

Company - MAYKIT WRIGHT LTD

Facility - Tool room - East Factory.

Date - 29/8/95

Operator profile - Apprentice / Fully skilled.

Equipment identity & date	Directive Conformity	Risk Assmnt Report no.	Accident history	Notes	Hazard identity	Hazard type	Action required	Implemented & inspected - reference
Bloggs centre lathe. Serial no. 8390726 Installed 1978	None claimed	RA302	None	Electrical equipment complies with BS EN 60204 E stops fitted (replaced 1989)	Chuck rotation with guard open.	Mechanical Entanglement Cutting	Fit guard interlock switch	25/11/94 J Kershaw Report no 9567
					Cutting fluid	Toxic	Change to non toxic type	30/11/94 J Kershaw Report no 9714
					Swarf cleaning	Cutting	Supply gloves	30/11/94 J Kershaw Report no 9715
Bloggs turret head milling m/c Serial no 17304294 Manuf 1995 Installed May 95	M/c Dir. EMC Dir	RA416	None		Movement of bed (towards wall)	Crushing	Move machine to give enough clearance	13/4/95 J Kershaw Report no 10064

Fig. 31

Chapter 5

SAFETY RELATED CONTROL SYSTEMS

First of all what is a safety related control system? (often abbreviated to SRCS).

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

Its complexity will vary from a typical simple system, such as a guard door interlock switch and emergency stop switch connected in series to the control coil of power contactor, to a compound system comprising both simple and complex devices communicating through software and hardware.

In order to provide the safety function the system must continue to operate correctly under all foreseeable conditions.

So how do we design a system to achieve this, and when we have done that, how do we show it?

The draft European Standard prEN 954-1 “Safety related parts of control systems” deals with these aspects.

It lays down a “language” of five categories for benchmarking and describing the performance of SRCSs.

Table 32 is a summary of the categories.

SUMMARY OF REQUIREMENTS	SYSTEM BEHAVIOUR	PRINCIPLE
<p>CATEGORY B (see note 1)</p> <ul style="list-style-type: none"> - Safety related parts of machine control systems 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.	By selection of components (Towards PREVENTION of faults)
<p>CATEGORY 1</p> <ul style="list-style-type: none"> - The requirements of category B apply together with the use of well tried safety components and safety principles. 	As described for category B but with higher safety related reliability of the safety related function. (The higher the reliability, the less the likelihood of a fault)	
<p>CATEGORY 2</p> <ul style="list-style-type: none"> - The requirements of category B and the use of well tried safety principles apply. - The safety function(s) shall be checked 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. 	<p>The loss of safety function is detected by the check.</p> <p>The occurrence of a fault can lead to the loss of safety function between the checking intervals.</p>	By structure (Towards DETECTION of faults)
<p>CATEGORY 3 (see notes 2 & 3)</p> <ul style="list-style-type: none"> - The requirements of category B and the use of well tried safety principles apply. - The system shall be designed so that a single fault in any of its parts does not lead to the loss of safety function. 	<p>When the single fault occurs the safety function is always performed.</p> <p>Some but not all faults will be detected.</p> <p>An accumulation of undetected faults can lead to the loss of safety function.</p>	
<p>CATEGORY 4 (see notes 2 & 3)</p> <ul style="list-style-type: none"> - The requirements of category B and the use of well tried safety principles apply. - The system shall be designed so that a single fault in any of its parts does not lead to the 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. 	<p>When the faults occur the safety function is always performed.</p> <p>The faults will be detected in time to prevent the loss of safety functions.</p>	

Table 32

Note 1: Category B in itself has no special measures for safety but it forms the base for the other categories.

Note 2: Multiple faults caused by a common cause or as inevitable consequences of the first fault shall be counted as a single fault.

Note 3: The fault review may be limited to two faults in combination if it can be justified but complex circuits (e.g. microprocessor circuits) may require more faults in combination to be considered.

So how do you decide on which category you need?

In order to translate these requirements into a system design specification there has to be an interpretation of the basic requirements.

