

Health and Safety Executive Field Operations Directorate Polymers and Fibres Sector Paper Mills 2002/3		Sector Information Minute	
		SIM 4/2002/12	
		Open Government Status	Fully Open
Cancellation Date	For FOD SIU use	Author Unit/Section	Polymers and Fibres
Version No & Date	For FOD SIU use		

To
RSG/SSG Specialist Inspectors, AFQ Inspectors

TECHNICAL ISSUES ARISING FROM THE IMPLEMENTATION OF MAKING PAPER SAFELY

This SIM provides technical details on the implementation of the Safety-Related Control Systems element of the guidance booklet "Making Paper Safely".

Overview of the issue

The new Paper and Board Industry Advisory Committee (PABIAC) guidance *Making Paper Safely* (MPS) was published in February 2001. A small number of mills, in conjunction with local inspectors, sought clarification about the application of the guidance given in paragraphs 31–47 of the booklet regarding safety-related control systems in papermaking. Research was undertaken and the text was revised to try to assist paper mills in achieving the practical implementation of the guidance. The revised text is reproduced in full in a technical annex to this SIM. This will be issued as an addendum to *Making Paper Safely*.

Safety-related control systems are one component of the control measures necessary to control risks of serious injury or death arising from the papermaking process, in particular the physical safeguards on paper, board and tissue machines. A number of mills have been unable to complete work to achieve compliance with *Making Paper Safely* in the absence of a framework to make decisions about safety-related control systems.

Benchmark

Making Paper Safely is the published industry standard for health and safety in the papermaking process. The technical annex to this SIM forms part of that guidance and will be distributed to all mills via trade associations and other intermediaries.

The original guidance in paragraphs 31–47 of the booklet did denote some categories for the safety related control systems. The revised guidance does not do so, but provides a more detailed framework for mills to apply in reaching the appropriate solution for their paper mill. This means that there will be a period of development as paper mills apply the framework. Best practice and the technical benchmark will be developed on the basis of this action.

Strategic Factors

Effective implementation of the industry standard *Making Paper Safely* is an important element of a wider PABIAC Initiative to reduce the incidence of ill health and injury in the industry.

The Sector will closely monitor stakeholders' response to the revised guidance. Arrangements will be made via trade associations for one or two technical seminars to be held. The specialist who led the development will introduce the guidance to paper mill representatives who will then have an opportunity to ask questions and raise any concerns.

The resolution of this issue and the production of the revised guidance were achieved because of the strong partnership between mills, operational inspectors, suppliers, PABIAC and the Sector.

It is important that we continue to ensure a consistent approach to such issues. Any Inspector who identifies an issue that cannot be resolved locally is encouraged to refer the matter to the Sector, and/or to suggest that the mill contacts the Paper Federation of Great Britain for advice.

Enforcement conclusion

Mills should have identified any aspects of safety related control system work that prevented them from achieving compliance with *Making Paper Safely* in their correspondence to local inspectors about progress with their action plans. The Sector view is that delays in completion of work directly attributable to difficulties with safety-related control systems, which mills clearly identified as an issue, would justify a reasonable extended period for achieving compliance with *Making Paper Safely*. Any inspector who believes that the timescale given by mills is still excessive should consult the Sector.

This is a complex technical issue. The guidance advises mills that it is essential that work on the specification, design and development of programmable safety-related control systems is carried out by people who are competent in this particular field and who, in particular, are skilled in the concepts of capturing safety requirements; safety validation; safety-related system architecture design, hardware and software realisation; and project safety assurance. Specialist electrical inspectors should be consulted regarding translation of the contents of the technical annex into practical local solutions where necessary.

The Sector will support appropriate enforcement action in accordance with the Enforcement Policy set out in SIM 4/2000/11.

Date first issued: 15 July 2002

TECHNICAL ANNEX - SAFETY-RELATED CONTROL SYSTEMS

What is a control system?

1. A control system responds to input signals from the machine, or from the operator, and generates output signals, which make the machine operate in a desired manner. So if, for example, an operator presses a start button, the control system may respond by closing a contactor and energising a motor.
2. Control systems can be implemented in a range of technologies, but this guidance is mostly concerned with electrotechnical systems employing electrical, electronic and programmable electronic technologies. Electrotechnical control systems can range from simple electromechanical relay based systems to complex programmable systems with multiple analogue and digital inputs and outputs.

