. The machinery and control system designers contacted accepted that hazard and risk analysis was a necessary activity that had to be performed throughout the design. This analyses was largely focused upon the hazards that may occur during normal use where risk estimation based largely upon EN 954-1 was used in conjunction with other standards to determine the depth of measures that needed to implemented to safeguard a machine.

6. The specification of safety functions was, in most cases, combined with the specification of other machinery functions as part of a structured process that typically was performed by a combination of disciplines, such as marketing, design, quality control, after-sales support, etc. This process was generally based upon the principles of safety integration but had been cultured by experience of previous machinery developments whereby manufacturers tended to customise control and safety solutions to specific machine types.

Examples of this practice include application programs for CNC controllers, safety components for access controls, fencing and so on.

7. Large machinery users typically devise their own specifications in order to achieve consistent standards of safety, operability, and availability. In such cases there was evidence to support the involvement of machinery operators and other users in establishing these specifications.

Also, the specifications seen included cross-references to relevant ‘A’ and ‘B’ standards harmonised under the Machinery Directive.

8. The derivation of performance requirements for control systems was taken from standards (EN 60204-1, EN954-1, relevant ‘C’ standards) that had been harmonised under the Machinery Directive. Therefore, control systems were in each case categorised in accordance with the risk graph at Annex B of EN 954-1.

A meeting with a machinery manufacturer revealed a preference for Category 3 safety performance regardless of the other options available. This misuse of the safety performance criteria in EN 954-1 was described as a defence against potential product liability issues.

9. The design and implementation of control system safety functions using software-based subsystems and components were not generally used by the organisations contacted. The role of software was recognised and widely accepted in diagnostic and monitoring as part of back-up functions which can assist in fault finding and maintenance.

Software-based safety functions were considered to be specialised and requirements for reliable operation were described in terms of multi-channel control system architectures. The measures and techniques for software implementation at

machinery, including diagnostic coverage, were more fully understood by control system integrators rather than machinery designers.

10. Details of design and development process described in the questionnaire, namely behaviour under fault conditions, diagnostic coverage and proof testing, were in most cases described as issues that needed to be addressed by the designer rather than as specific factors that should be achieved. This was due to the misinterpretation of these parameters which are not normally used in the machinery sector (e.g. proof testing was mistakenly taken to mean routine checks at safeguards or self checking functions at machine controllers) or referred to by other terminology (e.g. behaviour under fault conditions was not considered since the sector has traditionally achieved safety by stopping a machine in response to single fault conditions).

11. Operational aspects of safety-related control systems, in terms of operation, maintenance and repair, were only partially covered by the 'information for use' provided by the organisations contacted. This information was typically in the form of documentation supplied with a machine, training provided to operators and technicians, development tools for NC controller software, and password protection at operator interfaces.

Component suppliers and control system integrators did not routinely supply maintenance data, such as type and frequency of inspection and test.

12. The approaches examined for modification of safety-related systems ranged from controlled change requests through after-sales contacts and/or authorised distributors through to customer initiated changes by supplying manufacturers approved spares. Despite the existence of these schemes all the manufacturers considered it likely that customers would diagnose and repair with 'similar' replacement components where circumstances required machinery to be available for production.

The measures inspected to control modifications and retrofitting of replacement parts did not adequately evaluate the impact of a modification upon the functional safety of electrical/ electronic/programmable safety-related systems.

13. Verification and validation procedures were applied by all the organisations contacted. These procedures tended to complement quality control activities that were routinely carried out during acceptance and beta testing of new machinery and/or control systems.

Safety-related component and systems, including programmable electronic controllers and devices based upon solid-state electronic logic, tended to be subject to third-party approval and certification as part of the 'CE marking process'. Control system integrators were fully aware of the requirements to control versions of software for operating systems, compilers, and development tools.

