

## Chapter 6

### FURTHER CONSIDERATIONS AND EXAMPLES

In this section we shall give examples of safety related control circuits with reference to recommended practices and the safety related control system categories where appropriate.

#### *General requirements*

The system must be capable of withstanding all expected influences. These will include temperature, environment, power loading, frequency of use, airborne interference, vibration etc. The standard EN 60204-1 “Safety of machinery - Electrical equipment of machines - Specification for general requirements” provides detailed guidance on such things as electric shock protection, wiring practices, insulation, equipotential bonding, equipment, power supplies, control circuits and functions etc. A knowledge of this standard is essential for those concerned with the design and maintenance of safety related control systems.

#### *Circuits and Monitoring Safety Relay Units*

The examples given below are based on the use of a control interlocking switch but the same principle can be applied to other switching device e.g. emergency stop or trip devices.

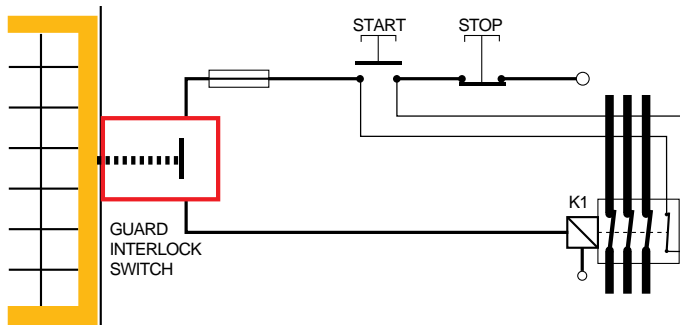


Fig. 36

#### *CATEGORY 1*

Fig. 36 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 it should be installed in accordance with the relevant

clauses of standard EN 60204. It should be routed and protected in a manner which prevents any foreseeable short circuits or earth faults. This system will satisfy the requirements of category 1.

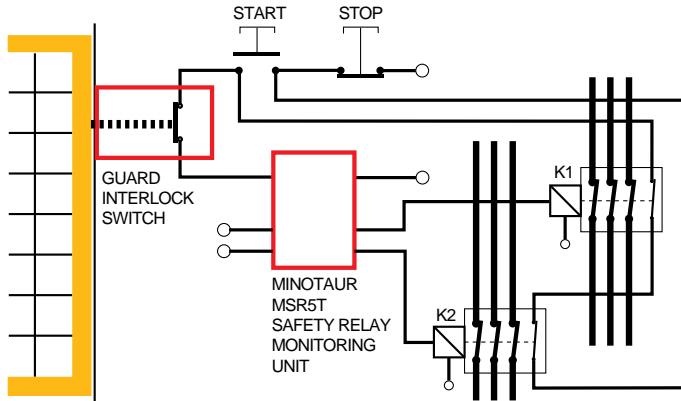


Fig. 37

**CATEGORY 1**

Fig. 37 shows a slightly more complex circuit. In this case there is a requirement for the interlock device to control more than one contactor, each being on a different power circuit. Its component parts must be given the same considerations. With a non-safety related circuit an ordinary relay could be used to “split” the signal but where safety is concerned this would definitely not be acceptable as they can (and sometimes do) stick. Therefore a monitoring safety relay unit such as the MINOTAUR MSR5T is used to provide an ensured safety relay action. This system will satisfy the requirements of category 1.

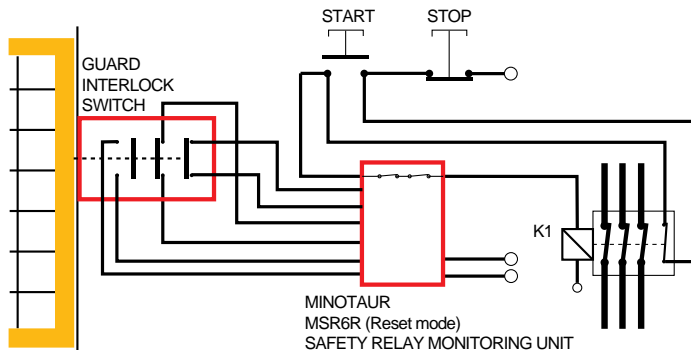
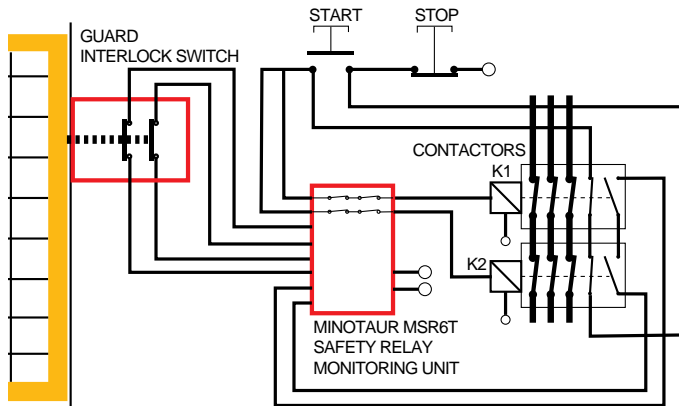


