Automation and Robotics in Construction XI
D.A. Chamberlain (Editor)
1994 Elsevier Science B.V.

Safety of programmable machinery and the EC directive

S.P.Gaskill

Health and Safety Executive Technology & Health Sciences Division, Magdalen House, Bootle,UK

Abstract

This paper discusses the application of European standards to automated machinery. It aims to guide compliance with the Council Directive[1] of 14 June 1989 on the approximation of the laws of the Member States relating to machinery. This Directive is commonly known as the Machinery Directive. It is enacted in UK Law by The Supply of Machinery (Safety) Regulations 1992[2]

1. INTRODUCTION

Much of today's modern machinery has programmable electronic control. The complexity of such control systems raises questions of safety; it may be very difficult or it may even be impossible to ensure that they will always behave as expected under all foreseeable conditions. Dangerous faults may not only be caused by random hardware failure but also by systematic faults inadvertently designed into the system.

Manufacturing industry in the UK has favoured safeguarding computer controlled machines by preventing access to dangerous parts, so that faults do not lead to danger. There are numerous potential applications, particularly in the construction industry, that cannot be safeguarded in this way, eg because of practicability of guarding portable machinery on site, unauthorised site access by contractors, public, etc.

Therefore, it is necessary for the machine design and its safeguards to prevent faults from causing hazards that lead to an unacceptable risk of injury. This requires a thought through safety strategy that starts with the concept of the machine, at the beginning of the product lifecycle.

From January 1995 machines not undergoing the appropriate conformity assessment and not declared to comply with the essential health and safety requirements of the machinery directive may not be marketed in the European Community.

The directive requires a machine's manufacturer, or the manufacturer's representative in the European community to ensure and guarantee that certain technical documentation, including a technical construction file, is and will remain on his premises for any inspection purposes. It is intended that this documentation demonstrate how the essential safety requirements have been met. As machinery becomes more complex it will become more difficult to demonstrate that it is, indeed, safe.

There are unlimited potential applications for automation in construction. The types of machine, their applications and their relationship with other machines will influence their design and selection of safeguards. European standards, written in support of the machinery directive, guide manufacturers to comply with the safety requirements laid out in the directive.

A strategy for designing complex, programmable, systems with a suitable, high level, of safety was first put forward in 1988 by the Health and Safety executive in its guidance "PES - Programmable Electronic Systems in Safety Related Applications"[3]. IEC SC65A (secretariat) 122 and 123 are addressing this area in their draft standard "Functional safety: safety-related systems"[4]. These documents use a risk based approach to determine a required level of safety and discuss how safety related systems may be used to contribute towards risk reduction.

This paper outlines the requirements of the machinery directive, discusses potential difficulties in validating the safety of complex machinery and introduces strategies for designing safe systems.

2. EUROPEAN LAW

The Machinery Directive/Supply of Machinery (Safety) Regulations 1992

The machinery directive[1] is enacted in UK Law by The Supply of Machinery (Safety) Regulations 1992[2]. The regulations came into force on the 1 January 1993. There is, however, a two year transitional period where manufacturers can either:

- comply with the regulations in full, or;

- comply with the national legislation in force on 31 December 1992 in the member state in which the machine is marketed.

From 1 January 1995 a manufacturer of machinery, or the manufacturer's authorised representative in the Community, must comply with the regulations in full.

2.1 Essential Safety Requirements (ESRs)

The Machinery Directive is a new approach directive. It sets out essential requirements that must be met before products may be put on the market in the European Economic Community. To comply with the directive, machinery must satisfy the essential safety requirements (ESR) set out in Annex 1 of the directive. The ESRs apply to all machinery. They are written in general terms, are wide ranging and take into account potential dangers to operators and to others.

The ESRs are mandatory. However, when taking into account the current state of the art, it may not be possible to meet the objectives set by them. In this case the machinery must be designed and constructed with the purpose of approaching those objectives. The ESRs need to be applied with discernment to take into account the state of the art at the time of construction and of technical and economic requirements.