14. Functional safety assessments were reported to be applied to new machinery by internal test departments using subsets of the design requirements specification. There was insufficient evidence to suggest that this criteria or the competence of the

test and quality engineers undertaking the assessment was capable, in every case, of providing confidence that the safety performance achieved for a complex machine was commensurate with the target defined in the specification. This was often the result of poorly defined and ambiguous test specifications which only made provision for functional testing on a limited basis.

For machinery developed with a view to manufacturing only a limited number of units (typically not exceeding 50 machines) it was found that third party assessment was likely to be performed. This approach was also an option preferred for smaller machinery manufacturers.

15. Competence of machinery designers and control systems specialists was considered to be an important factor by all the organisations contacted where electrotechnical safety-related systems had been implemented. The approach taken was in all cases based upon a combination of experience, knowledge and skills that were not specifically relevant to safety.

Guidance on existing and emerging safety issues, such as programmable electronic systems, tended to be gathered from a wide range of sources. These included industry associations, relevant standards and publicly available guidance from HSE and other government departments.

Conclusions

All the organisations contacted during completion of Task 3 had well structured design processes for the development of machinery. These processes included a number of common issues related to essential health and safety requirements which underpin the Machinery Directive (89/392/EEC as amended).

The design processes examined included activities which were generally consistent with the safety lifecycle model described in IEC 61508. The extent to which these activities, such as conceptual design and hazard and risk analysis, were carried out was dependent upon the nature of the machine design and similarity with other existing machine types. This approach often meant that risk reduction criteria was not applied at all electrotechnical safety solutions, such as hardwired control system interlocking and isolation, where they had been used previously by an organisation.

The effectiveness of these 'previously used' electrotechnical safety solutions was based upon the designers awareness of similar applications of the safeguard. This means of evaluating safety performance is inadequate and, unsurprisingly, it was found that safety component suppliers and control system integrators considered that greater use of hazard and risk analyses should be made at each application.

These shortcomings in accepting previously used safety solution were, in most cases, offset by the use of relevant standards and third party assessment of machinery and their safety-related control systems. Despite the existence of this 'safety net' this is a matter of concern which needs to be addressed for future developments where more complex safety-related control systems are likely to be implemented.

There was a high level of awareness of harmonised standards due to the current legislative framework for machinery safety. Nonetheless it was evident that misuse and misinterpretation of the requirements of EN 954-1 for safety-related parts of control systems was a common occurrence as discussed in the WP4 Task 1 report[3]. This was noted in the selection of safety performance categories and the implementation of EN 954-1 for safety-related systems which comprise programmable electronic devices and equipment.

In contrast there was a low level of awareness of the principles of IEC 61508. This was found to be the case at most organisation contacted with the exception of component suppliers and control system integrators with experience of complex electronic and programmable electronic safety-related systems for machinery.

The electrotechnology utilised at safety -related control systems was predominantly electrically based mainly as a result of the accepted practices such as hardwired interlocking that have evolved in the machinery sector. Despite this it was apparent from discussions with machinery designers that the flexibility and performance available through programmable electronic safety solutions were significant factors likely to influence the design of machinery control systems in future developments - for instance, the ability to more closely integrate safety within a machines control system was a concept discussed at a number of contacts.

Although the introduction of programmable electronic safety-related systems was an attractive proposition for many of the organisations contacted, a number of difficulties need to be resolved to ensure that safety performance is properly addressed. These difficulties are primarily associated with the poor quality of data available for components and devices, effective software engineering methods and techniques need to be developed for the sector and competence of personnel involved throughout the overall design lifecycle needs to include a proper awareness of functional safety to complement the skills and knowledge already acquired by many machinery designers.

