SAFETY RELATED CONTROL SYSTEMS

In a previous article we discussed the issues relating to machine safety systems focusing mainly on the PUWER regulations and risk assessments. In this issue will take this subject a step further and explain some of the control system principles that can be applied to equipment often found in today's milling environment.

Mill operators should be well aware of the importance of complying with British and International safety standards in order to ensure continued functionality of equipment and safety for users. This means that during the operation of machinery users must be fully protected from access to the moving parts and within modern automatic production facilities this protection is built in to the control system.

Safety Principles

Choice of Protective Measures
When the risk assessment shows that a machine or process carries a risk of injury the hazard must be eliminated or contained. The manner in which this is achieved will depend on the nature of the machine and the hazard. In basic terms this means preventing any access to the relevant parts while they are in a dangerous condition.

The best choice of protective measure is a device or system that provides the maximum protection with the minimum hindrance to normal machine operation. It is important that all aspects of machine use are considered, as experience shows that a system, which is difficult to use, is more liable to be removed or by-passed.

To achieve this there is a choice of either:

1. Preventing access during dangerous motion or

2. Preventing dangerous motion during access.

The following gives a brief overview of the characteristics of the most commonly used devices.

Fixed Enclosing Guards
If the hazard is on a part of the machinery, which does not require access, it should be permanently guarded with fixed enclosing guards.

Movable Guards with Interlocking Switches
If access is required there must be a movable guard, which is interlocked with the power source of the hazard in a manner, which ensures that whenever the guard door is not closed the hazard power will be switched off. This approach involves the use of an interlocking switch fitted to the guard door. The control of the power source of the hazard is routed through the switch section of the unit. The power source is usually electrical but it could also be pneumatic or hydraulic. When guard door movement (opening) is detected the interlocking switch will isolate the hazard power supply either directly or via a power contactor (or valve).

Some interlocking switches also incorporate a locking device that locks the guard door closed and will not release it until the machine is in a safe condition. For the majority of applications the combination of a movable guard and an interlock switch with or without guard locking is the most reliable and cost effective solution.

Two-Hand Controls
The use of two-hand controls is a common method of preventing access while a machine is in a dangerous condition. Two start buttons must be operated at the same time to run the machine.

This ensures that both hands of the operator are occupied in a safe position and therefore cannot be in the hazard area.

Preventing Dangerous Motion
When frequent access is required physical guarding at the hazard is sometimes too restrictive for part loading or adjustment. In this situation a device is required to prevent dangerous motion while allowing unrestricted access by sensing the presence of the operator and isolating the power source.

Photoelectric Light Curtains
These devices emit a “curtain” of harmless infrared light beams in front of the hazard area. When any of the beams are blocked by intrusion towards the hazard area the light curtain control circuit switches off the hazard power source. Light curtains are extremely versatile and can guard areas many meters wide. Through the use of mirrors the light beams can be diverted around corners to enclose a machine. They are available with different light beam spacings making them suitable for applications ranging from perimeter guarding for industrial robots to point of access guarding on presses and shears.

Pressure Sensitive Safety Mats
These devices are used to provide guarding of a floor area around a machine. A matrix of interconnected mats is laid around the hazard area and any pressure (e.g., an operator’s footstep) will cause the mat controller unit to switch off power to the hazard.

Pressure Sensitive Edges
These devices are flexible edging strips that can be mounted to the edge of a moving part, such as a machine table or powered door, that poses a risk of a crushing or shearing. If the moving part strikes the operator (or vice versa), the flexible sensitive edge is depressed and will switch off the hazard power source. Sensitive edges can also be used to guard machinery where there is a risk of operator entanglement. If an operator becomes caught in the machine, contact with the sensitive edge will shut down machine power. Light curtains, floormats and sensitive edges can all be classified as “trip devices.” They do not actually restrict access but only “sense” it. They rely entirely on their ability to both sense and switch for the provision of safety: it is important that their control circuit incorporates self-monitoring and fail-safe measures. In general they are only suitable on machinery, which stops reasonably quickly after switching off the power source.

Emergency Stop Devices
Wherever there is a danger of an operator getting into trouble on a machine there must be a facility for fast access to an emergency stop device. The e-stop device must be continuously operable and readily available. Each operator panel must contain at least one e-stop device. Additional e-stop devices may be used at other locations as needed. E-Stop devices come in various forms. Pushbutton switches and cable pull switches are examples of the more popular type devices. When the e-stop device is actuated, it must latch in and it must not be possible to generate the stop command without latching in. The resetting of the emergency stop device must not cause a hazardous situation. A separate and deliberate action must be used to re-start the machine.

Safety Related Control Systems

A safety related control system is the part of a machine that prevents hazardous condition from occurring. It can be a separate dedicated system or integrated with the normal machine control system.

So how do we design a system to achieve this, the standard ISO 13849-1 “Safety related parts of control systems” deals with these aspects. It explains the criteria for five categories for benchmarking and describing the performance of the control system. Category 1 is aimed at the prevention of faults; Categories 2, 3 and 4 require that if faults cannot be prevented they must be detected. The categories can be summarized as follows,

Category B

In itself has no special measures for safety but it forms the base for other categories. Safety related parts of machine control system and/or their protective equipment, as well as their components, shall be designed, constructed, selected, assembled and combined in accordance with relevant standards so that they can withstand the expected influence. When a fault occurs it can lead to a loss of the safety function.