2.2 Documentation

To comply with the directive the responsible person must either make a declaration of incorporation, if the machine is to be a part of a larger machine, or make a declaration of conformity and affix an EC mark to the machine, see Fig 1.

Certain machines, listed in Annex 4 of the directive, are considered to have particular risks. There are extra requirements for these machines, including assessment for conformity by a notified body. Most automatic machinery will not fall into this category.

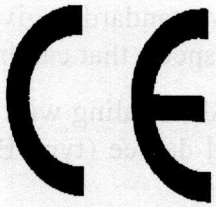

Fig 1

The declaration of incorporation or declaration of conformity is intended to be available to the purchaser and declares that the machinery complies with the relevant ESRs.

Before the responsible person signs the declaration he must ensure and be able to guarantee that technical documentation, including a technical construction file, is and will remain available, for inspection purposes, for a period of 10 years from the date the last unit of relevant machinery is produced. The file is intended to demonstrate how the equipment has been designed to comply with the ESRs. For series manufacture, he must also document the measures that will be implemented to ensure that the machinery remains in conformity with the provisions of the directive.

The above documentation need not permanently exist in a material manner but it must be possible to assemble it and make it available within a period of time commensurate with its importance. It does not have to include detailed plans or any other specific information as regards the sub-assemblies used for the manufacture of the machine unless a knowledge of them is essential for verification of conformity with the ESRs.

The DTI booklet "The Single Market - Machinery Safety"[10] gives further advice on the requirements of the directive.

3. EUROPEAN STANDARDS

There are two ways to conform with the technical measures required by the directive:

a) Interpret the technical measures directly from the ESRs;

b) Use Harmonised European Standards, produced by the European Committee for Standardisation (CEN) and the European Committee for Electrotechnical Standardisation (CENELEC) under a mandate from the European Commission and with a reference placed in the official journal of the European Community.

These standards are written in support of the directive. Compliance with harmonised standards will deem the manufacturer, or representative in the community, to have complied with the relevant ESRs.
There are three types of European standard as defined by CEN :

Type A standards (fundamental safety standards) giving basic concepts, principles for design, and general aspects that can be applied to all machinery;

Type B standards (group safety standards) dealing with one safety aspect (type B1) or one type of safety related device (type B2) that can be used across a wide range of machinery;

Type C standards (machine safety standards) giving detailed safety requirements for a particular machine or group of machines.

3.1 Safety strategy

The standard EN292, Safety of Machinery - Basic Concepts for design[5] & [6], assists designers and manufacturers to interpret the ESRs and it provides a framework of guidance to enable them to produce machines that are safe for their intended use. It also provides a strategy for the selection of safeguards. The strategy may be used by manufacturers designing a machine to comply directly with the ESRs or by standard makers producing subsequent B and C type standards. This strategy is summarised in Fig 2.

The strategy involves:

a) Determine the system boundary: intended use, space limits, time limits etc;

b) Identify and describe, by their nature and consequence, the hazards which may be generated by the machine, in all phases of the life of the machine including hazards generated by human interaction with the machine and hazards generated by foreseeable misuse;

c) Assess the risk for each hazard in terms of probability of the occurrence of an injury or damage to health and the highest foreseeable severity of this injury or damage to health;

d) Ensure that safety is adequate.

The strategy uses three hierarchical methods for selecting safety measures to ensure adequate safety:

e) risk reduction by design, avoiding or reducing as many of the hazards as possible by suitable choice of design features;

f) safeguarding, (guards or safety devices used to protect against hazards which cannot reasonably be avoided or sufficiently limited by design);

g) information for use (this should include information regarding residual risks that cannot be eliminated or sufficiently reduced by design and against which safeguarding is not - or not totally - effective).