References

1. EN 954: Safety of machinery - Safety related parts of control systems:
   Part 1. General principles for design. 1996
   Part 2. Validation (DRAFT)
2. IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems:
   Part 1. General requirements. 1998
   Part 2. Requirements for electrical/electronic/programmable electronic safety-related systems (FDIS)
   Part 3. Software requirements. 1998
   Part 4. Definitions and abbreviations. 1998
   Part 5. Examples of methods for the determination of safety integrity levels. 1998
   Part 6: Guidelines on the application of Parts 2 and 3. (FDIS)
   Part 7: Overview of techniques and measures. (FDIS)
3. 'A Study of the Links & Divergences Between Draft IEC 61508 and EN 954' Issue 02 September 1998, STSARCES Project. Eur Ing S J Brown and Eur Ing S Frost, HSE.

ANNEX 1

MACHINERY DESIGNERS/ MANUFACTURERS/ SUPPLIERS QUESTIONNAIRE

MACHINERY DESIGNERS/ MANUFACTURERS/ SUPPLIERS QUESTIONNAIRE:

Functional safety of electrical/ electronic/ programmable electronic (E/E/PE) safety-related control systems

The European Commission has initiated a research project, referred to as STSARCES, to examine the validation aspects of safety-related parts of control systems for machinery with regard to ensuring that modern electronic and programmable electronic technologies are properly applied in the context of safety.

This questionnaire has been prepared by the Health and Safety Executive (HSE) as part of a contribution intended to complete knowledge into the practical applicability to machinery of two standards which deal with safety-related control systems. These standards are BS EN 954-1:1997 'Safety of machinery - Safety-related parts of control systems - Part 1. General principles for design' and IEC 61508 (Draft) 'Functional safety of electrical/electronic/programmable electronic safety-related systems'.

The purpose of this research is to determine the extent to which risk-based techniques and principles described in these standards may be used by machinery designers, manufacturers and suppliers, including vendors of machine control subsystems, in the design and development of machinery. In particular, the questionnaire considers those aspects of machine control systems design which may be relevant to safety provisions arising from the Machinery Directive (89/392/EEC as amended by 91/368/EEC).

The content of the questionnaire is focused upon existing design practices followed by the machinery sector and has been structured against the overall safety lifecycle (Figure 1). This lifecycle model forms a strategy for the design, installation, operation and use of equipment which incorporates safety-related control systems and is recommended by existing and emerging standards in this field.

If any difficulties are experienced with any aspect of this questionnaire please discuss with the HSE contact at the telephone number given below.

Thank you for your co-operation in completing this questionnaire.

Return completed questionnaires to:

Eur Ing Steve Frost
Health & Safety Executive
Directorate of Science & Technology
Electrical & Control Systems Unit
Magdalen House
Stanley Precinct
Bootle, Merseyside L20 3QZ
Tel: 0151-951 4968 Fax: 0151-951 4630

1.0 CONCEPT

1.1 **Conceptual design activity** (Box 1 in Figure 1)

This refers to the initial stage in the overall safety lifecycle of a product. The objective of a conceptual analysis is to develop a level of understanding of the machinery and its operating environment (physical, legislative, etc.) in sufficient detail to enable the other safety lifecycle activities to be carried out.

The successful completion of this activity requires sufficient information to be generated in order to gain a thorough familiarity with the machinery, its required control functions, its operating environment, applicable safety regulations and the likely sources of hazards, including hazards arising from interaction with other items of machinery.

In your opinion, to what extent is this form of 'conceptual' phase undertaken when designing machinery? If this is an explicit stage in the design process followed within your organisation, what information makes up the inputs and outputs (i.e. deliverables for the next stage of the design process) to ensure satisfactory completion?

(Please insert your comments in the space provided below)

2.0 HAZARD & RISK ANALYSIS OF THE EQUIPMENT UNDER CONTROL

2.1 **Hazard & risk analysis** (Box 3 in Figure 1)

A hazard and risk analysis may be used to determine the hazards and hazardous events of the machinery and its control system (under all modes of operation) for all reasonably foreseeable circumstances, including fault conditions and misuse. Any such analysis needs to take into account hazards which can arise from the machining process and the working environment.