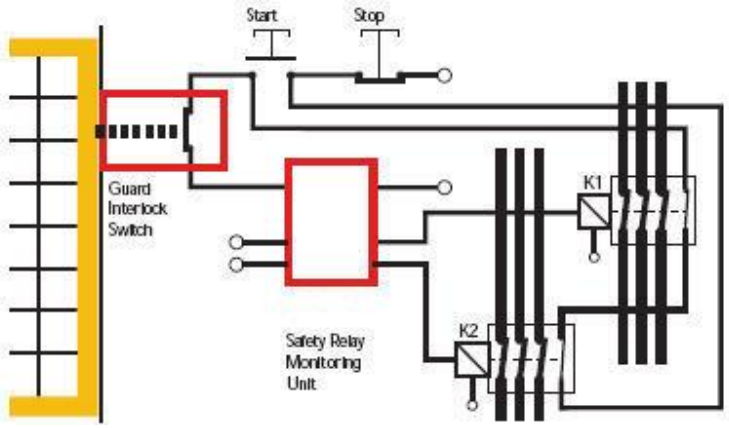

Figure 1

Category 1

Category B and Category 1 are applied together with the use of well-tried safety components and safety principles. This combination has a higher safety related reliability and less likelihood of a fault.

Figure 1 shows a simple safety related control circuit. The interlock device has positive mode operation and satisfies the requirements of category 1. The contactor is correctly selected for its duty and is designed and manufactured to specific standards. The part of the system most prone to a fault is the connecting wiring. In order to overcome this, the wiring should be installed in accordance with the relevant clauses of IEC 60204-1. It should be routed and protected in a manner that prevents any foreseeable short circuits or ground faults. This system will satisfy the requirements of category 1.

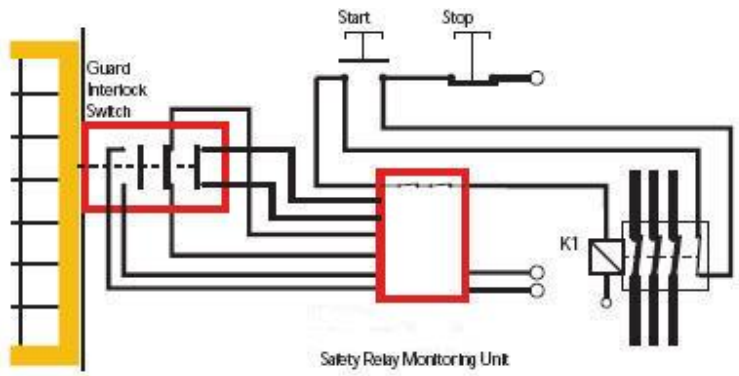

Figure 2

Category 2
Category B and Category 2 are applied together with the use of well-tried safety principles. This combination leads to safety function(s) check at machine start-up and periodically by the machine control system. If a fault is detected a safe state shall be initiated or if this is not possible a warning shall be given. Any loss of safety function is detected by the check but the occurrence of a fault between the checking intervals could lead to the loss of safety function.

Figure 2 shows a system, which satisfies the requirements of category 2 and therefore must undergo a test of the safety function before the machine can be started. It must also be tested periodically. At initial power up the Safety relay will not allow switching of power to the contactor until the guard is opened and closed. This initiates a check for any single faults in the circuit from the switch to the Safety relay. Only when this check is successful will the contactor be energized. At every subsequent guard operation the circuit will be similarly checked.

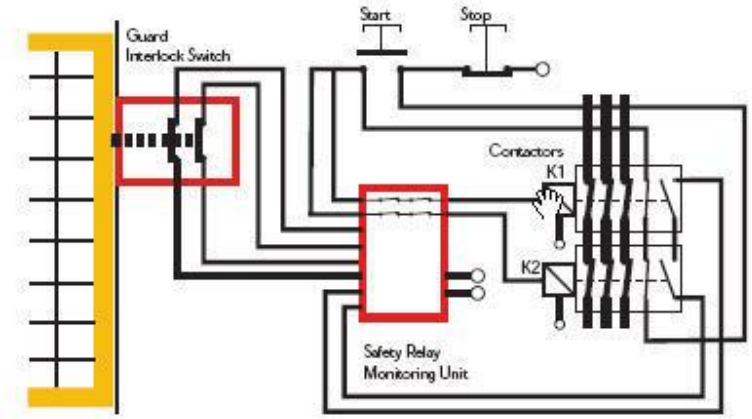

Figure 3

Category 3
Category B and Category 3 are applied together with the use of well-tried safety principles. The system is designed so that a single fault in any of its parts does not lead to loss of safety function. When the single fault occurs the safety function is always performed. Some but not all faults will be detected. An accumulation of undetected faults can lead to the loss of safety function.

Figure 3 shows a system that satisfies the requirements of category 3 and is often suitable for applications with higher risk estimations. It is a dual channel system that is fully monitored, including the two contactors. On opening and closing the guard, any single dangerous fault will cause the safety relay to lock off power to the contactors until the fault is corrected and the Safety relay is reset.

Category 4
Category B and Category 4 are applied together with the use of well-tried safety principles. The system shall be designed so that a single fault in any of its parts does not lead to loss of safety function. The single fault is detected at or before the next demand on the safety function. If this detection is not possible then an accumulation of faults shall not lead to a loss of safety function. When the faults occur the safety function is always performed. The faults will be detected in time to prevent the loss of safety functions.

Category 4 requires that the safety system function is still provided even with an accumulation of undetected faults. The most practicable way of achieving this is to employ continuous or high frequency monitoring techniques. This is not feasible with most mechanical or electro-mechanical components (e.g., mechanical switches, relays, contactors) such as those used in interlocking

and emergency stop systems. These techniques are viable (and often used) to monitor solid-state electronic components because a high frequency change of state is possible and does not substantially degrade the life of the component. Therefore the category 4 approach is often found in self-contained “sub-systems” such as light curtains.