Harpur Hill, Buxton
Derbyshire, SK17 9JN
T: +44 (0)1298 218000
F: +44 (0)1298 218590
W: www.hsl.gov.uk

HEALTH & SAFETY LABORATORY

Standards which are relevant to the selection and use of electrical switches for safety related controls in mine shaft and winding systems

HSL/2007/58

Project Leader: **D C Gregory**

Author(s): **D C Gregory R B Lee**

Science Group: **Hazard Reduction**

ACKNOWLEDGEMENTS

I would like to acknowledge the cooperation of Maltby Mine, Transmitton and Qualter Hall for providing information used in the background to this report.

CONTENTS

EXECUTIVE SUMMARY

Objectives

To review the guidance, protocols and standards that are currently available for the selection of suitable switches etc for safety related applications in mine shafts including safety critical applications, the failure of which could lead to major loss of life and damage. This has been extended to look at the safety-related control system in its entirety.

To develop a reference guide/aide memoir for best practice in relation to safety-related control systems in mine shafts.

Main Findings

There are no specific standards for control system design and safety switch selection, for the prevention/detection of shaft intrusions. New machinery standards follow the BS EN 61508:2002 series approach, applying a safety integrity level to the machine, which the control system and safety switches have to meet. Whilst there will be difficulties in trying to back engineer a 20+ year old system to comply fully with this approach, it should be possible to identify any areas that do not follow best practice.

Recommendations

- Identify and assess the hazard and then select an appropriate Safety Integrity Level (SIL) for the risk control functions of the equipment;
- Ensure that all mechanically-actuated position switches are actuated in the positive mode;
- Ensure that all hardware is suitable for the environment in which it is to operate, in particular with respect to resistance to corrosive liquids, ingress of dust and the ability to withstand impact damage;
- Provide additional measures to prevent/detect failure where magnetic and proximity type safety switches are used.

In accordance with the selected SIL:

- Employ redundancy and diversity to avoid common cause failure, where necessary, to achieve and maintain the SIL;
- Ensure suitable measures are taken to prevent inadvertent or deliberate alteration if a safety related control system is capable of being re-programmed;
- Ensure Safety related software is self-monitoring;
- Ensure that the decision making process for implementation of a new system or modification of an existing system, is suitably documented in a transparent, traceable and comprehensible way and this documentation is retained and available for the purpose of external assessment and validation.

1 INTRODUCTION

On 3 March 2006, a serious incident occurred at the No.2 shaft at Maltby Mine while the friction winding system was being used to wind workmen into the mine in push-button winding mode. The 3 deck cage, with 18 men in the top deck, was descending to the pit bottom at a speed of approximately 10 m/s when it hit a drawbridge type platform at an intermediate inset 151m above the pit bottom. A hydraulic fault resulted in the platform not fully reaching its safe position before the Onsetter switched off the powerpack for the hydraulic system and the platform gradually began to lower into the path of the cage.

The investigation found that the 'TUB4' lever switch that should have detected that the platform was not in the fully raised position, had suffered from environmental attack and was seized in the 'closed contact' position, falsely indicating that the platform was raised. The switch was a single line component and relied on internal springs to open the contacts, (non-positive operation) when the platform was not in the fully raised, safe position.

In the 1980's when the winding system was installed, the coal mining industry had its own electrical acceptance scheme under which apparatus and systems were examined for operational safety, practical application and technical design. With the decline of the industry there has been little progress in improving / updating the items included in this scheme. The machinery safety regulations have, on the other hand, been reviewed and updated to take into account technical innovation that has been applied to this field.

A number of visits have been made to Maltby mine to familiarise ourselves with the operational environment and to discuss proposals for improvement to the safety switches. As a result of this, concerns were raised as to the integrity of the control software and a further meeting was held with Transmitton, the designers and manufactures of the control system, to discuss this in greater detail.

This work has reviewed the guidance and standards relevant to machine safety and relates the relevant parts to the above issues. It also tries to identify potential weaknesses that do not take into account the severity of the coal-mining environment.

2 OVERVIEW OF THE SHAFT AND WINDING SAFETY CONTROL SYSTEM (TRANSMITTON SYSTEM)

INTRODUCTION

Electrical switches forming part of a shaft and winding safety control system, hereafter referred to as ‘safety switches’, should be suitable for the specific safety application.

However, the selection of suitable safety switches forming part of a shaft and winding safety control system will be of little value in itself, if the parent safety control system does not have the necessary safety integrity level. The safety integrity level of the whole system needs to be considered. At the time of the Maltby Mine shaft incident, the safety control system was a Transmitton system, commonly used in UK mine shafts, and consisted of:

a). Control System

The original hardware type TM101 Mark 1 system was developed in 1972. This was adapted and developed for use on shaft interlocking and shaft signalling TM102 in 1977. The mark 2 system as fitted at Maltby was developed in the early 1980’s and installed at Maltby in 1987. The system consists of the mark 2 central station and H series outstations at the different levels in the shaft.

b). Central Station

During start-up and normal operation the central station carries out checks for memory faults, EPROM and essential boards fitted and uses a hardware watchdog timer that must be reset by the software within a preset time interval. The individual boards within the central station also have a “check back” system that has to be satisfied along with the watchdog.

c). H series outstation

The outstations contain 3 EPROM’s to store the compiled code, one for the communications, one for the executive and the final one for the system configuration. In reality it is only the configuration software that is modified and this is achieved using a bespoke piece of software developed by Transmitton.

An oscillating output is used to drive the safety switch circuits, the operation of the switches is monitored by diode proved inputs. By momentarily stopping the oscillators the ability of the inputs to detect an open state is checked. The system also incorporates the same checks on memory, etc. as the central station and again has a watchdog timer.

The Transmitton TM102 mark 1 and 2 represented cutting edge technology at the time it was designed and installed. The TM102 uses many safety-related hardware and software techniques that were incorporated into guidance documents and standards several years later. However, as technology and techniques have advanced, standards and guidance have evolved. Although the system is still fit-for purpose, there is not enough information to reverse engineer the hardware and development process to ascertain if TM102 system complies with guidance and standards referred to in this report and therefore it is not practical to try to allocate the system a Safety Integrity Level.

3 RELEVANT STATUTORY PROVISIONS GUIDANCE AND STANDARDS

The statutory provisions relevant to the provision and use of safety controls for mine shafts and winding systems are:

The Provision and Use of Work Equipment Regulations 1998

The Mines (Shafts and Winding) Regulations 1993

The main industry guidance which is relevant is the Safe Manriding in Mines Report (SMIM) 1976 Parts 1 & 2, in particular Part 1B section 19, paragraph 7.