In your opinion, to what extent is a hazard and risk analysis performed during the design of machinery? If such an analysis is performed, what criteria is used to determine the level of risk reduction required to ensure safety? Are the techniques best described as qualitative, quantitative or a combination of both? For quantitative assessments what source of component failure or reliability data is used?

(Please insert your comments in the space provided below)

2.2 **Specification of safety functions** (Box 4 in Figure 1)

This aspect of the design/ development process relates to the specification of machinery safety functions which are intended to mitigate against the hazards identified by the hazard and risk analysis. These functions may incorporate safety-related control systems (e.g. electro-sensitive safety systems) , external risk reduction facilities (e.g. the provision of fire extinguishers or pedestrian railings) and other technology safety-related systems (e.g. mechanical guards).

In practice, this specification of safety functions may be derived from actions taken to comply with the Essential Health and Safety Requirements of the Machinery Directive which involves the application of the principles of safety integration:

- eliminate or reduce risks as far as possible (inherently safe machine design and construction);
- take the necessary protection measures in relation to risks that cannot be eliminated; and
- inform users of the residual risks due to any shortcomings of the protection measures adopted, indicate whether any particular training is required and specify any need to provide personal protection equipment.

In your opinion, to what extent is the specification of safety functions at a machine determined from a risk based analysis undertaken during design of the machine? If not, what measures are taken to ensure that the design of a machine will safeguard operators, users etc. against foreseeable hazards which may occur during it's service lifetime?

(Please insert your comments in the space provided below)

2.3 Derivation and specification of performance requirements for control systems (Box 5 in Figure 1)

Emerging and existing standards dealing with the design of machinery control systems describe a formal process whereby, for each hazard, the necessary risk reduction is derived from the risk at the machinery and the level of safety which results in a specification of how the level of safety (and associated risk reduction) will be achieved. This may be done by describing what the machine's safety-related systems will do (i.e. the safety functions) and with what probability they will do it as required (i.e. the safety integrity). At this stage the safety-related systems can take the form of external facilities or control systems (of any technology). 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 machine's safety functions are implemented with the required level of safety integrity (taking into account the total effect of all the designated safety-related systems).

In your opinion, is this approach representative of the machine control systems design philosophy employed by your organisation? If not, what methodology is used to translate risk reduction (associated with particular hazards) to the performance requirements for safety-related parts of machinery control systems? What techniques are used to measure the 'effectiveness' of the safety-related control systems? Would you consider that these measures are categorised to reflect the risks in a hierarchical format? Is this hierarchy described quantitatively or qualitatively?

(Please insert your comments in the space provided below)

3.0 DESIGN & DEVELOPMENT PROCESS

3.1 **Design** (Boxes 9, 10 and 11 in Figure 1)

An overall objective for the design of a machine should be to ensure that it is capable of meeting the specified safety requirements, whereby it is possible to justify the techniques and measures that have been selected to achieve the performance requirements for control systems. Alternatively, it may that a list of the design features is provided along with a design rationale for the performance category achieved.

Development of an appropriate machinery control system architecture (i.e.. the specific configuration of hardware and software elements in a system) which considers the hazards and risks to users, operators, etc. may involve consideration of the following characteristics.

3.1.1 Behaviour under fault conditions[1]

This aspect of the operation of a machinery control system may require assessment of fault requirements which depend upon the assigned safety integrity level, extent of diagnostic coverage, knowledge of component failure modes, testability of components and knowledge of component reliability.

In your organisation, is this form of assessment carried out during machinery design and, if so, what would you consider to be essential factors that dictate the fault requirements, for example, the number of single element faults or the probability of failure which may be tolerated without giving rise to danger?

(Please insert your comments in the space provided below)

Note 1: Faults in a control system can be considered as either detected or undetected. However, the extent to which such conditions effect the safety integrity of a machine are likely to be dependent upon the overall fault tolerance of the control system.