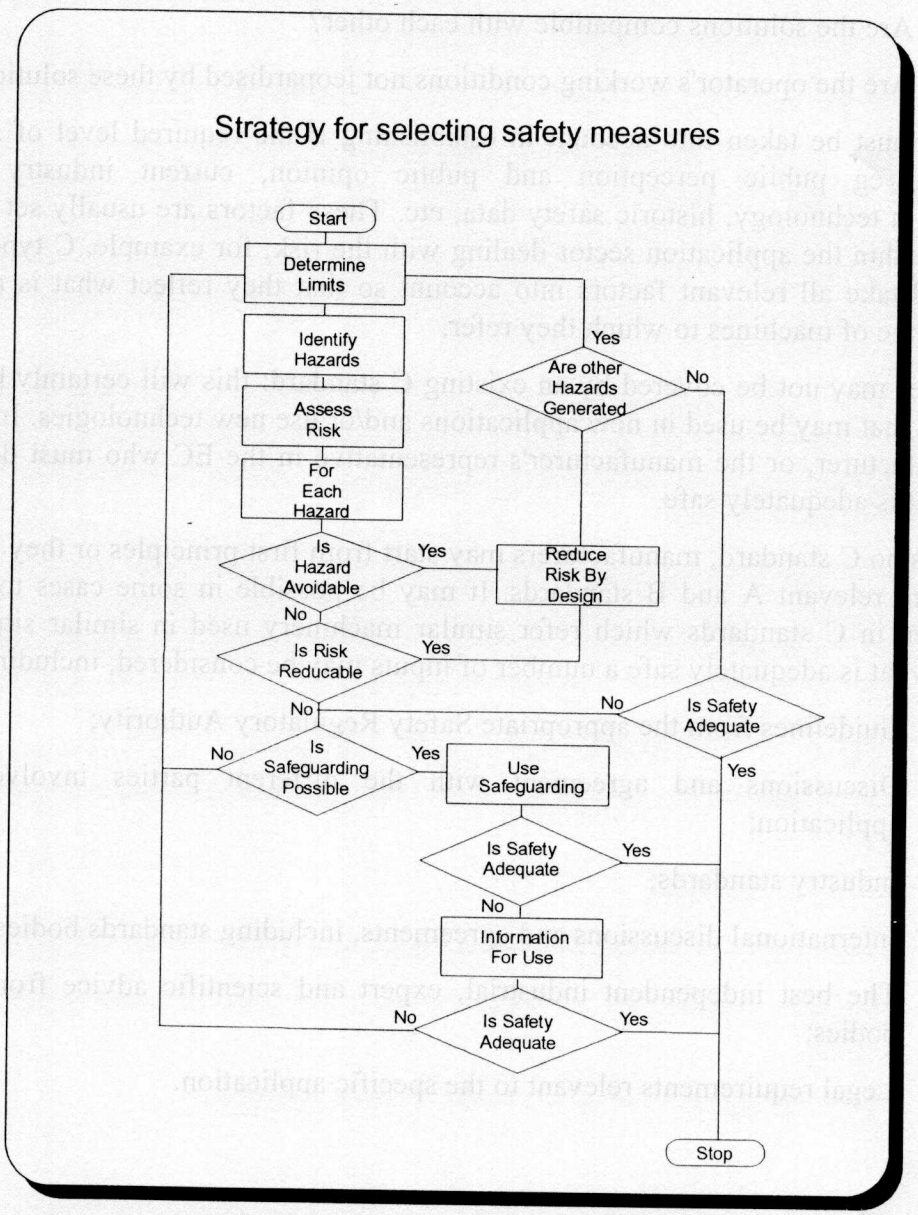

Fig 2

The determination of what may be accepted as adequate safety is not a straightforward task. The standard defines "Is safety adequate?" as:

- Has the required level of safety been reached?
- Is it certain that an adequate level of safety cannot be achieved more easily?
- Is it certain that the measures taken :
  do not excessively reduce the machine to perform its function?
  do not generate new, unexpected, hazards or problems?
- Are there solutions for all operating conditions and all intervention procedures?
- Are the solutions compatible with each other?
- Are the operator's working conditions not jeopardised by these solutions?