The following is a list of standards that have possible relevance to this application:

- PD5304:2005, Guidance on the safe use of machinery; (section 4.1)
- BS EN 60204-1:2006, Safety of machinery-Electrical equipment of machines-Part 1: General requirements; (section 4.2)
- BS EN 954-1:1997, Safety of machinery-Safety related parts of control systems-Part 1. General principles for design; (section 4.3)
- BS EN 1088:1996, Safety of machinery-Interlocking devices associated with guards-Principles for design and selection; (section 4.4)
- EN ISO 13849:2006, Safety of machinery-Safety-related parts of control systems
  Part 1: General principles for design (section 4.5)
  Part 2: Validation; (section 4.6)
- BS EN 62061:2005, Safety of machinery-Functional safety of safety-related electrical, electronic and programmable electronic control systems; (section 4.7)
- BS EN ISO 12100-2:2003, Safety of machinery- Basic concepts, general principles for design; (section 4.8)
- BS EN 61508 series:2002 (section 4.9)

To help to try to apply the guidance and standards the manriding cage, drawbridge and control system were considered to be a machine that requires a high level of safety integrity, given that in the event of a system failure the likelihood of multiple serious injuries or fatalities would be significant. The comments from the relevant guidance and standards reflect this with appropriate paragraphs being reviewed in greater detail.

4 SUMMARY OF GUIDANCE AND STANDARDS

4.1 PD5304:2005, GUIDANCE ON THE SAFE USE OF MACHINERY

This document is the main reference used in the training of HSE inspectors for the inspection and safety assessments of a whole range of machines found in industry. It provides guidance on the safe use of machinery supplied prior to the Supply of Machinery (Safety) Regulations 1992 [3] (normally machines supplied before 1995).

Section 5. Aspects of machine design to eliminate or reduce risks

5.3.7 Program or sequence control

A hazard analysis and risk assessment ought to be carried out to establish the full implications of a program error.

5.14 Electrical systems

States that electrical equipment should conform to BS EN 60204-1 or the appropriate machine standard where one exists. Annex C of 60204-1 includes passenger lifts as being covered by this document.

5.23 Programmable systems

Systems intended to be capable of reprogramming present assurance problems if safety is affected. Such systems include:

a) disc, cam or drum arrangements operating switches;

b) selector switches or valves affecting otherwise “hardwired” logic;

c) card readers;

d) punch tape readers;

e) magnetic tapes or discs;

f) electronic or optical storage.

Ways of preventing inadvertent or deliberate alteration of the stored program ought to have been considered. These should encompass both reliability and security of the storage system and include the following measures:

1) pinned cams;

2) program storage in read only memory (ROM);

3) locks restricting access;

4) password access to software.

Section 9. Interlocking considerations

9.1 Functions of an interlock

The function of an interlock is described as an interaction with a guard. For this application, we are indicating the safe retraction/storage of the drawbridge. This means that the safe storage of the drawbridge is equivalent to the guard being closed.

9.1 a) states, “Until the guard is closed the interlock prevents the machinery from operating”

9.6 Electrical interlocking devices

9.6.1 General

This lists the types of electrical interlocks available, the operation of which, is discussed in separate chapters. Three types of interlocks have been considered for this application to date, they are:

1. cam operated position switches (9.6.2);
2. inductive proximity switches (9.6.6);
3. magnetic switches (9.6.7).

It also states, “Devices ought to have been selected only from those where the performance, as stated by the manufacturer, is suitable for the specific safety application” and lists the performance data that should be considered:

1. resistance to environmental conditions (IP rating), corrosion resistance, vibration resistance, electromagnetic disturbances;
2. life evaluation;
3. duty rating;
4. reliability.

The mining environment can be physically demanding on components and it would be advisable that the robustness of the safety switches, with regards to mechanical impact damage should be a factor.

9.6.2 Cam-operated position switch

This section describes the difference in operation between a positive and non-positive position switch and that positive mode switches should incorporate direct opening action.

9.6.6 Proximity switch

Proximity switches which rely solely on the presence or absence of metal for their actuation are not generally suitable for interlocking duties because they can easily be defeated.

Those which have been specifically designed for interlocking often rely on the use of a special, e.g. coded, complementary target. These switches should conform to BS EN 60947-5-3 and whose performance, stated by the manufacturer, is suitable for the specific safety application (BS EN 1088:1996, 6.3).

9.6.7 Magnetic switch

Magnetic switches should only be selected whose performance, stated by the manufacturer, is suitable for the specific safety application (BS EN 1088:1996, 6.3).

Where the switching element is a reed, such switches are not generally suitable for interlocking duties, because the reed can fail to danger, they can be defeated by the use of a suitable magnet, and vibration can cause malfunction. There are reed switches available that have been specifically designed for machinery safeguarding. The design should provide maximum immunity from vibration and contact welding. If overloaded, the switch should fail to an open circuit condition (BS EN 1088:1996, 6.3.5 and Annex J).

Section 10. Safety related control system

10.1 General

“Some interlocking systems have more than one control channel, e.g. dual control systems. It is often advantageous to design these systems so that similar failures in both channels from the same cause (common cause failures) are minimised”

10.2 Interlocking control systems and architectural considerations

Three types of interlocking systems are described with different levels of safety integrity:

1. 10.2.1.2 Dual-control system interlocking with cross-monitoring
   Has the highest level of integrity with two separate power interrupting devices. The power interrupting devices are monitored so that the failure of their control system or the devices themselves is immediately detected and further operation of the machinery prevented.
2. 10.2.1.3 Dual-control system interlocking without cross-monitoring
   Follows the same principles as those described above but without the facility to automatically monitor the correct functioning of the power interrupting devices. Regular checks are required to prove the functionality of both devices, but in the event of an undetected failure the integrity of the system is reduced to that of single-control system interlocking.
3. 10.2.1.4 Single-control system interlocking
   This is the type of system that was initially installed at Maltby mine.

10.2.2 Failures in interlocking control systems

The possibility of the interlocking system as a whole failing to danger should have been minimized.

Power supply failures are more frequent than failures of components themselves. Components relying on the power supply for their functioning should be installed so that power loss minimizes failure to danger of the system as a whole.

An example is given as to why positive mode position switches should be used in preference to non-positive mode switches. However positive mode switches can fail to danger in the event of excessive wear, or displacement of the cam, track, follower or internal and external mounting, resulting in insufficient movement to change the state of the interlock. Without frequent inspection, this situation can remain undetected.

10.2.2.2 Types of failures

List the most common failures that interlocking control systems can suffer from, not all of which are electrical. Particular attention is made to the mechanical arrangements for actuating position switches.

Systems as a whole can still fail due to multiple component failure e.g. common cause failures, these can typically result from:

1. external environment;
2. components from a substandard batch being used in each channel;
3. damage due to localized fire or impact.

10.2.3 Integrity of interlocking control systems

The integrity of an interlocking control system depends not only on the direct effects of failures or defeats but also whether or not those failures or defeats lead to damage to other components or interconnections within the system. Therefore, an important consideration should be circuit protection.

Other basic criteria for improving the integrity of an interlocking control system include:

a) correct installation;

b) good quality, high integrity components, protected to withstand the environment and rated for the duty they perform;

c) minimizing by design, manufacture and correct installation, the probability of an earth fault occurring;

d) minimizing failure to danger;

e) minimizing misuse.

Power interlocking systems eliminate intermediate components used in control interlocking systems thereby reducing the probability of failure. Alternatively, the probability of failure of a control interlocking systems can be reduced by incorporating additional interlocking and/or monitoring channels.