What is a safety related control system?

3. A control system in a paper making machine should be regarded as being safety-related if it contributes to reducing any risk to an acceptable level or if it is required to function correctly to maintain or achieve safety. The functions carried out by a safety-related control system are termed 'safety functions'. Generally, safety functions either prevent the initiation of a hazard or detect the onset of a hazard. Safety-related control systems should be designed and configured to a) be reliable enough (bearing in mind the consequences of any failure) and b) to perform the necessary functions to achieve or maintain a safe state or mitigate the consequences of a hazard.
4. For the purposes of this guidance, a distinction is drawn between those electrotechnical safety-related systems that use programmable technologies (such as a programmable logic controller (PLC) or microcontroller) and those that do not use programmable electronic devices (such as systems that use electromechanical components). The main purpose of this subdivision is to assist the designer to decide which of the 2 main standards that address the design of safety-related control systems to use: BS EN 61508 or BS EN 954-1.
5. Regardless of which standard is used, the design must take full account of the level of risk reduction that the system is required to achieve. This is because, in principle, the required level of risk reduction will have a significant influence on the design techniques needed for reliability and tolerance to faults.

General Principles of Safety-Related Control System Design

6. The design characteristics for reliability and fault tolerance of a safety-related control system must stem from the basic risk assessment carried out on the machine. This assessment will identify aspects of the machine's operation that create risks that may need to be reduced to an acceptable level.

7. Designers may employ a range of techniques to reduce the level of risk, many of which will not involve the use of safety-related control systems. For example, the use of fixed guards will prevent access to dangerous parts, and the provision of platforms and walkways will reduce the risk of falls from height. However, in many cases risks cannot be reduced to acceptable levels without incorporating safety-related control systems. In this case, the designer needs to understand and assess the contribution that these systems make to the reduction of risk, and the consequential reliability and fault tolerance that the systems will need. The more critical the role played by the safety-related part of the control system, the more reliable and resistant to faults it must be. This property is known as the safety integrity of the system, which is a measure of how well the safety-related control system will perform the required safety function(s) under all stated conditions within a stated period of time when required to do so. An adequate level of safety integrity may be achieved by a combination of:

- the reliability of the hardware and software; and
- the way the parts are combined in the design of the control system; and
- the use of diagnostic and testing techniques.

8. The designer should identify all the safety functions to be performed by the safety-related control systems and then specify their required safety integrity levels. This specification is known as the Safety Requirements Specification and is of fundamental importance for achieving safety by design. The overall process is illustrated in Figure 1.

9. In designing a safety-related control system to achieve an appropriate level of safety integrity that is commensurate with its contribution to risk reduction at the machine, the following requires consideration:

- Reliability of the equipment that comprise the safety-related control system;
- Use of techniques such as redundancy and/or automatic diagnostics;
- How to prevent, as far as possible, faults in design and manufacture of hardware and software (e.g. software 'bugs' or faulty wiring);
- How to incorporate design features which may help the control system to recover from faults during operation (e.g. program sequence monitoring);
- Behaviour of the safety-related control system under fault conditions (failure modes).
- How to test the safety-related system(s) initially to show, as far as possible, that there are no design, or manufacturing or installation faults before the machine is put into operation.

