

## Further Considerations and Examples

Figure 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 (with more features) may also depend on programmable devices and software.

To anticipate and eliminate all dangerous faults in an electronic but nonprogrammable 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 Figure 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.

### Further Considerations and Examples

This section provides 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 expected influences. These will include temperature, environment, power loading, frequency of use, airborne interference, vibration, etc. The standard IEC 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 devices (e.g., emergency stop or trip devices).

#### Category 1

Figure 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, 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.

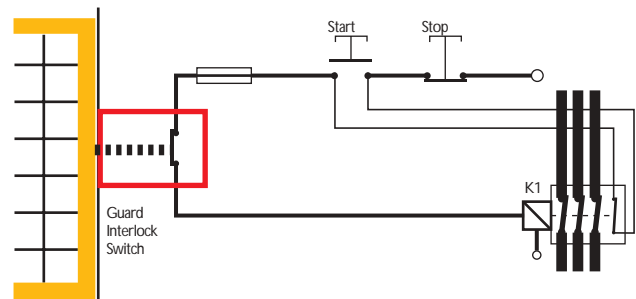


Figure 36

Figure 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.

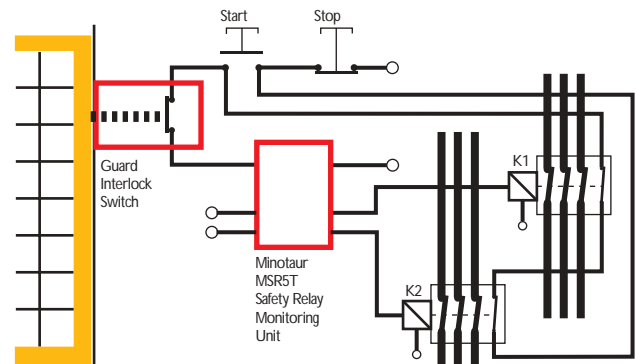


Figure 37

With a nonsafety 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 Guardmaster MINOTAUR MSR5T is used to provide an ensured switching action. This system will satisfy the requirements of category 1.

#### Category 2

Figure 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.



## Safety Principles

### Further Considerations and Examples

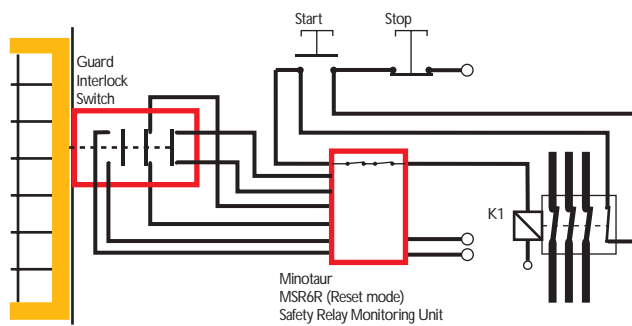


Figure 38

#### Category 3

Figure 39 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 Minotaur to lock off power to the contactors until the fault is corrected and the Minotaur is reset.

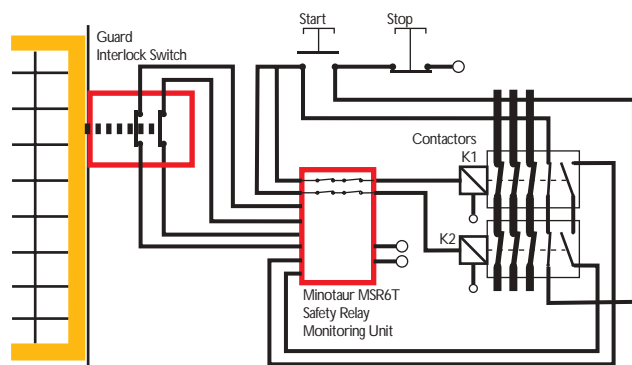


Figure 39

#### Category 4

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.

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

In other words, we can stop it without machine damage OR stop it SAFELY—BUT NOT BOTH. Three solutions are given below:

##### 1. Safety Related Programmable Systems

In theory it is possible to design a programmable system that has a safety integrity level high enough for safety related use. In practice this would 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 must 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, impossible.

The standard IEC 61508 deals with this subject in great detail and anyone concerned with safety related programmable systems is advised to study it.

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 Figure 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.

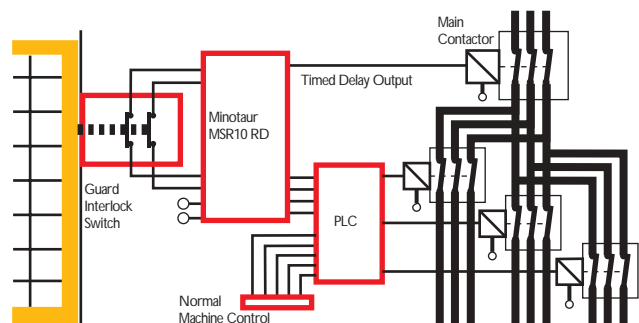


Figure 40



The Guardmaster 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 family of Guardmaster products 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 the Minotaur output delay period into account. This is particularly important when using this factor to determine the positioning of devices in accordance with standard EN 999.

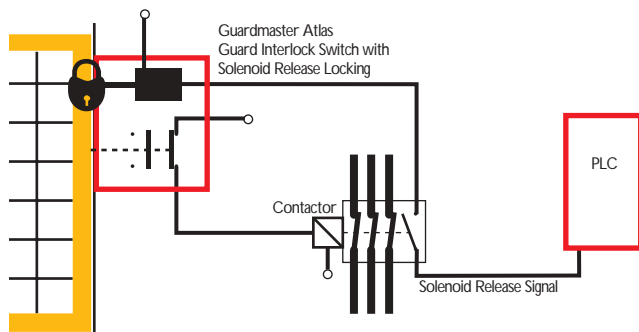


Figure 41

3. Programmable System Controlled Guard Locking Devices (see Figure 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.

In order to allow opening of the guard door the Guardmaster 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 CU1 timed delay unit or CU2 stopped motion detector in conjunction with the P.L.C. (Either the Guardmaster Atlas or TLS-GD2 switches can be used in this application).

## Other Considerations

### Machine Re-start

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. A common way of achieving this is to rely on a latching contactor start arrangement as shown in Figure 42. An interlocked guard door is used as an example here but the requirements apply to other protection devices and emergency stop systems.

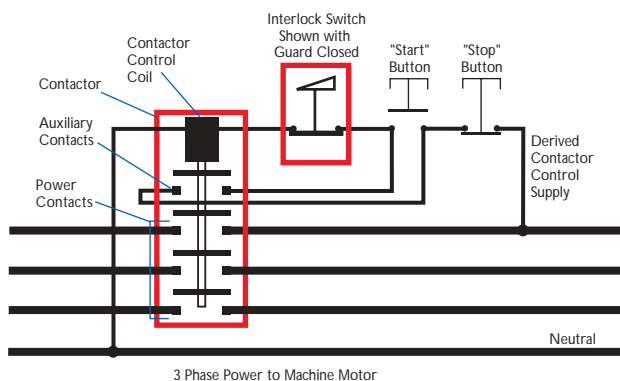


Figure 42

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 ISO 12100-1 Paragraph 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.