Many factors must be taken into account in establishing if the required level of safety has been reached, eg public perception and public opinion, current industry practice, developments in technology, historic safety data, etc. These factors are usually set implicitly or explicitly within the application sector dealing with the risk; for example, C type standard makers should take all relevant factors into account so that they reflect what is acceptably safe for the range of machines to which they refer.

Some machines may not be covered by an existing C standard: this will certainly be true for new machines that may be used in new applications and/or use new technologies. In this case, it is the manufacturer, or the manufacturer's representative in the EC who must develop the case as to what is adequately safe.

Where there is no C standard, manufacturers may start from first principles or they may adopt principles from relevant A and B standards. It may be possible in some cases to adapt the guidance given in C standards which refer similar machinery used in similar situations. In determining what is adequately safe a number of inputs may be considered, including:

- Guidelines from the appropriate Safety Regulatory Authority;
- Discussions and agreement with the different parties involved in the application;
- Industry standards;
- International discussions and agreements, including standards bodies;
- The best independent industrial, expert and scientific advice from advisory bodies;
- Legal requirements relevant to the specific application.

4. COMPLEX CONTROL SYSTEMS

As machine safety systems become more complex it becomes increasingly difficult to ensure that an adequate level of safety has been attained. This is particularly true for programmable systems. Programmable electronic systems (PES) are reliable and offer a much wider functionality than conventional, hard wired control systems. They are, however, very complex to analyse for safety. It may not be practical, or may even be impossible, to predict the effect of failure of each single component. Systematic failures inadvertently designed into the system, particularly software faults, could cause a machine to act in an unexpected, perhaps dangerous, manner.

Because of these uncertainties, sub clause 12.3.5 of EN60204-1:1993 "Safety of Machinery - Electrical Equipment of Machines": Part 1 "General Requirements"[7], advises against reliance on the correct operation of a single channel of programmable electronics, and prefers the use of hard-wired electro-mechanical components for emergency stop functions. It is a requirement of this standard that where programmable equipment is used for such functions, other appropriate measures (eg diversity and redundancy) shall be employed.

Most PES controlled machines have comprehensive self diagnostic and checking features. These improve safety performance but, when configured within a single channel, it may not be possible to ensure absolutely that an adequate level of safety has been attained. The rate of change of this technology also prevents a historical prospective from establishing a level of confidence of the integrity of this type of equipment.

4.1 Existing Techniques to Ensure Safety of Complex Machinery

Developing European standards that address the safety of complex plant and equipment, such as prEN 30218 "Manipulating Industrial Robots - Safety"[8] ,base technical measures for the prevention of accidents on two fundamental principles:

a) The absence of persons in the safeguarded space during automatic operation;

b) The elimination of hazards or at least their reduction during interventions (eg teaching, program verification) in the safeguarded space.

The standard covers all types of manipulating robots that are used in many industrial applications. The type of robot, its application and its relationship with other machines will influence its design and the selection of safeguards. To help designers select safety measures it follows the safety strategy outlined in EN 292-1[5].

When selecting safety measures, the design of the robot system is to be given first consideration while still maintaining acceptable level of performance. Where this is not possible, safeguarding is to be considered in such a manner that the flexibility of the robot system is in its application is retained.

The two fundamental principles require several actions including:

a) The creation of a safeguarded space and a restricted space (see Fig 3);

b) A design of the robot such as to allow the maximum number of tasks to be performed from outside the safeguarded space;

c) Provision of compensatory means of safety in case of interventions within the safeguarded space.

The standard calls for safety functions to be maintained in the case of a failure of any single component, electric, electronic, mechanical, pneumatic or hydraulic. Safety functions include, limiting the range of motion, emergency and safe stopping, reduced speed, and safeguard interlocking.