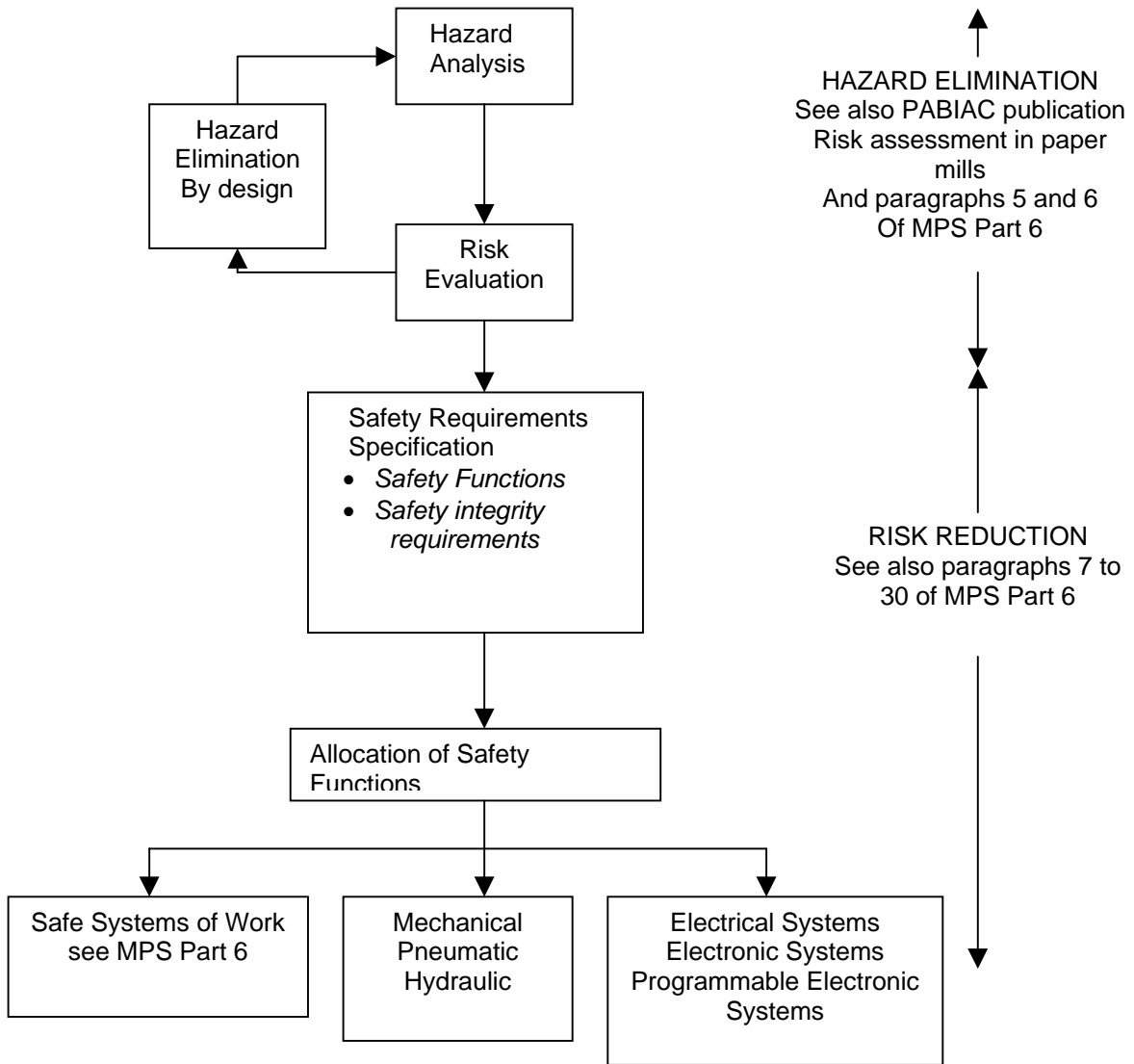


Figure 1 - The risk control process

How to design periodic test and inspection procedures for the safety-related system(s) periodically for the lifetime of the machine to show that no part (including both hardware and software) has changed or deteriorated beyond reasonable limits.

10. These issues must be taken into account for all parts of the safety-related control system including hardware, software and the way that parts are combined during integration. Remember that the safety-related control system comprises everything necessary to carry out the required safety function (e.g. sensors, control logic and brakes).

11. The following points aim to assist in the process of designing safety-related control systems. They are applicable to new machines, machines being refurbished to present day standards and to older machines being reassessed for the purpose of improving safety.

- As part of the risk assessment exercise, determine which of the measures relies on a safety-related control system.
- For each safety function, determine the contribution required from the safety-related control system to achieve the necessary level of risk reduction.
- Draw up the safety requirements specification that relates the required safety integrity level to each of the safety functions.
- Design the system, including the safety-related system.
- Validate the design to ensure that it meets the safety requirements specification. This should include consideration of the consequences of failures. This may require the application of Failure Mode and Effects Analysis (FMEA) to the control circuits to determine the behaviour under fault conditions. (In the simplest form of FMEA the question “what happens if a particular part fails to function as intended” is asked). The design should consider failures within purpose built control units, such as electronic motor drives, as well as those in circuitry external to the drives. There are a number of standards on safety-related systems available that provide relevant guidance, the main two being BS EN 954-1 and BS EN 61508. It is essential that designers are familiar with these standards and are competent to apply their principles in practice.
- Document the process so that anyone who needs to can understand how and why the system meets the safety requirements.