10.2.4 Choice of interlocking control systems

Manufacturers ought to have selected systems of interlocking for particular applications taking account of:

a) the frequency with which approach to the danger zone is required;

b) the probability and severity of harm should the interlock system fail;

c) the resources required to reduce the risk.

10.2.5 Electrical considerations

10.2.5.1 General

The following should be the main items for consideration:

a) interlocking devices used for interfacing with guard movement;

b) signal operated devices, e.g. relays or contactors;

c) interconnections within the system, e.g. wiring

d) overall system design.

All electrical control systems can fail in ways that could result in a hazardous situation.

10.2.5.7 Systems incorporating solid-state devices or components

10.2.5.7.1 General

Individual solid-state devices and components are usually extremely reliable although it is possible that the overall reliability of a system could be reduced because of the high number of components sometimes used.

Solid-state devices can be affected by electromagnetic disturbances. It is therefore essential that any control system for machinery safeguarding incorporating solid-state devices ought to have been designed not to be adversely affected by any mains borne or radiated disturbances which can occur in the environment for which it was intended.

10.2.5.7.2 Input and fixed logic stages

In electronic stages, it is often possible to improve the integrity of a single-channel system by employing pulse or modulation techniques, with internal checking, instead of increasing the number of channels.

Where integrated circuits form part of a multi-channel system, any one integrated circuit device should only have been used for one signal-processing channel.

10.2.5.7.3 Programmable logic stages

Programmable logic stages involve solid-state devices which are capable of processing input signals in accordance with a pre-arranged instruction (or program) normally to produce electrical outputs. The same integrity considerations apply as for fixed logic stages.

10.3 Safety-related control systems

10.3 .1 General

Machinery electrical control systems, particularly those that are programmable, often have (incorporate) safety functions that have to be effective during many modes of operation of the machine; and not just for safeguarding.

The system is supposed to have been designed in a manner that reduces the possibility of errors being introduced. The higher the level of integrity required and the more complex the system, the greater the extent of the check.

The increasing complexity of typical programmable electronic systems highlights the difficulties faced by the designer who needs to assure system integrity.

BS EN 62061 is a standard for machinery electrical/electronic/programmable electronic safety-related control systems and implements BS EN 61508 for the machinery sector and ought to have been taken into account by designers and suppliers of new machinery.

10.3.2 Categories of safety-related parts of control systems

BS EN 954-1:1997, Clause 6 specifies five categories of safety-related parts of control systems by using the following in various combinations:

a) sound engineering practice;

b) proven circuit techniques and components;

c) functional testing;

d) redundancy.

These categories are not considered to be truly hierarchical with respect to each other and the control media used.

10.3.3 Safety integrity levels (SILs) of electrical, electronic and programmable electronic control systems

BS EN 62061 specifies the requirements for safety integrity levels 1 to 3 (four safety integrity levels are specified in BS EN 61508). These SIL’s are truly hierarchical; SIL 3 being the highest in safety performance for machine safety control functions.

4.2 BS EN 60204-1:2006, SAFETY OF MACHINERY-ELECTRICAL EQUIPMENT OF MACHINES-PART 1: GENERAL REQUIREMENTS

4.4 Physical environment and operating conditions

4.4.1 General

The electrical equipment shall be suitable for the physical environment and operating conditions of its intended use.

4.4.6 Contaminants

The electrical equipment shall be adequately protected against contaminants (for example dust, acids, corrosive gases, salts) that can be present in the physical environment in which the electrical equipment is to be installed.

4.4.8 Vibration, shock, and bump

Undesirable effects of vibration, shock and bump shall be avoided by the selection of suitable equipment, by mounting it away from the machine, or by provision of anti-vibration mountings.

9 Control circuits and control functions

9.4.2 Measures to minimize risk in the event of failure

9.4.2.1 Use of proven circuit techniques and components

Some of the measures to consider:

1. stopping by de-energizing;
2. switching devices having a direct opening action;
3. circuit design to reduce the possibility of failures causing undesirable operations.

9.4.2.2 Provision of partial or complete redundancy

By providing partial or complete redundancy, it is possible to minimize the probability that one single failure in an electrical circuit can result in a hazardous operation.

9.4.2.3 Provision of diversity

The use of control circuits having different principals of operation, or using different types of components or devices can reduce the probability of hazards resulting from faults and/or failures.

9.4.2.4 Provision for functional tests

Functional tests may be carried out by the control system, or manually by inspection or tests at start-up and at predetermined intervals, or a combination as appropriate.

10 Operator interface and machine mounted control devices

10.1.2 Location and mounting

As far as is reasonably practicable, machine-mounted control devices shall be:

1. readily accessible for service and maintenance;
2. mounted in such a manner to minimize the possibility of damage from activities such as material handling.

10.1.3 Protection

The degree of protection together with other appropriate measures shall afford protection against:

1. the effects of aggressive liquids, vapours, or gases found in the physical environment or used on the machine;
2. the ingress of contaminants (for example swarf, dust, particular matter).

10.1.4 Position sensors

Position sensors shall be so arranged that they will not be damaged in the event of overtravel.

Position sensors in circuits with safety-related control functions shall have direct opening action or shall provide similar reliability.

10.3 Indicator lights and displays

10.3.1 General

Indicator lights and displays shall be selected and installed in such a manner as to be visible from the normal position of the operator.

Indicator light circuits used for warning lights shall be fitted with facilities to check the operability of these lights.

11.3 Degrees of protection

The protection of controlgear against ingress of solid foreign objects and of liquids shall be adequate taking into account external influences under which the machine is intended to operate.

4.3 BS EN 954-1:1997, SAFETY OF MACHINERY-SAFETY RELATED PARTS OF CONTROL SYSTEMS-PART 1. GENERAL PRINCIPLES FOR DESIGN

1 Scope

This European Standard applies to all machinery applications for professional and non-professional use. Also, where appropriate, this standard can be applied to the safety related parts of control systems used in other technical applications.

4 General considerations

4.3 Process for the selection and design of safety measures

This involves 5 steps.

Step 1: Hazard analysis ands risk assessment

- Identify the hazards present at the machine during all modes of operation and at each stage in the life of the machine.

- Assess the risks arising from those hazards and decide on the appropriate risk reduction for that application.

Step 2: Decide measures for risk reduction by control means

- Decide the design measures at the machine and/or the provision of safeguards to provide the risk reduction.

Step 3: Specify safety requirements for the safety-related parts of the control system

- Specify the safety functions to be provided in the control system.

- Specify how the safety functions will be realized and select the category(ies) for each part and combinations of parts within the safety-related parts of the control system.

Step 4: Design

- Design the safety-related parts of the control system according to the specification developed in step 3.

- Verify the design at each stage to ensure that the safety-related parts fulfil the requirements from the previous stage in the context of the specified safety function(s) and category(ies).

Step 5: Validation

- Validate the achieved safety functions and category(ies) against the specification in step 3. Re-design as necessary.

- When programmable electronics are used in the design of safety-related parts of the control systems other detailed procedures are required. At the time this standard was published these procedures were still under consideration.