First of all let us dispose of one popular misconception. It is a commonly held belief that category 1 gives the least protection and category 4 gives the best. *This is not the reasoning behind the categories.* They are intended as reference points which describe the functional performance of different method types of safety related control systems (or their constituent parts).

Category 1 is aimed at the PREVENTION of faults. It is achieved by the use of suitable design principles, components and materials. Simplicity of principle and design together with the use of materials with stable and predictable characteristics are the keys to this category.

Categories 2, 3 and 4 require that if faults cannot be prevented they must be DETECTED (and appropriate action taken). Monitoring and checking are the keys to these categories. The most usual (but not the only) method of monitoring is to duplicate the safety critical functions (i.e. redundancy) and compare their operation.

Perhaps the best way to make further progress is to use examples.

The example in fig. 33 is a simple system comprising a guard door interlock switch connected in series to the control coil of a power contactor. If we consider that the aim is toward complete reliability with no possibility of a failure to a dangerous condition, which of the categories is most appropriate?

The diagram below also shows the location and nature of potential dangerous faults.

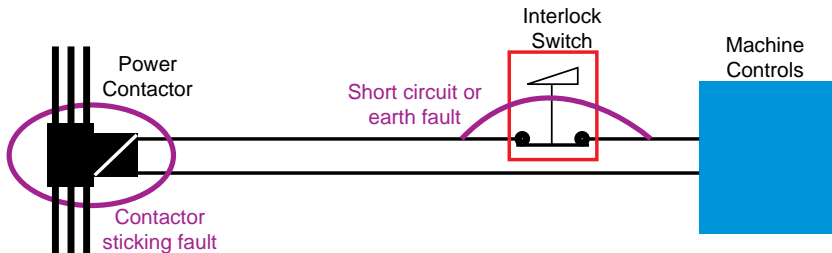


Fig. 33

If we refer to table 32 which type of category is the most appropriate? The prevention of faults or the detection of faults?

The first step is to separate the system into its major components and consider their modes of potential failure.

In this example the components are:

Interlock switch.

Contactor.

Wiring.

The **interlock switch** is a mechanical device. The task which it performs is a simple one i.e. opening the contacts when a guard door is opened. It fulfills the requirements of category 1 and by the use of correct design principles and materials it can be proved that, when used within its stated operating parameters, it will have no failures to a dangerous condition. This is made feasible by the fact that the device is relatively simple and has predictable and provable characteristics.

The **contactor** is a slightly more complex device and may have some theoretical possibilities for failure. Contactors from reputable manufacturers are extremely reliable devices. Statistics show that failures are rare and can usually be attributed to poor installation or maintenance.

Contactors should always have their power contacts protected by an overcurrent cut-out device to prevent welding.

Contactors should be subject to a regular inspection routine to detect excessive contact pitting or loose connections which can lead to overheating and distortion.

The contactor should comply with relevant standards which cover the required characteristics and conditions of use.

By attending to these factors it is possible to keep the possibilities of failure to a minimum. But for some situations even this is unacceptable and in order to increase the level of safety provision we need to use duplication and monitoring.

The wiring which connects the components together must also be considered. Undetected short circuit and ground faults could lead to a dangerous condition but if it is properly designed and installed using standards such as EN 60204 for guidance then the chances of failure are greatly reduced.

This system can provide a significant level of safety which may be adequate for many situations. You may have noticed however that both the contactor and the wiring are prone to unlikely though theoretically foreseeable faults. In some cases it may be possible, by taking precautions (e.g. with regard to cable protection and routing) to eliminate all fault possibilities. If this is not feasible then techniques relevant to categories 2, 3 & 4 such as duplication and monitoring are usually both more practical and cost effective.