12. To maintain safety integrity levels, all safety related control systems should be tested regularly as part of a preventative maintenance strategy. For any particular safety-related control system, the frequency of testing should be determined taking into account the required safety integrity level, the safety demand rate on the system, the degree of fault tolerance, and the diagnostic capabilities of the safety-related

control systems. For example, consider a machine with an overspeed detection and protection system in which failure of the system could lead to injury in the event of the machine exceeding its maximum speed. It is likely that the demand rate on the safety function (i.e. prevention of speed above a set value) will be very low in normal operation and its design may be such that a potentially dangerous fault could remain undetected until a demand is placed on the system. In this type of safety-related control system, the overall safety integrity level could be improved by arranging for the safety function to be tested as part of a routine maintenance programme at a frequency recommended by the designer, with instructions on the maintenance regime being included in the machine's documentation.

13. The following points are applicable when modifications are being made to safety-related control systems. Typical reasons for modification of a safety-related control system include changes to the conditions of use, incident/accident experience, and modification of the machine or its operating modes.

- The proposed modification should be assessed to determine the contribution that the modified safety-related control system will make towards risk reduction. The proposed modification should then be analysed to establish the impact on the hardware and software elements of safety-related control system. This should include an appropriate review of the failure modes, particularly new failure modes that may be introduced by the modification, and their consequences for safety at the papermaking machine.
- Where it is agreed that a modification can be made without an adverse impact on safety, hardware and software changes to the safety-related control system should be processed within a structured work programme incorporating, as appropriate, specification, design, integration, installation, commissioning, and validation.
- The changes made to the safety-related control system should be documented and marked with appropriate version numbers and dates.
- Prior to re-instating the papermaking machine into normal operation it is recommended that the modification work be reviewed by a competent person to ensure that the work has been fully implemented.

Programmable Safety-Related Control Systems

14. In general, programmable electronic safety-related control systems on paper making machines should make use of devices that have been specifically designed and assessed for use in safety-related applications. General industrial programmable logic controllers (PLC), or general purpose computers and similar devices, will usually not have sufficient safety integrity for safety-related applications unless additional measures are employed to protect against failure and the overall arrangements are assessed against relevant standards.

15. The safety integrity level (SIL) claimed for any PLC or similar device that has been supplied for use in safety-related applications should be equal to that of the most

critical safety function that it performs. For papermaking machines, it is recommended that single PLCs and similar programmable devices used in safety-related applications should, in themselves, be capable of satisfying the requirements of SIL 3 in accordance with BS EN 61508. This also applies to the application software (e.g. ladder logic, function blocks).

16. Programmable safety-related control systems contain software components so, in addition to considering the design features needed to control the effects of random hardware failures, the designer must take steps to ensure that the software does not contain faults, known as systematic faults, that can lead to danger. Since it is generally recognised that software cannot be tested with sufficient confidence to detect all such faults, the preferred approach to minimising the likelihood of errors being introduced during the specification and development of the software is to ensure that the project is well managed within a structured framework, with progressive verification and validation of the software components throughout the development cycle including any final development work during commissioning activities. It is strongly recommended that such work be carried out within a formal quality control system.

17. Within this framework, the accuracy and completeness of the initial specification for the requirements for safety performance in the control system is of fundamental importance - if the initial specification is at all deficient, the follow-on stages in the development cycle will not prevent systematic faults from being inadvertently introduced, no matter how rigorously they are implemented.

18. It should be recognised that a programmable safety-related control system at a papermaking machine may also include non-programmable technologies, such as electrical and electronic parts (e.g. gate switches, transposing relays, etc). These parts normally have assigned safety performance categories to BS EN 954-1:1997. Prior to their integration into a programmable safety-related control system it is important that the designer/integrator is able fully to determine whether their application will allow the safety function to achieve the appropriate safety integrity level.