5 Characteristics of safety functions

5.2 Stop function

A stop function initiated by a protective device shall, as soon as necessary after the actuation, put the machine in a safe state.

5.4 Manual reset

After a stop command has been initiated by a protective device, the stop condition shall be maintained until the manual reset device is actuated and safe conditions for restarting exist.

There is also a list of conditions on the manual reset function.

6 Categories

6.1 General

The safety-related parts of control systems shall be in accordance with the requirements of one or more of the 5 categories specified in 6.2.

6.2 Specification of categories

6.2.1 Category B

This is the basic level. The safety-related parts of the control system shall, as a minimum, be designed, constructed, selected, assembled and combined, in accordance with the relevant standards, using basic safety principles for the specific application. The occurrence of a fault can lead to the loss of the safety function.

6.2.2 Category 1

The requirements of category B, plus the safety-related parts of control systems to category 1 shall be designed and constructed using well-tried components and well-tried safety principles. As with category B, the occurrence of a fault can lead to the loss of the safety function.

6.2.3 Category 2

The requirements of category B, the use of well-tried safety principles plus the safety-related parts of control systems to category 2 shall be designed so that their function(s) are checked at suitable intervals by the machine control system. The occurrence of a fault can lead to the loss of the safety function between checks.

6.2.4 Category 3

The requirements of category B, the use of well-tried safety principles plus the safety-related parts of control systems to category 3 shall be designed so that a single fault in any of these parts does not lead to the loss of the safety function. Accumulation of undetected faults can lead to the loss of the safety function.

6.2.5 Category 4

The requirements of category B, the use of well-tried safety principles plus the safety-related parts of control systems to category 4 shall be designed so that:

1. a single fault in any of these safety-related parts does not lead to a loss of the safety function; and
2. the single fault is detected at or before the next demand upon the safety functions. If detection is not possible, then an accumulation of faults shall not lead to the loss of the safety function.

Annex B (informative)

Guidance for the selection of categories

B.1 General

This annex describes a simplified method based on EN 1050 to select the appropriate categories as reference points for the design of the various safety-related parts of a control system. The guidance given in this annex should be considered as part of the risk assessment given in EN 1050 and not a substitute for it.

Three parameters are used for selecting the category, these are:

1. severity of the injury, S1 slight (normally reversible) injury, S2 Serious (normally irreversible) injury including death
2. frequency and/or exposure time to the hazard, F1 and F2. F2 should be selected if a person is frequently or continuously exposed to the hazard. It is irrelevant whether the same or different persons are exposed to the hazard on successive exposures, e.g. for the use of lifts.
3. possibility of avoiding the hazard, P1 and P2. When a hazardous situation occurs P1 should only be selected if there is a realistic chance of avoiding an accident or of significantly reducing its effect. P2 should be selected if there is almost no chance of avoiding the hazard.

Annex C (informative)

List of some significant faults and failures for various technologies

C.1 Electrical/electronic components

Gives a list of some of the faults/failures that should be considered for electrical/electronic components.

It should be noted that with the ratification of EN ISO 13849-1:2006 there will be a three year transition period during which EN 954-1 can still be used.

4.4 BS EN 1088:1996, SAFETY OF MACHINERY-INTERLOCKING DEVICES ASSOCIATED WITH GUARDS- PRINCIPLES FOR DESIGN AND SELECTION

4 Operating principles and typical forms of interlocking devices associated with guards

4.1 Interlocking principles

4.1.1 Control Interlocking

The stop command from the interlocking device is introduced into the control system so that interruption of the energy supply to the machine actuators, or mechanical disconnection of moving parts from the machine actuators, is triggered by the control system (indirect interruption).

4.1.2 Power interlocking

The stop command from the interlocking device directly interrupts the energy supply to the machine actuators or disconnects moving parts from the machine actuators. 'Directly' means, that unlike control interlocking, the control system does not play any intermediate role in the interlocking function.

5 Provision for the design of interlocking devices

5.1 Actuation modes for mechanically actuated position detectors

When a single detector is used to generate a stop command, it shall be actuated in the positive mode. Non-positive mode actuation is only allowed in conjunction with a detector with positive mode actuation, notably to avoid common cause failures. The design of the actuator should be as simple as possible, since this may reduce the probability of failure.

5.2 Arrangement and fastening of position detectors

5.2.1 Position detectors shall be arranged so that they are sufficiently protected against a change of their position. In order to meet this requirement:

- the fasteners of the position detectors shall be reliable and loosening them shall require a tool;
- the use of slots shall be limited to initial adjustment;
- provision shall be made for positive location after adjustment (e.g. by means of pins or dowels)

Replacement of the detectors shall be possible without any readjusting need.

5.2.2 In addition the following requirements shall be met:

- self-loosening or easy defeat of the detector and of its actuator shall be prevented;
- the support for position detectors shall be significantly rigid to maintain correct operation of the position detector;
- the movement produced by mechanical actuation shall remain within the specified operating range of the position detector to ensure correct operation and/or prevent overtravel;

- the position detector shall be located and, if necessary, protected so that damage from foreseeable external causes is avoided;
- easy access to position detectors for maintenance and checking for correct operation shall be ensured.

5.3 Arrangement and fastening of cams

Rotary and linear cams for mechanically actuating position detectors shall be designed so that:

- they are positively located, and fixed by fasteners requiring a tool for loosening them;
- their self loosening is prevented;
- they can only be mounted in a correct position;
- they do not damage the position detector or impair its durability.

5.4 Reducing the possibility of common cause failure

When switching elements have been made redundant, common cause failures shall be avoided.

5.4.1 Positive and non-positive mode association of mechanically actuated position sensors

Typical causes for failure of mechanically actuated position detectors are:

- excessive wear of the actuator or of the cam;
- misalignment between the cam and actuator
- jamming of the actuator making actuation by the spring impossible.

5.7 Design to minimize defeat possibilities

5.7.1 General

Interlocking devices shall be designed and instructions for their installation and maintenance shall be given so that they cannot be defeated in a simple manner.

5.7.2 Design to minimize defeat of mechanically actuated position detectors

5.7.2.1 Cam-operated position detectors

When a single detector is used, it shall be actuated in the positive mode since, among other characteristics, this mode of actuation prevents the detector from being defeated in a simple manner.

5.7.3 Design to minimize defeat of proximity switches and magnetic switches

Proximity switches and magnetic switches, which rely solely on the presence or absence of detectable material or of a magnet for their actuation, can easily be defeated. Therefore their method of mounting shall give protection against defeat.

Where there is a risk of a substitute actuator being used to defeat the system, an obstruction should be incorporated into the mechanical arrangement to prevent the substitute actuator being used to actuate the switch.

6 Additional technological requirements for electrical interlocking devices

6.1 Compliance with EN 60204-1

Electrical interlocking devices shall comply with EN 60204-1, with particular reference to:

- 11.3 ‘Degrees of protection’ of EN60204-1:2006 for protection against ingress of solids and liquids;
- 10.1.4 ‘Position sensors’ of EN60204-1:2006 for position switches.

6.2 Interlocking devices incorporating mechanically actuated position switches

Where a single position switch is used it should be actuated in the positive mode, where two position switches are used they should operate in opposite modes.