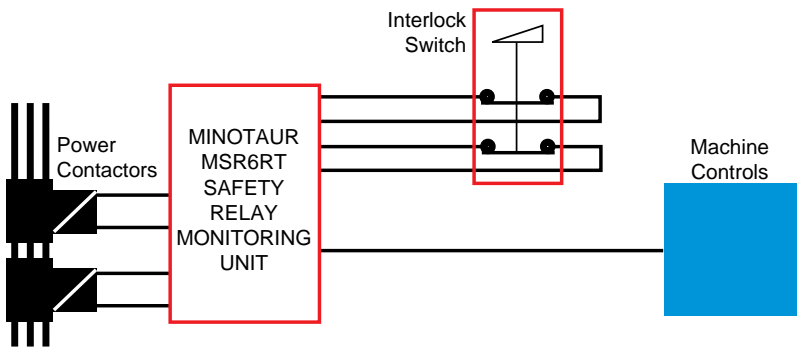


Fig. 34

Fig. 34 shows a system which fulfills the requirements of category 3. A MINOTAUR MSR6RT safety monitoring relay unit is used to monitor a two channel control circuit. Any single fault on the wiring or contactors will be detected by the Minotaur at the next demand on the safety function. NOTE: Although the interlock switch now has double pole contacts it is still a device which fulfills the requirements of category 1 - forming part of a system which fulfills the requirements of category 3.

This poses the inevitable question of when, and to what degree, do we need to take such measures.

The simple answer is to say that it depends on the results of the risk assessment. This is the correct approach but we must understand that this includes all factors and not just the level of risk at the hazard point. For example, it may be thought that if the risk estimation shows a high level of risk, the interlock switch should be doubled up and monitored. But in many circumstances this device, due to its application, design and simplicity, will not fail to danger and there will be no undetected faults to monitor.

Therefore the situation is becoming clear, **the type of category used will depend on both the risk assessment and the nature and complexity of the device or system.** It is also clear that where a total system meets the requirements of category 3 for example it may include devices to category 1.

If there are fault possibilities the higher the degree of risk, obtained at the **risk estimation**, the greater the justification for measures to prevent or detect them and the type of category should be chosen to give the most suitable and efficient method of doing this. Remember, the level of risk estimate is one factor but the nature of the protective device or system and the machine's operating characteristics must also be taken into account.

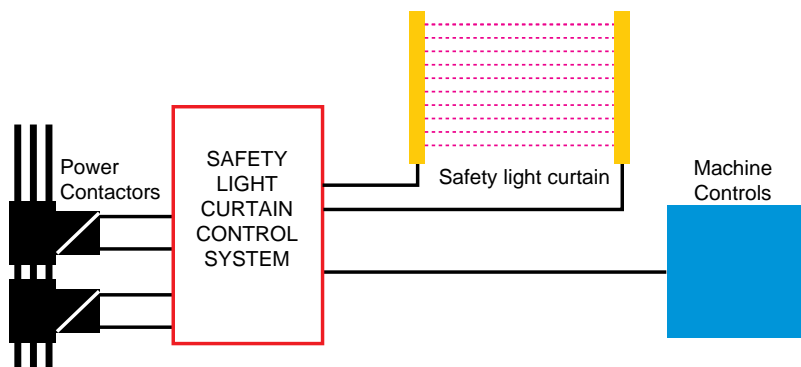


Fig. 35

Fig. 35 shows the same basic circuit but the interlock switch is replaced by a safety light curtain.

The **safety light curtain** is a complex device. Even in its simplest form it will have a relatively large number of electronic components including integrated circuits. More sophisticated types (and hence with more features) may also depend on programmable devices and software.

To anticipate and eliminate all dangerous faults in an electronic but non-programmable device would be a huge task and with a programmable device it would be virtually impossible. Therefore we must accept that faults will be possible and the best answer is to detect them and ensure that the necessary protective action is taken (e.g. locking out to a safe state). So we would need a device that satisfies the requirements of category 2, 3 or 4. With a simple circuit such as in fig. 35 the light curtain will also monitor the wiring and contactors. As all light curtains are relatively complex, the choice of categories will usually depend solely on the results of the risk assessment. This does not preclude the fact that it may be possible to work to a different category if a device uses an unconventional but provable approach.

We can see from the last two examples that the **same** degree of protection is provided by two types of systems using devices satisfying **different** categories.

Hopefully these examples will encourage a pattern of logic to enable the correct decision to be made.