19. It is essential that work on the specification, design and development of programmable safety-related control systems is carried out by people who are competent in this particular field and who, in particular, are skilled in the concepts of capturing safety requirements; safety validation; safety-related system architecture design, hardware and software realisation; and project safety assurance. The Institution of Electrical Engineers, in conjunction with the British Computer Society, has published guidance on the competence requirements for people working in this field¹.

¹Safety, Competency & Commitment - Competency Guidelines for Safety-Related System Practitioners; IEE; ISBN 0 85296 787 X

Non-Programmable Safety-Related Control Systems

20. This type of safety-related control system does not contain programmable electronics, although it is recognised that systems implemented in non-programmable technologies may in themselves be quite complex in nature. They include electromechanical relay-based systems, hydraulic and pneumatic systems, and mechanical systems that can be assessed using deterministic principles.

21. The general principles for the design of these systems are similar to those used for programmable systems. This is because the requirements should be based on a fundamental assessment of the risks created by the machine and the extent to which the safety-related control system is needed to reduce those risks to an acceptable level, taking into account all other measures taken to control the level of risk.

Use of Standards for Safety-Related Control Systems

22. The transposed harmonised standard BS EN 954–1 *Safety of Machinery - Safety related parts of control systems* provides requirements by which the safety related parts of control systems of all operating media can be categorised in a qualitative manner according to their reliability and performance under fault conditions.

23. Guidance on the processes and procedures appropriate to the design and development of electrical, electronic and programmable electronic technology based safety-related control systems is set out in the basic safety publication BS EN 61508: *Functional safety of electrical / electronic / programmable electronic safety related systems*. It provides guidance on all aspects of the design, development and use of safety-related control systems using the Safety Lifecycle model to indicate the measures that should be applied from the conceptual design phase through to decommissioning. It describes quantitative and qualitative methods of control system analysis.

24. Machinery designers should decide on the appropriate standard that can be applied to the safety related control circuits, see the flowchart in Figure 2.

BS EN 954

25. This is a harmonised standard that includes a mechanism by which the safety-related parts of control systems can be categorised in a qualitative manner according to their performance under fault conditions and where the behaviour of the system under fault conditions can be completely determined by analytical and/or test methods.