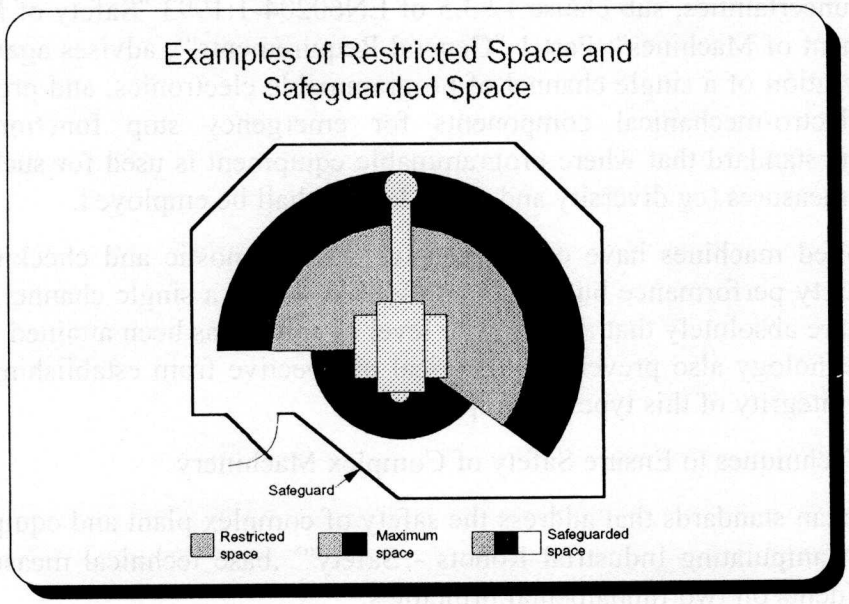

Fig 3

4.2 Advanced applications

As technology develops the suitability of excluding persons from a safeguarded space during automatic operation will become less practicable. Technology will allow, for example, the development of complex mobile or portable machines, that may be hazardous, and the development of hazardous machines that may be interactive with their operators and/or others. There are many potential applications for advanced automation in the construction industry.

For mobile/portable machinery it may still be possible to exclude persons from a safeguarded space: the space may itself be mobile with the machine. It is unlikely that it would be possible to use conventional guarding, but it may be possible to set up a virtual guard by the use of advanced techniques to sense the presence of persons inside the safeguarded space. Some advanced techniques do exist which could perform this function, eg image recognition, but, as these are themselves complex systems, the integrity of the safety system may be as difficult to assess as the integrity of the machinery being safeguarded.

For interactive machines, the only viable method of ensuring that a machine is safe is to ensure that it will always operate correctly and that no random hardware faults or systematic faults, may cause the machine to act in an uncontrolled or unpredictable manner.

The only way to do this is to follow a thought through safety strategy using quality techniques to give a level of confidence that the achieved level of safety meets the required level.

4.2.1 European Standards

At present there is no European standard being developed which directly addresses the safety of complex PES safety systems. Part two of prEN 954 "Safety related parts of control systems"[9] may address this problem in part. This standard categorises control systems according to their behaviour in case of a fault. Part two of the standard covers validation.

4.2.2 PES

The HSE guidance documents "PES"[3], although published in 1988, still provide sound advice on how to implement and use PESs safely. It bases the safety of a PES on three criteria,

a) The reliability of its component parts

b) The configuration of the system (diversity and redundancy)

c) Overall Quality

All three criteria are important for safety; however, only the third criteria, overall quality fully addresses systematic faults, particularly where those faults may be introduced at an early stage in the system lifecycle, eg during specification.

4.2.3 IEC SC65A

The international standard being developed by IEC SC65A[4] addresses this problem directly. It uses the concept of target safety integrity levels. The target integrity level is chosen according to the amount of risk reduction that must be attributed to the safety related system to reduce the overall risk to a tolerable level (see fig 4).