Fig. 38

## CATEGORY 2

Fig. 38 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 Minotaur 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 Minotaur. Only when this check is successful will the contactor be energized. At every subsequent guard operation the circuit will be similarly checked.



*Fig. 39*

## CATEGORY 3

Fig. 39 shows a system which satisfies the requirements of category 3 and is often suitable for applications with higher risk estimations. It is a dual channel system which is fully monitored including the two contactors. On opening and closing the guard, any single dangerous fault will cause the Minotaur to lock off power to the contactors until the fault is rectified and the Minotaur is reset.

## CATEGORY 4

Category 4 requires that the safety system function is still provided even with an accumulation of undetected faults (see page 47). 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 are used in interlocking and emergency stop systems.

These techniques are viable (and often used) to monitor solid state electronic components because a high frequency changing 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.  
*P.E.S. (Programmable Electronic Systems)*

In the safety related circuits shown above, the protective device is directly connected to the contactor(s) using only wiring and simple or fully monitored electro-mechanical devices. This is the normally recommended “hard wired” method. Its simplicity means that it is reliable and relatively easy to monitor. Increasingly the normal operational control of machinery is being handled by programmable equipment. With the advances in technology, programmable and complex electronic control systems could be regarded as the central nervous system of many machines. Whatever happens in the control system will affect the machine action and conversely whatever happens to the machine action will affect the control system. Stopping one of these machines by any source other than its control system may result in severe tool and machine damage as well as program loss or damage. It is also possible that, upon restarting, the machine may behave in an unpredictable manner due to “scrambling” of its control command sequence.

Unfortunately most programmable electronic systems have too many failure modes due to their complexity to allow their use as the only way of stopping the machine on command from an guard door interlock or emergency stop button.

In other words we can stop it without machine damage OR stop it SAFELY BUT NOT BOTH. So what do we do? Three solutions are given below:-

### *1 - Safety Related Programmable Systems*

In theory it is possible to design a programmable system which has a safety integrity level high enough for safety related use. In practice this would normally be achieved by using special measures such as duplication and diversity with cross monitoring. In some situations this may be possible but it is important to realize that these special measures will need to be applied to all aspects including the writing of software.

The basic question is, can you prove that there will be no (or sufficiently few) failures. A full failure mode analysis for even relatively simple programmable equipment may, at best, be excessively time consuming and expensive or, at worst, be impossible.

The draft standard IEC 1508 deals with this subject in great detail and anyone concerned with safety related programmable systems is advised to study it when it becomes available.

The development costs of these systems are justifiable in applications where they have significant advantages or no other method will work.

2 - Monitoring Unit with Time Delayed Override Command.  
 (see Fig. 40) This system has the high integrity level of hard wiring and also allows a correctly sequenced shut-down which protects the machine and program.

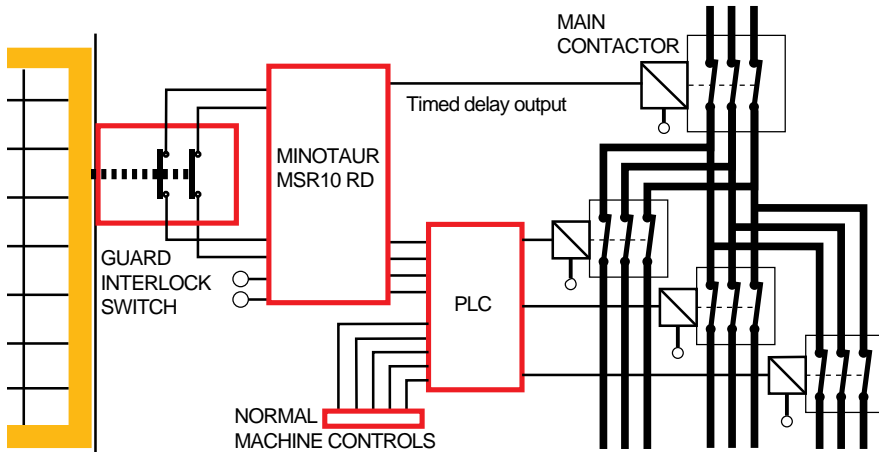


Fig. 40

The MINOTAUR MSR10RD primary outputs are connected to inputs at the programmable device (e.g. P.L.C.) and the delayed outputs are connected to the contactor. When the guard interlock switch is actuated, the primary outputs on the Minotaur switch immediately. This signals the programmable system to carry out a correctly sequenced stop. After sufficient time has elapsed to allow this process the delayed output on the Minotaur switches and isolates the main contactor.