6.3 Interlocking devices incorporating non-mechanically actuated position switches (proximity switches and magnetic switches)

An interlocking device incorporating non-mechanically actuated position switches can be used to overcome problems arising from the use of mechanically operated switches when a guard can be removed completely from a machine and/or the environmental conditions require a sealed switch.

6.3.1 Equivalence with mechanically actuated position switches

When non-mechanically actuated position switches are used, the safety achieved shall not be less than that obtainable with mechanically actuated position switches.

Equivalent safety may be achieved for instance by:

- minimizing the possibility of defeat
- using the techniques described in 4.11 of EN ISO 12100:2003, especially duplication(or redundancy) and automatic monitoring, as well as diversity of design and/or technology to avoid common cause (common mode) failure.

6.3.5 Specific provision for magnetic switches

Magnetic switches used without additional measures, such as overcurrent protection and/or redundancy and automatic monitoring, are generally not suitable for interlocking applications, principally because they can fail to danger. Malfunction by vibration shall be prevented.

7 Selection of an interlocking device

7.1 General

The aim of this clause is to advise machine designers and type C standard makers on how to select an interlock device suitable for a specific application.

In selecting an interlock device for a machine, it is necessary to consider all phases of the interlock device life cycle.

The most important selection criteria are:

- the conditions of use and the intended use of the machine
- the hazard present at the machine
- the severity of the possible injury
- the probability of failure of the interlock device
- stopping time and access time considerations
- the frequency of access
- the duration of person exposure to the hazard(s)
- performance considerations

Further guidance on all of the above criteria is given in individual sections for each topic.

Annex J (informative) Electrical interlocking device incorporating magnetically actuated (magnetic) switches

Advantages	Disadvantages
Compact, no external moving parts.	Sensitive to electromagnetic interference.
High resistance to dust, liquids.	No positive opening of contacts
Easily kept clean.	Possible contact welding in case of overcurrent.

Remarks

The disadvantages quoted above make it necessary for the magnetic switches to be automatically checked at each switching cycle, and for overcurrent protection to be provided.

The device is designed so as to require a coded magnet in order to be actuated. This prevents it from being defeated in a simple manner.

4.5 EN ISO 13849-1:2006, SAFETY OF MACHINERY-SAFETY-RELATED PARTS OF CONTROL SYSTEMS-PART 1: GENERAL PRINCIPLES FOR DESIGN

This is a recently ratified standard that replaces EN 954-1:1997. The safety categories in EN 954-1 are replaced by Performance Levels. These are determined by a similar type of 'risk graph' used for the safety categories in EN 954-1.

The standard takes a four-stage approach to the design of a safety-related control system:

1. risk assessment;
2. for the identified risks, allocate Performance Level(PL);
3. devise a system that is suitable for the performance level;
4. validate the design to check it meets the requirements of the risk assessment.

Step 4 involves the use of manufactures data for the reliability of the components.

4 Design considerations

4.3 Determination of required performance level (PL_r)

There are 5 levels a to e, with a being the least stringent.

For each selected safety function to be carried out by a safety-related part of a control system, a required performance level shall be determined and documented. The determination of the required performance level is the result of the risk assessment and refers to the amount of the risk reduction to be carried out by the safety-related parts of the control system. Annex A of the standard provides guidance on determining PL_r.

In standards in accordance with EN 61508, the ability of safety-related control systems to perform a safety function is given through a SIL. The relationship between the two concepts PLs and SILs) is given in table 4 in the standard.

4.6 Software safety requirements

4.6.1 General

All lifecycle activities of safety-related embedded or application software shall primarily consider the avoidance of faults introduced during the software lifecycle. The main objective of the following requirements is to have readable, understandable, testable and maintainable software.

4.6.2 Safety-related embedded software (SRESW)

This section gives lists of the basic measures that have to be applied for the SRESW to meet the required performance level (PL_r), a to e for the application.

4.6.3 Safety-related application software (SRASW)

This section gives lists of the basic measures that have to be applied for the SRASW to meet the required performance level (PL_r), a to e for the application. For SRASW for components with

PL_r from c to e there are a number of additional measures with increasing efficiency (lower effectiveness for PL_r of c, medium effectiveness for PL_r of d, higher effectiveness for PL_r of e) are required or recommended.

Embedded software is supplied by the control manufacturer and is not accessible for modification by the user of the machinery. Typically, micro controllers, application specific integrated circuits (ASIC's) and read only memory (ROM) are embedded devices. Application software would be found in programmable logic controllers (PLC's) and computers.

5 Safety functions

Requirements are similar to those of EN 954.

6 Categories and their relation to $MTTF_d$[1] of each channel, DC_{avg}[2] and CCF[3]

6.2 Specification of categories

6.2.3 Category B

Requirements are the same as that of EN 954.

The maximum PL achievable with category B is PL = b.

6.2.4 Category 1

Requirements are the same as that of EN 954, but there is additional information on "well tried component" with reference to the suitability being dependant on the application and an example of additional safety measures that may be necessary outside the control system.

The maximum PL achievable with category 1 is PL = c.

6.2.5 Category 2

Requirements are the same as that of EN 954.

The maximum PL achievable with category 2 is PL = d.

6.2.6 Category 3

The requirements are the same as that of EN 954 except that in EN 954 significant common mode faults are taken into account. This standard refers to diagnostic coverage (DC), which uses failure mode and effects analysis (FMEA), to ensure that all relevant faults and/or failure modes are considered.

6.2.7 Category 4

The requirements are the same as that of EN 954 except for this standard states, "The diagnostic coverage (DC_{avg}) of the total SRP/CS shall be high, including the accumulation of faults. The $MTTF_d$ of each of the redundant channels shall be high. Measures against CCF shall be applied".

Neither category 3 or 4 has a defined maximum achievability of a PL.

---

[1] *Mean time to dangerous failure*
[2] *Diagnostic coverage*
[3] *Common cause failure*

7 Fault consideration, fault exclusion

7.1 General

In accordance with the category selected, safety related parts shall be designed to achieve the required performance level (PL_r). The ability to resist faults shall be assessed.

7.2 Fault consideration

EN ISO 13849-2 lists the important faults and failures for the various technologies. The lists of faults are not exclusive and, if necessary, additional faults shall be considered and listed. In such cases, the method of evaluation should also be clearly elaborated. For new components not mentioned in EN ISO 13849-2, a failure mode and effects analysis (FMEA, see IEC 60812) shall be carried out to establish the faults that are to be considered for those components.

In general, the following fault criteria shall be taken into account:

- if as a consequence of a fault, further components fail, the first fault together with all the following faults shall be considered as a single fault;
- two or more single faults having a common cause shall be considered as a single fault (known as a CCF);
- the simultaneous occurrence of two or more faults having separate causes is considered highly unlikely and therefore need not be considered.

7.3 Fault exclusion

It is not always possible to evaluate SRP/CS without assuming that certain faults can be excluded. For detailed information on fault exclusion, see EN ISO 13849-2.

Fault exclusion can be based on

- the technical improbability of occurrence of some faults
- generally accepted technical experience, independent of the considered application, and
- technical requirements related to the application and specific hazard.