SYSTEM INTEGRITY LEVEL	TARGET SAFETY INTEGRITY	
	SAFETY-RELATED CONTINUOUS CONTROL SYSTEMS (dangerous failures per hour)	SAFETY-RELATED PROTECTION SYSTEMS (probability of failure to perform its design function on demand)
4	$\geq 10^{-9}$ *to* $< 10^{-8}$	$\geq 10^{-5}$ *to* $< 10^{-4}$
3	$\geq 10^{-8}$ *to* $< 10^{-7}$	$\geq 10^{-4}$ *to* $< 10^{-3}$
2	$\geq 10^{-7}$ *to* $< 10^{-6}$	$\geq 10^{-3}$ *to* $< 10^{-2}$
1	$\geq 10^{-6}$ *to* $< 10^{-5}$	$\geq 10^{-2}$ *to* $< 10^{-1}$

Fig 4

The tolerable risk level may be thought of as that which it is possible to justify the risk by showing that it is as low as reasonably practicable. The higher or more unacceptable the risk, the more, proportionately, those responsible for reducing the risk would be expected to spend to reduce it.

The proposed standard adopts an overall safety lifecycle as the key framework The safety lifecycle may be mapped to corresponding phases of the product lifecycle. All phases of the lifecycle follow a quality approach. For each phase, the following must be specified:

- The objectives to be achieved;
- The requirements to meet the objectives;
- The scope of each phase;
- The required inputs to the phase, and;
- The deliverable to comply with the requirements.