This range of Guardmaster devices can be used with various protective devices and is available with other configurations and switching arrangements to suit the requirements of particular systems.

Note: Any calculations to determine the overall stopping time must take account of the Minotaur output delay period. This is particularly important when using this factor to determine the positioning of devices in accordance with standard pr EN 999.

3 - Programmable System Controlled Guard Locking Devices.  
(see Fig. 41)

This system again provides the high integrity level of hard wiring combined with the ability to give a correctly sequenced shut down but it is only applicable where the hazard is protected by a guard.

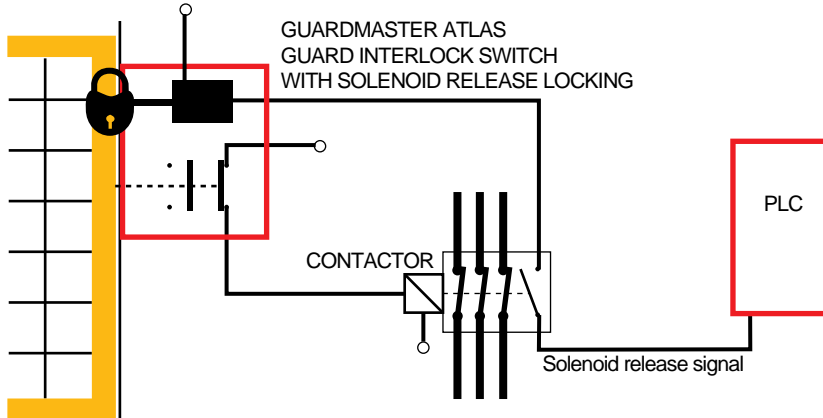


Fig. 41

In order to allow opening of the guard door the ATLAS solenoid must receive a release signal from the P.L.C. This signal will only be given after a stop command sequence has been completed. This ensures there is no tool damage or program loss. When the solenoid is energized the door can be opened which causes the control circuit contacts on the ATLAS to isolate the machine contactor.

In order to overcome machine run-down or spurious release signals it may be necessary to use a Guardmaster Cerberus CU1 timed delay unit or CU2 stopped motion detector in conjunction with the P.L.C. (Either the Atlas or Titan switches can be used in this application).

#### OTHER CONSIDERATIONS

##### *Machine restart - Manual/Auto Reset and Control Guards*

If (for example) an interlocked guard is opened on an operating machine, the safety interlock switch will stop that machine. In most circumstances it is imperative that the machine does not restart immediately when the guard is closed. The most common way of achieving this is to rely on a latching contactor start arrangement as shown in fig. 42 (an interlocked guard door is used as an example here but the requirements apply to other protection devices and emergency stop systems).