Detailed justification has to be documented for any faults that are excluded.

Annex A (informative)

Determination of required performance level (PL_r)

Provides guidance on selecting parameters S (severity of injury), F (frequency and/or exposure time to hazard) and P (possibility of avoiding the hazard) for the risk estimation.

Annex F (informative)

Estimates for common cause failure (CCF)

BS EN 61508-6:2002 Annex D provides a comprehensive procedure for measures against CCF for sensors/actuators and separately for control logic, but not all measures given are applicable to the machinery site. The most important measures are included in this Annex.

Annex I (informative)

Examples

Provides examples for a single-channel system and a redundant system.

4.6 EN ISO 13849-2:2003, SAFETY OF MACHINERY-SAFETY-RELATED PARTS OF CONTROL SYSTEMS-PART 2: VALIDATION

8 Validation of environmental requirements

The performance specified in the design for the safety-related parts of the control system shall be validated with respect to the environmental conditions specified for the control system.

Where applicable validation shall address:

- expected mechanical stresses from shock, vibration, ingress of contaminants;
- mechanical durability
- electrical ratings and power supply;
- climatic conditions (temperature and humidity);
- electromagnetic compatibility (immunity).

Annex D (informative)

Validation tools for electrical systems

This annex contains guidance on the basic safety principles, well-tried safety principles and well-tried components required to establish the category B,1,2,3 or 4 in Section 6 of EN ISO 13849-1:2006.

This annex also includes fault lists and fault exclusions for a range of assemblies and components.

4.7 BS EN 62061:2005, SAFETY OF MACHINERY-FUNCTIONAL SAFETY OF SAFETY-RELATED ELECTRICAL, ELECTRONIC AND PROGRAMMABLE ELECTRONIC CONTROL SYSTEMS

This standard is machine sector specific within the framework of IEC 61508. It is intended to facilitate the specification of the performance of safety-related electrical control systems (SRECS) in relation to the significant hazards of machines.

This standard contains a great deal of information, but is probably only applicable to a new installation as it would most likely be very difficult to back engineer all the documentation required. An indication of the requirements of each clause is given below, however the standard should be read to gain the full detail.

3.2 Terms and definitions

3.2.3 Electrical control system

All the electrical, electronic and programmable electronic parts of the machine control system used to provide, for example, operational control, monitoring, interlocking, communications, protection and safety-related control functions.

3.2.4 Safety-Related Electrical Control System

SRECS

Electrical control system of a machine whose failure can result in an immediate increase of the risk(s)

4 Management of functional safety

4.2 Requirements

4.2.1 A functional safety plan shall be draw up and documented for each SRECS design project, and shall be updated as necessary. The plan shall include procedures for control of the activities specified in clauses 5 to 9.

5 Requirements for the specification of Safety-Related Control Functions (SRCFs)

5.1 Objective

This clause sets out the procedures to specify the requirements of SRCF(s) to be implemented by the SRECS

6 Design and integration of the safety-related electrical control system (SRECS)

6.1 Objective

This clause specifies requirements for the selection or design of a SRECS to meet the functional safety integrity requirements specified in the safety requirements specification (clause 5)

The sections 6.2 to 6.13 contain a great deal of information which is difficult to condense, the list of headings indicates the topic covered.

6.2 General requirements

6.3 Requirements for behaviour (of the SRECS) on detection of a fault in the SRECS

6.4 Requirements for systematic safety integrity of the SRECS

6.5 Selection of safety-related electrical control system

6.6 Safety-related electrical control system design and development

6.7 Realisation of subsystems

6.8 Realisation of diagnostic functions

6.9 Hardware implementation of the SRECS

6.10 Software safety requirements specification

6.11 Software design and development

6.11.3 Application software design and development

Note This subclause is based on IEC 61508-3

6.12 Safety-related electrical control system integration and testing

6.13 SRECS installation

7 Information for use of the SRECS

7.1 Objective

Information on the SRECS shall be provided to enable to enable the user to develop procedures to ensure that the required functional safety of the SRECS is maintained during use and maintenance of the machine.

8 Validation of the safety-related electrical control system (SRECS)

8.2 General requirements

8.2.1 The validation of the SRECS shall be carried out in accordance with a prepared plan (this includes both hardware and software).

Annex A (informative)

SIL assignment

A1 General

This informative Annex provides one example of a qualitative approach for risk estimation and SIL assignment that can be applied to Safety-Related Control Functions (SRCFs) for machines. Examples of other techniques that may be used for SIL assignment are given in IEC 61508-5.

Note 2 In a large number of machine specific standards (“C” type standards in CEN) risk estimation has been carried out to select a required Category in accordance with ISO 13849-

1:1999 for safety related parts of machine control systems. It is noted that for simplification, the following relationships are commonly used:

- required category 1 to required SIL1
- required category 2 to required SIL1
- required category 3 to required SIL2
- required category 4 to required SIL3

A2 Risk estimation and SIL assignment

The risk related to the identified hazard	=	the severity of the possible harm	and	the probability of the occurrence of harm

The probability of the occurrence of harm has three parameters, frequency and duration of exposure (Fr), probability of occurrence of a hazardous event (Pr) and probability of avoiding or limiting harm (Av). These parameters should be estimated independently of each other. A worst-case assumption needs to be used for each parameter to ensure that SRCF(s) are not incorrectly assigned a lower SIL than is necessary.

4.8 BS EN ISO 12100-2:2003, SAFETY OF MACHINERY- BASIC CONCEPTS, GENERAL PRINCIPLES FOR DESIGN – PART 2: TECHNICAL PRINCIPLES

This document supersedes EN 292-2:1991.

4.11 Applying inherently safe design measures to control systems

4.11.1 General

In order to prevent hazardous machine behaviour and to achieve safety functions, the design of control systems shall comply with the principles and methods presented in this subclause 4.11 and in 4.12. These principles and methods shall be applied singly or in combination as appropriate to the circumstances (see ISO 13849-1 and IEC 60204-1:1997, clauses 9 to 12).

4.11.7 Safety functions implemented by programmable electronic control systems

4.11.7.1 General

The programmable electronic control system should be installed and validated to ensure that the specified performance (e.g. safety integrity level (SIL) in IEC 61508 series) for each safety function has been achieved.

4.11.7.2 Hardware aspects

The hardware (including e.g. sensors, actuators, logic solvers) shall be selected (and/or designed) and installed to meet both the functional and performance requirements of the safety functions to be performed.

4.11.7.3 Software aspects

The software (including internal operating software (or system software) and application software) shall be designed so as to satisfy the performance specification for the safety functions (see also IEC 61508-3).

4.11.7.4 Application software

Application software should not be re-programmable by the user. This may be achieved by use of embedded software in a non re-programmable memory (e.g. micro-controller, application specific integrated circuit (ASIC)).

When the application requires reprogramming by the user, the access to the software dealing with safety functions should be restricted.

4.11.12 Provision of diagnostic systems to aid faultfinding

Diagnostic systems to aid faultfinding should be included in the control system so that there is no need to disable any protective measure.