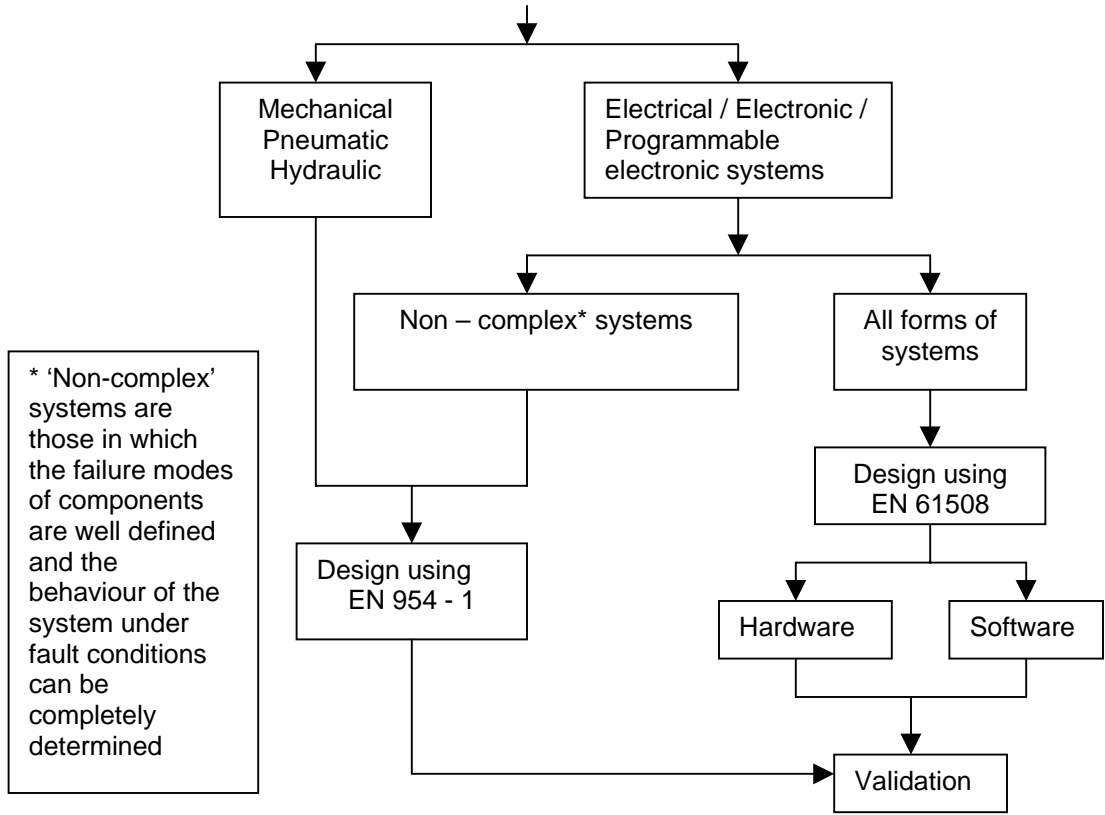


Figure 2 – Use of standards

26. The standard categorises systems, in total or in part, according to their ability to resist the occurrence of faults and whether they will continue to perform their safety function after a fault has occurred. Fault resistance may be achieved by the reliability of the hardware and the way the component parts are combined in the design of the control system.

Categories of control systems used in BS EN 954-1

27. There are five main categories of performance of control systems in accordance with the standard which are broadly:

Category	Basic Requirements
B	Use of good engineering principles
1	Use of well-tried components and principles (reducing the probability of failure)
2	Incorporates a safety function check at machine start-up and may also be checked periodically (safety monitoring) A single fault may lead to the loss of the safety function
3	A single fault will not cause the safety function to fail (redundancy of hardware)
4	Two or more faults will not cause the safety function to fail (redundancy and monitoring)

Application of BS EN 954-1

28. It is important to bear in mind that safety-related parts of control systems may not neatly fit into a single category, particularly if they use different energy sources - a control system can incorporate electrical, electronic, programmable electronic, pneumatic or hydraulic devices.

29. The categories should not be regarded as hierarchical with regard to safety. For example, a single positively operated safety switch element, manufactured to a published safety standard will, itself, meet the requirements of Category 1 but not the criteria for higher categories. However, its level of safety performance may be considered at least as reliable as technologies that meet Categories 2 and 3. Therefore, the selection of categories for the safety functions on paper making machines is a matter of judgement that should be based on the risk assessment and failure analysis.

30. A British Standards Institute (BSI) published document PD CR 954-100:1999: *Guide on the use and application of EN 954-1: 1996*, provides further information.

BS EN 61508

31. Guidance on the processes and procedures appropriate to the design and development of safety-related control systems is published in BS EN 61508; the standard relates to systems implemented in electrical, electronic and programmable electronic technologies. This standard is a basic safety publication in the IEC and has been formally adopted within Europe but not harmonised to a specific Directive. It is regarded as the authoritative good practice in this field.

32. BS EN 61508 contains advice on the system hardware and software architectures aimed at achieving an adequate level of safety integrity. A quantitative analysis concept in BS EN 61508 is that of Safety Integrity Levels (SILs), which specify the failure rate (for continuous mode safety functions) and probability of failure on demand (for 'on demand' safety functions) for each safety function. SILs range from SIL1 to SIL4, with the latter having the highest level of safety integrity. The failure rates allocated to SIL values are shown in the following table; this definition of SILs is most appropriate in machinery safety applications. The initial risk assessment process determines the SIL of a safety function, the analysis of the machine's safety requirements and the level of risk considered acceptable in the specific application. It is essential that a competent person undertake this analysis.

SIL	Dangerous failure rate of the safety function (per hour)
4	$\mu 10^{-9}$ to $<10^{-8}$
3	$\mu 10^{-8}$ to $<10^{-7}$
2	$\mu 10^{-7}$ to $<10^{-6}$
1	$\mu 10^{-6}$ to $<10^{-5}$

33. A SIL is assigned to each safety function in a safety-related control system and has a strong influence on the requirements that have to be taken into account during the design and integration of a safety-related control system. These measures, together with the calculation of failure rates for the safety-related control systems, are an integral part of the process of achieving a safe design.

34. Part 5 of BS EN 61508 gives examples of methods for the determination of SILs for allocation to safety functions. Note that the examples given in BS EN 61508-5 only illustrate general principles and should not be used directly without development to take into account the risk factors (especially tolerable risk) associated with specific applications.