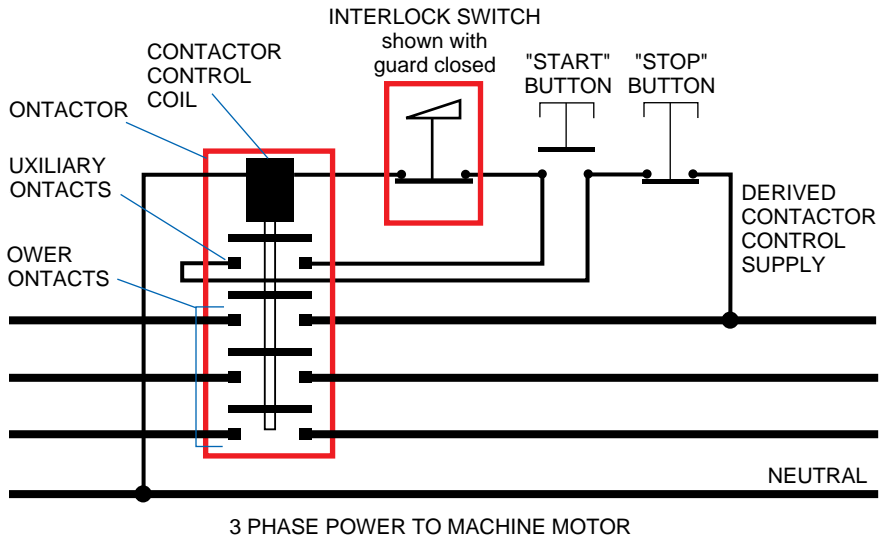


Fig. 42

Pressing and releasing the start button momentarily energizes the contactor control coil which closes the power contacts. As long as power is flowing through the power contacts the control coil is kept energized (electrically latched) via the contactor's auxiliary contacts which are mechanically linked to the power contacts. Any interruption to the main power or control supply results in the de-energizing of the coil and opening of the main power and auxiliary contacts. The guard interlock is wired into the contactor control circuit. This means that restart can only be achieved by closing the guard and then switching "ON" at the normal start button which resets the contactor and starts the machine.

The requirement for normal interlocking situations is made clear in EN 292 part 1 3.22.4 (extract)

*-When the guard is closed, the hazardous machine functions covered by the guard can operate, but the closure of the guard does not by itself initiate their operation.*

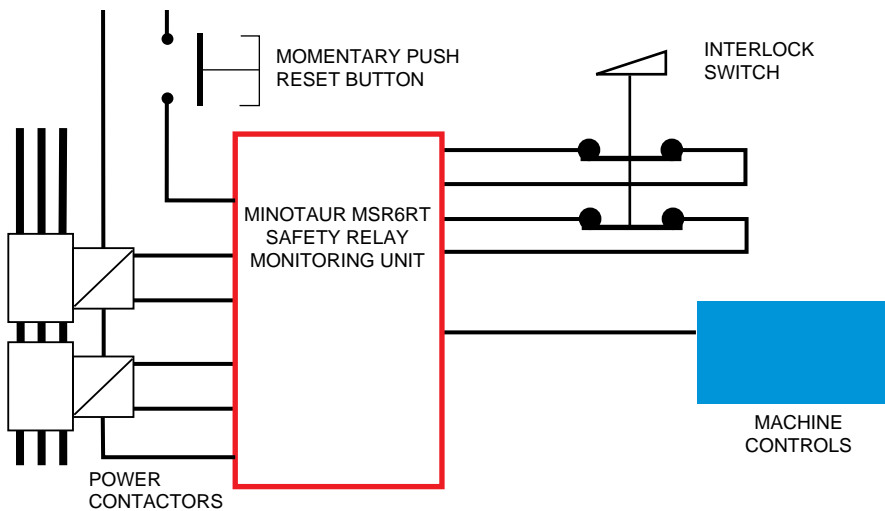
Many machines already have either single or double contactors which operate as described above (or have a system which achieves the same result). When fitting an interlock to existing machinery it is necessary to determine whether the power control arrangement meets this requirement and take additional measures if necessary.

### *Auto/Manual reset*

On some types of protective devices, after actuation of the safety function, the output will remain off until the device has been reset.

Some devices are available in either manual reset or auto-reset versions.

A **manual reset** depends on a manual switching action after the de-actuation of the device and may also trigger a system integrity check before the safety system is reset to render the machine capable of being started. It will require the operation of a button or key operated switch which may be fitted either on the device, the control unit or at a remote location. Wherever it is, it should provide a good view of the hazard so that the operator can check that the area is clear before operation.



*Fig. 43*

In Fig. 43, after the guard has been opened and closed again the Minotaur will not allow the machine to be restarted until the reset button has been pressed and released. When this is done the Minotaur checks that both contactors are OFF and that both interlock circuits (and therefore the guard) are closed. If these checks are successful the machine can then be restarted from the normal controls.

An **auto-reset device** does not require a manual switching action but after de-actuation it will always conduct a system integrity check before resetting the system.

*An auto-reset system should not be confused with a device without reset facilities.* In the latter the safety system will be enabled immediately after de-actuation but there will be no system integrity check.

### *Control Guards*

A control guard stops a machine when the guard is opened and directly starts it again when the guard is closed.

The use of control guards is only allowed under certain stringent conditions because any unexpected start-up or failure to stop would be extremely dangerous. The interlocking system must have the highest possible reliability (it is often advisable to use guard locking).

The use of control guards can **ONLY** be considered on machinery where there is **NO POSSIBILITY** of an operator or part of his body staying in or reaching into the danger zone while the guard is closed.

The control guard must be the only access to the hazard area.