4.12 Minimizing the probability of failure of safety functions

The continued operation of the safety function is essential for the safe use of the machine. This can be achieved by:

4.12.1 Use of reliable components

“Reliable components” means components which are capable of withstanding all disturbances and stresses associated with the usage of the equipment in the conditions of intended use (including the environmental conditions), for the period of time or the number of operations fixed for the use, with a low probability of failures generating a hazardous malfunction of the machine.

Note 1 “Reliable components” is not a synonym for “well-tried components”.

Note 2 Environmental conditions which are to be taken into considerations are, for instance: impact, vibration, cold, heat, moisture, dust, corrosive and/or abrasive substances, static electricity, magnetic and electric fields.

4.12.2 Use of “orientated failure mode” components

“Orientated failure mode” components or systems are those in which the predominant failure mode is known in advance and which can be used so that such a failure leads to a non-hazardous alteration of the machine function.

The use of such components should always be considered, particularly in cases where redundancy is not employed.

4.12.3 Duplication (or redundancy) of components or subsystems

In the design of safety-related parts of the machine, duplication (or redundancy) of components may be used so that, if one component fails, another component (or components) continue(s) to perform its (their) function, thereby ensuring that the safety function remains available.

In order to allow proper action to be initiated, component failure shall be preferably detected by automatic monitoring or in some circumstances by regular inspection, provided that the inspection interval is shorter than the expected lifetime of the components.

Diversity of design and/or technology can be used to avoid common cause failures (e.g. from electromagnetic disturbance) or common mode failures.

5 Safeguarding and complementary protective measures

5.3 requirements for the design of guards and protective devices

5.3.3 Technical characteristics of protective devices

Protective devices shall be selected or designed and connected to the control system so as to ensure correct implementation of their safety function(s).

Protective devices shall be either selected as meeting the appropriate product standard or designed according to one or several of the principles formulated in ISO 13849-1

Protective devices shall be installed and connected to the control system so that they cannot be easily defeated.

4.9 BS EN 61508:2002, FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS

Part 3: Software requirements

1 Scope

Safety-related software includes operating systems, system software, software in communication networks, human-computer interface functions, support tools and firmware as well as application programs.

7.2 Software safety requirements specification

7.2.2.9 To the extent required by the description of the electrical/electronic/programmable electronic **(**E/E/PE) hardware architecture design, the software safety requirements specification shall consider the following:

1. software self-monitoring (for examples see C.2.5 and C.3.10 of IEC 61508-7);
2. monitoring of the programmable electronics hardware, sensors, and actuators;
3. periodic testing of the safety functions while the system is running;
4. enabling safety functions to be testable when the equipment under control (ECU) is operational.

7.4 Software design and development

7.4.2 General requirements

7.4.2.2 In accordance with the required safety integrity level, the design method chosen shall possess features that facilitate:

a) abstraction, modularity and other features that control complexity;

b) the expression of:

- functionality,
- information flow between components,
- sequencing and time related information,
- timing constraints,
- data structures and their properties,
- design assumptions and their dependencies;

c) comprehension by developers and others who need to understand the design;

d) verification and validation.

7.4.4 Requirements for support tools and programming languages

7.4.4.3 To the extent required by the safety integrity level, the programming language selected shall:

a) have a translator/compiler which has either a certificate of validation to a recognised national or international standard, or it shall be assessed to establish its fitness for purpose;

b) be completely and unambiguously defined or restricted to unambiguously defined features;

c) match the characteristics of the application;

d) contain features that facilitate the detection of programming mistakes;

e) support features that match the design method.

7.4.6 Requirements for code implementation

7.4.6.1 The source code shall

a) be readable, understandable and testable;

b) satisfy the specified requirements for software module design;

c) satisfy the specified requirements of the coding standard;

d) satisfy all relevant requirements specified during safety planning.

7.4.7 Requirements for software module testing

7.4.7.1 Each software module shall be tested as specified during software design.

7.4.7.2 These tests shall show that each software module performs its intended function and does not perform unintended functions.

7.8 Software modification

7.8.2 Requirements

7.8.2.1 Prior to carrying out any software modification, software modification procedures shall be made available.

7.8.2.2 A modification shall be initiated only on the issue of an authorised software modification request under the procedures specified during safety planning which details the following

a) the hazards which may be affected;

b) the proposed change;

c) the reason for the change.

7.8.2.6 The safety planning for modification of safety-related software shall include the following information:

a) identification of staff and specification of their required competency;

b) a detailed specification for the modification;

c) verification planning;

d) scope of revalidation and testing of the modification to the extent required by the safety integrity level.

7.9 Software verification

7.9.2.7 subject to 7.1.2.1, the following verification activities shall be performed:

a) verification of software safety requirements;

b) verification of software architecture;

c) verification of software system design;
d) verification of software module design;
e) verification of code;
f) data verification;
g) software module testing;
h) software integration testing;
i) programmable electronics integration testing;
j) software safety requirements testing (software validation).

Sections 7.9.2.8 to 7.9.2.13 give additional information on the requirements of a) to f) above.

5 CONCLUSION

There are no specific standards for control system design and safety switch selection, for the prevention/detection of shaft intrusions. New standards follow the BS EN 61508:2002 series approach, applying a safety integrity level to the machine, which the control system and safety switches have to meet. Whilst there will be difficulties in trying to back engineer a 20+ year old system to comply fully with this approach it should be possible to identify any areas that do not follow best practice.

The standards and guidance reviewed may not be exhaustive, but the information between documents on a particular subject is consistent.

For a safety related control system to be reliable/effective for this particular application the following recommendations should be used as a minimum with addition detail being obtained from the specific section of a standard for a particular area:

Recommendations

- Identify and assess the hazard and then select an appropriate Safety Integrity Level (SIL) for the risk control functions of the equipment;
- Ensure that all mechanically-actuated position switches are actuated in the positive mode.
- Ensure that all hardware is suitable for the environment in which it is to operate, in particular with respect to resistance to corrosive liquids, ingress of dust and the ability to withstand impact damage;
- Provide additional measures to prevent/detect failure where magnetic and proximity type safety switches are used.

In accordance with the selected SIL:

- Employ redundancy and diversity to avoid common cause failure, where necessary, to achieve and maintain the SIL;
- Ensure suitable measures are taken to prevent inadvertent or deliberate alteration if a safety related control system is capable of being re-programmed;
- Ensure Safety related software is self-monitoring;
- Ensure that the decision making process for implementation of a new system or modification of an existing system, is suitably documented in a transparent, traceable and comprehensible way and this documentation is retained and available for the purpose of external assessment and validation.