3.1.2 Diagnostic coverage[2]

The level of diagnostic coverage provided by the control system design can be used as a technique to control failures. However, its effectiveness may be limited by the extent to which faults may be detected.

In cases where this measure has been adopted, for example, within programmable electronic safety-related systems, how are the required measures for fault detection graded according to consequence, probability of failure and technology used?

(Please insert your comments in the space provided below)

Note 2: Diagnostic coverage may be defined as the fractional decrease in the probability of a dangerous hardware failure resulting from the operation of automatic diagnostic tests.

3.1.3 Proof testing[3]

A further measure that may be used to control failures is proof testing which requires that functional tests, referred to as proof tests, are undertaken at pre-determined intervals so that an assessment can be made of the probability of failure on demand of critical components and whether the machine's safety-related control systems adhere to specified safety performance criteria.

How is this type of system control measure intended to be applied to machinery designed by your organisation and in what form are recommended proof check intervals brought to the attention of operators, users, etc.?

(Please insert your comments in the space provided below)

Note 3: Proof testing may be defined as a periodic test performed to detect failures in a safety-related system so that, if necessary, the system can be restored to an "as new" condition or as close as is practical to this condition.

3.2 **Control systems integration** (Box 9 in Figure 1)

The objective of the integration phase of a development is to combine and test the machine's E/E/PE safety-related system (comprising software,

hardware, logic solvers, sensors, actuators, etc) as a collection of individual modules and/or subsystems to ensure that their design and performance conforms with their specification, for example, the E/E/PE system integration test specification. The purpose of these tests is to reveal any shortcomings in each E/E/PE safety-related sub-system prior to the their incorporation within the final assembly of the machinery. After satisfactory completion of this stage in the lifecycle, the control system vendor may pass on responsibility for the safety of the equipment to the machine designer/manufacturer

How is design integration managed within your organisation and what, if any, forms of documentation are used to control the activity? Is impact analysis carried out to identify components which may be affected by the results of integration testing? Are any similar forms of testing applied to software components of a machine control system and, if so, what do these tests comprise?

(Please insert your comments in the space provided below)

4.0 OPERATIONAL ASPECTS OF E/E/PE SAFETY-RELATED SYSTEMS

4.1 **Operation, maintenance and repair** (Boxes 6 and 14 in Figure 1)

Many organisations develop a range of procedures to ensure that the specified level of functional safety of a machine's E/E/PE safety-related system can be maintained during operation, maintenance and any subsequent repair work. These procedures may include descriptions of the routine actions which need to be carried out to maintain the "as designed" functional safety of the control system, maintenance procedures for fault diagnoses and repair, procedures for re-validation, and so on.

What information, if any, do you provide with machines to ensure that the functional safety of the control system is not adversely effected during operation and maintenance activities?

(Please insert your comments in the space provided below)

4.2 **Modification & retrofit** (Box 15 in Figure 1)

The primary requirement of any modification to the design of a safety-related system is to ensure that the functional safety of the machine's control system is maintained at an appropriate level of safety performance after corrections, enhancements or adaptations, for example, by retrofitting parts, have been undertaken. This normally requires that any modification or retrofit activity is carried out on a planned basis.

What provisions has your organisation made for modifications and, where applicable, retrofitting exercises, to machinery currently in the process of being manufactured, assembled or recently supplied to a customer? Are any techniques used to evaluate the impact that any modification may have upon the functional safety of a machine's E/E/PE safety-related system? What documentation is established and maintained as part of the modification procedures? Are there any specific measures taken to control the various configurations of software which may arise from any modifications?

(Please insert your comments in the space provided below)

5.0 CONFIRMATION OF SAFETY MEASURES FOR E/E/PE SAFETY-RELATED SYSTEMS

5.1 Verification

This activity requires a systematic examination of information produced during the machinery development process in order to demonstrate, for each phase of the overall safety lifecycle associated with the E/E/PE safety-related control systems, that the requirements have been satisfactorily fulfilled. This may be achieved by, for example, undertaking reviews of the outputs (typically documents) to ensure compliance with the objectives for each lifecycle phase, design reviews, and tests on the designed products.