35. A machinery sector implementation of BS EN 61508, IEC 62061, is being developed and it is anticipated that, once finalised, it will be published as a European Standard and that it will provide machine designers with guidance on how to develop and validate safety-related electrical, electronic and programmable electronic control systems.

Comparing SILs and Categories

36. The fact that categories in EN 954-1 and SILs in BS EN 61508 both have allocated numbers 1 to 4 does not mean that there is a direct relationship between them. Both standards are written from different perspectives so SILs and Categories are not comparable measures. Categories are not to be assumed as hierarchical measures for all applications but SILs are hierarchical because they relate to probabilities of failure.

37. As an approximation, the relationship between categories and SILs assigned to safety-related control functions to be implemented by electrical, electronic or programmable electronic safety-related control systems at a typical machine may be considered to be:

Category of safety-related control function in accordance with BS EN 954-1	Target failure measure for safety-related control function in accordance with BS EN 61508
1 or 2	SIL 1
3	SIL 2
4	SIL 3

It is very important to note that this approximation can only be used when considering the entire safety function that will be implemented by a safety-related control system at a papermaking machine. It does not apply to only a part of a safety-related control system.

Particular safety functions on paper making machines

38. There are 3 particular safety functions on paper making machinery that need to be given careful consideration, as detailed below. In addition, there can be many other safety functions that will need to be considered; these will include guard interlocking and hold-to-run control.

Emergency stop

39. The emergency stop function should be designed in accordance with BS EN 60204 -1:1998 *Safety of Machinery - Electrical equipment of machines Part 1: General requirements* and BS EN 418:1992 *Safety of Machinery - Emergency stop equipment: Functional aspects - Principles for design*. Stopping categories 0 or 1 may be used. Adequate environmental protection of the system hardware should be provided to reduce the probability of dangerous failures.

40. Since an emergency stop circuit can remain inactive for long periods of time it is important that the reliability and architecture of the design solution, and the

maintenance and testing requirements, are such that there is a high confidence that it will function effectively on demand.

41. The emergency stop function should not be reliant on the correct operation of a machine control system that deals with other safety functions and where unrevealed failures in the control system would negate the operation of the emergency stop functions. In such cases, an independent emergency stop control system should be provided.

Speed control system

42. The risks that occur in the event of overspeed at a machine arising from control system failure can be significant, particularly when the operator is working inside the hazardous area, for example to remove broke. The use of a hold-to-run or enabling device by the operator or an accompanying person will not eliminate the risks completely, so the control system should be designed, or modified, to minimise the risk of injury from:

- unexpected increase in crawl speed, hold-to-run speed or other pre-set low speed
- unexpected start up while machines are held at stop condition by the control system only, i.e. a category 2 stop as described in EN 60204 - 1.

43. Where reasonably practicable, to recognise a deviation from a set speed condition where danger could arise (including zero speed) design options should include one or more of:

- Monitoring techniques to enhance the safety features of the speed set point control circuitry and the reliability of the speed detection devices. Dangerous deviations detected by monitoring should initiate a safe stop.
- A speed reference tachometer / encoder / motion transducer or overspeed trip / detection device automatically set for use during slow speed or stop conditions. Activation should initiate a safe stop.
- Allow more time for machine operators to react by, for example:
 - modifying the acceleration or current limit control signals
 - modifying inertia compensation control signals

Pre-start warning device

44. Failure of a pre-start warning device could result in the machine being started before the waiting time has elapsed (i.e. people would not have enough time to leave a hazardous area on hearing the alarm) or the machine could be started up without a warning being sounded.

45. The aim should be to ensure that the pre-start warning system would have very high reliability and availability and be effective so that the warning signals can be recognised by all personnel who would be exposed to danger when machines are started.

46. The control system safety reliability considerations should include:

- monitoring of components so that recognised failures will prevent start up.
- applying redundancy techniques to the safety critical parts of the warning system.

47. The effectiveness considerations should include:

- Selecting the audible warning, or other warning indication device (including voice messages), so that it is easily understood by the workforce at risk, taking account of hearing impairment from medical conditions or use of hearing protection (PPE);
- where there are a number of separate machines, ensuring that each device dedicated to a particular machine is recognised by those at risk from the particular machine.