6 APPENDICES

Guidance on the selection and use of electrical safety switches and safety related control systems for use in mine shaft and winding systems

Component	Action	Requirements	Guidance / Standard	Meets requirements Y/N
Position Sensor General	Suitable for a safety related application.	Devices ought to have been selected only from those where the performance, as stated by the manufacturer, is suitable for the specific safety application. Performance data that should be considered:	PD 5304:2005, 9.6.1 BS EN 1088:1996, 6.3 BS EN 60204-1:2006, 4.4 EN ISO 13849-2:2003, 8 BS EN ISO 12100-2:2003, 14.12 Note 2	
		Resistance to environmental conditions (IP rating), corrosion resistance, vibration resistance, electromagnetic disturbances.		
		Life evaluation.		
		Duty rating.		
		Reliability.		
	Mounting of sensors	The fasteners of the position detectors shall be reliable and loosening them shall require a tool	BS EN 1088:1996, 5.2	
		The use of slots shall be limited to initial adjustment		
		Provision shall be made for positive location after adjustment (e.g. by means of pins or dowels).		
		Replacement of the detectors shall be possible without any readjusting need.		

Component	Action	Requirements	Guidance / Standard	Meets requirements Y/N
Position Sensor General	Mounting of sensors	The position detector shall be located and, if necessary, protected so that damage from foreseeable external causes is avoided.	BS EN 1088:1996, 5.2	
		Easy access to position detectors for maintenance and checking for correct operation shall be ensured.		
Cam Operated Position Sensor	Design to minimize defeat possibilities	Positive acting. Direct mechanical connection of actuator to switch, which forces an open circuit for an unsafe condition. (Direct opening action)	PD 5304:2005, 9.6.2 BS EN 1088:1996, 6.2 BS EN 60204-1:2006, 10.1.4	
	Mounting of cams	Rotary and linear cams for mechanically actuating position detectors shall be designed so that:	BS EN 1088:1996, 5.3	
		They are positively located, and fixed by fasteners requiring a tool for loosening them.		
		Their self loosening is prevented.		
		They can only be mounted in a correct position.		
		They do not damage the position detector or impair its durability.		

Component	Action	Requirements	Guidance / Standard	Meets requirements Y/N
Cam Operated Position Sensor	Failure	Mechanical arrangements for actuating position sensors should be such that the roller and cam or other device is adequately proportioned and made of appropriate material to withstand wear which might lead to ineffective actuation of the position switch	PD 5304:2005, 10.2.2.2	
Non-mechanically activated Position Sensor	Equivalence with mechanically actuated position sensor	Safety achieved shall not be less than that obtained with mechanically actuated position sensors.	BS EN 1088:1996, 6.3.1 EN ISO 12100:2003, 4.11 BS EN 60204-1:2006, 9.4.2.2, 9.4.2.3	
		Minimising the possibility of defeat		
		Using techniques such as, duplication (or redundancy) and automatic monitoring as well as diversity of design and/or technology to avoid common cause failure.		
Proximity Position Sensor	Design to minimize defeat possibilities	Proximity sensors designed for safety interlocking should have a coded, complementary target. Switches which rely solely on the presence or absence of metal for their actuation are not suitable for safety interlocking.	PD 5304:2005, 9.6.6 BS EN 1088:1996, 5.7.3	
Magnetic Position Sensor	Design to minimize defeat possibilities	Use of a coded magnet in order to be actuated.		

Component	Action	Requirements	Guidance / Standard	Meets requirements Y/N
Magnetic Position Sensor	Failure	Magnetic reed switches can fail to danger and require additional measures.	BS EN 1088:1996, 6.3.5 Annex J	
		Overcurrent protection		
		Redundancy		
		Automatic monitoring		
		Malfunction by vibration shall be prevented.		
Control Systems	Common Cause Failures	It is advantageous to design dual control systems so that similar failures in both channels from the same cause are minimised.	PD 5304:2005, 10.1	
	Redundancy	By providing partial or complete redundancy, it is possible to minimize the probability that one single failure in an electrical circuit can result in a hazardous operation	BS EN 60204-1:2006, 9.4.2.2 BS EN ISO 12100-2:2003, 4.12.3	
	Diversity	The use of control circuits having different principals of operation, or using different types of components or devices can reduce the probability of hazards resulting from faults and/or failures.	BS EN 60204-1:2006, 9.4.2.3 BS EN ISO 12100-2:2003, 4.12.3	
	Stop Function	A stop function initiated by a protective device shall, as soon as necessary after the actuation, put the machine in a safe state	BS EN 954-1:1997, 5.2	
	Manual Reset	After a stop command has been initiated by a protective device, the stop condition shall be maintained until the manual reset device is actuated and safe conditions for restarting exist.	BS EN 954-1:1997, 5.3	

Component	Action	Requirements	Guidance / Standard	Meets requirements Y/N
Control Systems	Power Failure	Components relying on the power supply for their functioning should be installed so that power loss minimizes failure to danger of the system as a whole.	PD 5304:2005, 10.2.2	
	Hardware / Software Failure	Complexity of safety control system is driven by the safety integrity level calculated for the operation.	PD 5304:2005, 10.2 BS EN 954-1:1997, 6 EN ISO 13849-1:2006, 6	
		Where higher safety integrity levels are required the software should be self-monitoring and the hardware monitored for correct operation.		
	Documentation	These references indicate information that has to be documented to comply with that standard. These include: decision making processes, implementation, modifications, specification, validation and verification plans, contents of documentation and examples.	EN ISO 13849-1:2006, 10 EN ISO 13849-2:2003, 3.5 – Table 2 BS EN 62061:2005, 7.2, 8, 9, 10, Table 8 BS EN 954-1:1997, 4.2, 8.1 BS EN 60204-1:2006, 18 BS EN 61508-1: 2002, 5, Annex A BS EN 61508-2: 2002, 7 BS EN 61508-7: 2002, B1.2	

Component	Action	Requirements	Guidance / Standard	Meets requirements Y/N
Software	Program or sequence control	A hazard analysis and risk assessment ought to be carried out to establish the full implications of a program error.	PD 5304:2005, 5.3.7	
	Prevention of inadvertent or deliberate alteration	Program storage in read only memory (ROM)	PD 5304:2005, 5.23 EN 62061:2005, 6.11.3.2.2	
		Password access to software		
	Documentation	These references indicate information that has to be documented to comply with that standard. These include: decision making processes, implementation, modifications, specification, validation and verification plans, contents of documentation and examples.	EN ISO 13849-1:2006, 10 BS EN 60204-1:2006, 11.3.4 BS EN 62061:2005, 7.2, 8, 9, 10, Table 8 BS EN 61508-1: 2002, 5, Annex A BS EN 61508-3: 2002, 5 BS EN 61508-7: 2002, B1.2	

7 REFERENCES

PD5304:2005, Guidance on the safe use of machinery.

BS EN 60204-1:2006, Safety of machinery-Electrical equipment of machines-Part 1: General requirements.

BS EN 954-1:1997, Safety of machinery-Safety related parts of control systems-Part 1. General principles for design.

BS EN 1088:1996, Safety of machinery-Interlocking devices associated with guards-Principles for design and selection.

EN ISO 13849:2006, Safety of machinery-Safety-related parts of control systems
Part 1: General principles for design
Part 2: Validation.

BS EN 62061:2005, Safety of machinery-Functional safety of safety-related electrical, electronic and programmable electronic control systems.

BS EN ISO 12100-2:2003, Safety of machinery- Basic concepts, general principles for design.

BS EN 61508:2002, Functional safety of electrical/electronic/programmable electronic safety-related systems, parts0-7.