Does your organisation employ this form of verification process for the safety-related properties of a machine development project? If not, is this type of demonstration required for other purposes to allow, for example, auditing of the design and development process? Describe the types of criteria, tools and techniques that you would expect to be used for verification activities.

(Please insert your comments in the space provided below)

5.2 **Validation** (Boxes 7 & 13 in Figure 1)

Validation comprises the means by which the safety-related aspects of a machine's control system can be determined to conform to the requirements for its intended use. In particular, validation should demonstrate that each safety-related system, or parts of it, meets the provisions of the specified safety characteristics for the E/E/PE safety-related system and any selected performance indicators[4].

What measures are taken in your organisation to ensure that safety-related control systems associated with a machine are adequately validated against the desired specifications? Outline the types of criteria used for machinery validation.

(Please insert your comments in the space provided below)

Note 4: Examples of selected performance indicators include the categories described in BS EN954-1:1997 'Safety of Machinery - Safety related parts of control systems - Part 1. General principles for design' and the safety integrity levels (SILs) described in draft IEC61508 'Functional safety of electrical/electronic/ programmable electronic safety-related systems'.

6.0 SAFETY MANAGEMENT ASPECTS

6.1 Functional safety assessment

A functional safety assessment may be carried out to investigate and produce a conclusive opinion on the level of functional safety achieved by a E/E/PE safety-related control system at a machine. This assessment is normally applied throughout the safety lifecycle where the personnel carrying out the assessment consider relevant activities and their expected outputs.

The assessors must be competent to carry out this type of investigation and have an appropriate degree of independence to ensure that their recommendations are not effected by organisational constraints. This may require the use of an independent person, independent department or independent organisation[5].

Is this type of functional safety assessment employed by your organisation as an essential part of a product development programme? What criteria are used to guide assessors with regard to their independence, the activities they need to consider, and the competence requirements relative to the intended application of the machine? If tools (for example, CAD/CAM systems, compilers, host target systems, etc) are used as part of the design or assessment for any E/E/PE safety-related control system are these subject to the functional safety assessment?

(Please insert your comments in the space provided below)

Note 5: The use of a third-party organisation is a legal requirement for the types of machine listed at Annex IV of The Machinery Directive (89/392/EEC as amended by 91/368/EEC).

6.2 Competence of persons

The successful implementation of a machine's E/E/PE safety-related control system is determined to a large extent by the effective co-ordination of the design and development process and the ability of personnel who work towards the organisations objectives by following pre-defined procedures and systems of work. These procedures and systems of work are determined by the management of functional safety (see 6.3) where the responsibilities placed upon individual members of staff can reflect their competence (often considered as a balance of knowledge, experience and training) in both specialist and non-specialist disciplines.

What guidelines on the competence requirements of those involved in any activity related to E/E/PE safety-related systems are used in your organisation?

(Please insert your comments in the space provided below)

6.3 Management of functional safety

This activity has two main objectives, namely:-

i) to specify the management and technical functions which should take place throughout the entire safety lifecycle in order to achieve the desired functional safety of a machine's E/E/PE safety-related control system; and
ii) to specify the responsibilities of the persons, departments and organisations responsible for each safety lifecycle phase or for activities within each phase.

The implications of functional safety management are wide ranging and are likely to have an impact upon organisational policy and strategy, the safety lifecycle phases that are applied, functional safety assessments, procedures for ensuring that all personnel involved in safety lifecycle activities are competent to carry out their respective tasks, etc.

What forms of functional safety management activities are carried out in your organisation? Does this scheme apply to suppliers providing products or services? How do you measure the overall effectiveness of functional safety management applied to a machine's E/E/PE safety-related system measured (i.e. progress monitoring, added value, accident statistics, etc)?

(Please insert your comments in the space provided below)