Figure 8: Safety Lifecycle: Overall Scheme

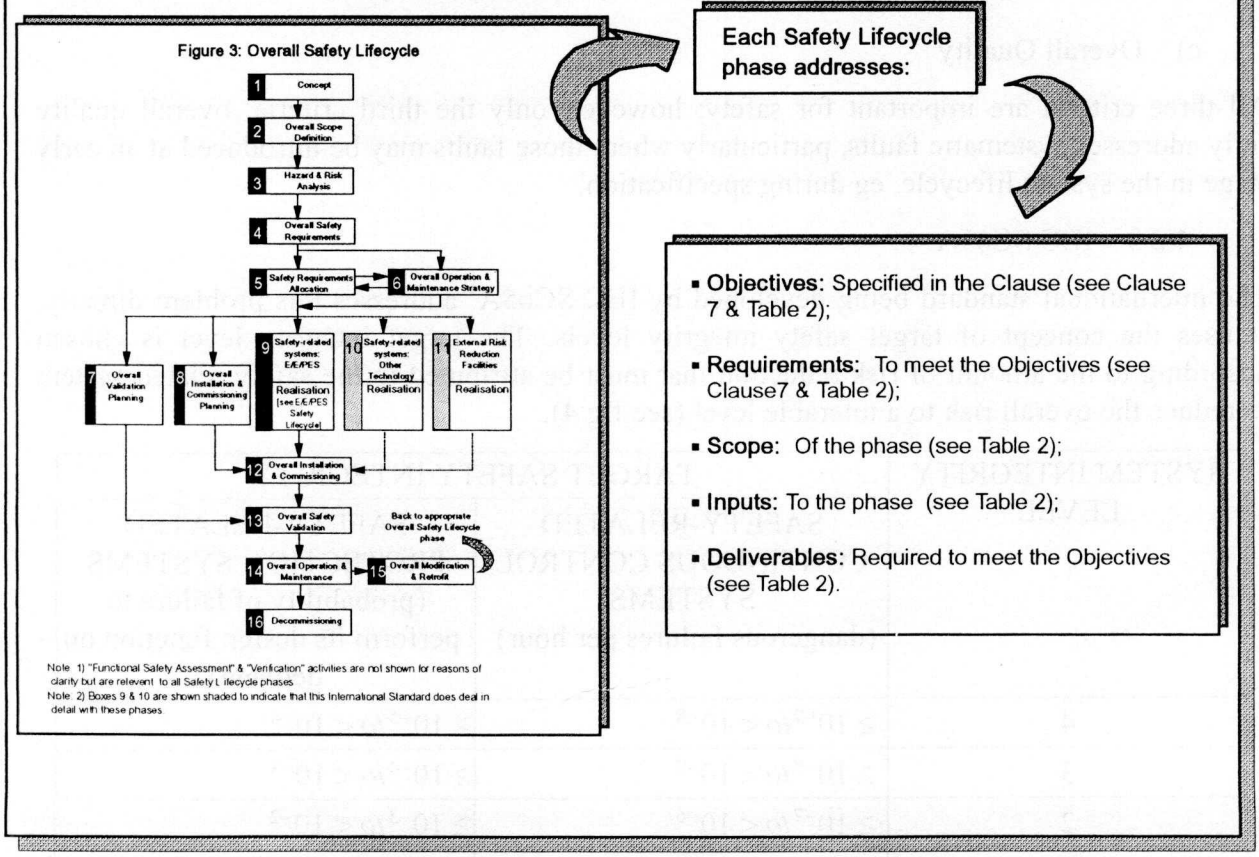

Fig 5

The standard also gives examples that recommend techniques/mesures which may be used contribute towards a level of confidence that the appropriate target safety integrity level has been met.

The standard is being developed in three parts. Part 1 deals with General Requirements, part 2 deals with specific requirements for Electrical/Electronic/Programmable Electronic Systems and part 3 deals with Software Requirements. All three parts of the standard are closely related and must be used together where appropriate.

5. CONCLUSION

The machinery directive[1] means a fundamental change in the way that new machinery is developed for safety. Prior to the directive, in the UK, it was possible for manufacturers to meet safety requirements by following detailed, prescriptive standards. The manufacturer and/or the manufacturer's agent did not need to assess if those measures were adequate, or evaluate risks. The machinery directive, in setting out broad ESRs and requiring technical documentation relating to safety, will, in my opinion, enhance safety awareness and ensure that manufacturers, and their agents, will have a sound understanding of the risks associated with the use of their machinery and appropriate steps which could be taken to minimise those risks.

Standards written in support of the directive will guide manufacturers towards meeting the directive ESRs, but will not diminish responsibility for assessing risks and determining the appropriate measures that should be taken to ensure that the machine is adequately safe.

The complexity of modern control systems means that it is becoming increasingly difficult to assess the machinery safety. Not only is the number of failure modes of so high as it is impossible to identify them, never mind test their effect on safety, but the complexity increases the susceptibility to dangerous systematic faults, inadvertently designed into the system. It is therefore not practicable, or may even be impossible, to test for all possible dangerous faults. Because of their nature, it is not possible to predict the, when or where systematic faults may arise.

The only way to address this problem practically is to use a thought through, risk based, quality approach throughout the lifecycle of the machine. This type of approach is used by IEC SC6A[4] in their developing standard.

6. REFERENCES

1 Official Journal Of European Communities, Volume 32, 29 June 1989, Pages L103/9 to L183/32 "Council Directive of 14 June 1989 on the approximation of the laws of the Member States relating to machinery (89/392/EEC) as amended by (91/386/EEC) and (93/44/EEC)"

2 The Supply of Machinery (Safety) Regulations 1992

3 HSE Guide-lines - Programmable Electronic Systems in Safety related Applications Part 1 (ISBN 0 11 883906 6) and Part 2 (ISBN 0 11 883906 3).

4 IEC/SC65A(Secretariat) 122 and 123 "Functional safety: safety-related systems";
Part 1: General Requirements;
Part 2: Requirements for Electrical/Electronic/Programmable Electronic Systems (E/E/PES);
Part 3: Software Requirements.

5 EN 292-1:1991, Safety of Machinery - Basic Concepts, general principles for design: Part 1: Basic terminology, methodology

6 BS EN 292-2:1991, Safety of Machinery - Basic Concepts, general principles for design: Part 2: Technical principles and specifications

7 BS EN 60204-1:1991 "Safety of Machinery - Electrical Equipment of Machines": Part 1 "General Requirements"

8 pr EN 30218 Manipulating Industrial Robots - Safety

9 prEN 954 "Safety related parts of control systems".

10 DTI, Europe Open For Business, Booklet "The Single Market - Machinery Safety", available from DTI's hotline: 081-200 1992.