Technical Paper – White Paper 7

Safety Related Control Systems

By Phil Chambers BSc, CMIOSH

Technical Paper

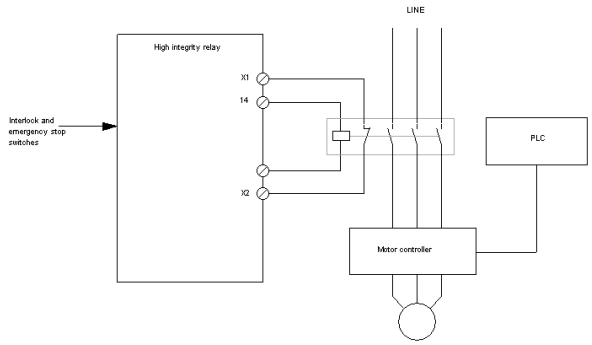
Overview

The safety related control system (SRCS) is that part of a machine's control system which uses inputs such as guard switches, light curtains and emergency stops to control access to dangerous parts of the machine. In order to attain the required safety integrity level, it is necessary to ensure that all parts of the SRCS are high-reliability devices and, where appropriate, component duplication and monitoring of the SRCS is provided. ISO 13849 specifies what safety integrity level is necessary and how this may be achieved. See Technical Paper 4 for details of 13849.

Acceptable arrangements

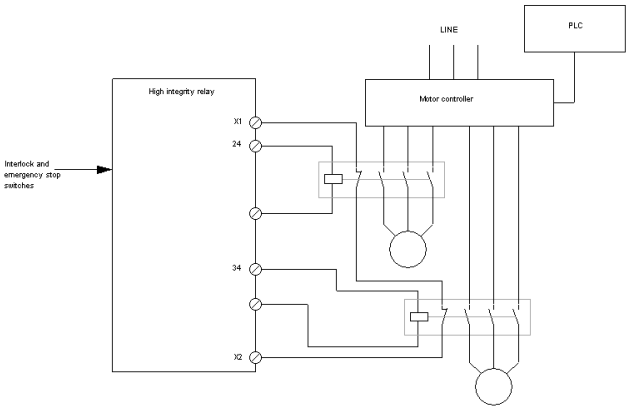
Input power to motor controller switched

Power is switched by a contactor activated by contacts from the high integrity relay. A pair of normally closed (N/C) contacts on the contactor is used each time the high integrity relay is reset to verify that the contactor is not jammed in the unsafe condition. Typically the contacts from interlock switches and emergency stops are duplicated to enable the appropriate safety integrity level to be attained.



Output power from motor controller switched

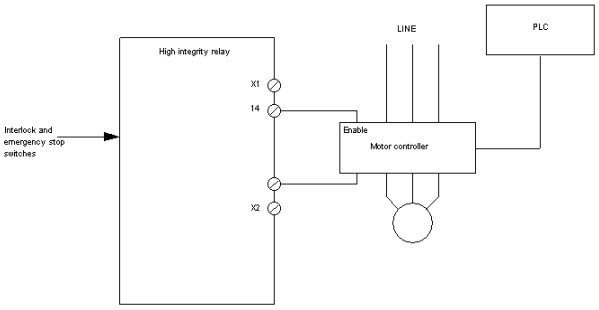
Power is switched by a contactor on each motor feed, activated by contacts from the high integrity relay. A pair of normally closed (N/C) contacts on each contactor, wired in series, is used each time the high integrity relay is reset to verify that the contactors are not jammed in the unsafe condition



Enable signal to motor controller switched

Some motor control circuits require resetting if their power is switched off. This would obviously be unacceptable in an interlock circuit.

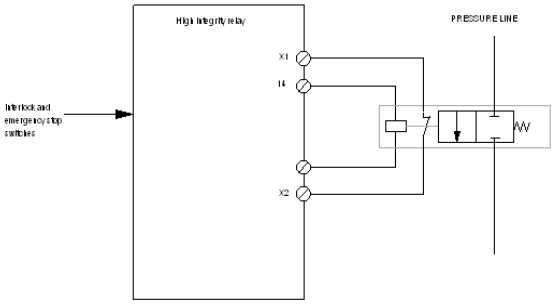
If the motor controller has an enable function, then this may be switched by the high integrity relay. A simple circuit within the motor controller then prevents the motor from being energised. Data on the reliability of this function must be included in the assessment carried out as required in EN 13849.



Technical Paper

Switching hydraulic pressure

Where the supply of hydraulic pressure must be blocked as part of the safety function, then a normally closed hydraulic valve is used, activated by the high integrity relay.

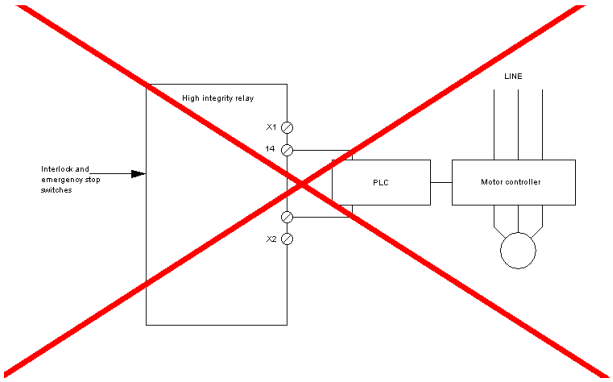


If the valve is a spool-type valve with the solenoid acting directly on the spool with a spring return, then such valves have the potential to become jammed by contamination in the spool clearance. This has the effect of the valve remaining in its unsafe state when de-energised. To prevent the safety circuit from being compromised, a spool position switch must be used, wired into the high integrity relay, in the same way as a N/C contact on an electrical contactor.

If the valve is a poppet type which has no tight clearances, then the need for a position feedback switch is not necessary.

Undesirable arrangements

Control system downstream of high integrity circuit.



The PLC or other type of control system should not be used where its performance forms part of the safety function. The integrity level of the safety related control system is high where it feeds into the PLC but is then compromised by the unknown reliability of the PLC.

Faults in the PLC or its program are uncontrolled. It typically both necessary and desirable to use contacts from the safety related control system to signal fault or interlock conditions to the PLC but the PLC should not be solely relied upon to limit machine energisation for safety reasons.

Note that this is not a hard and fast rule. It is feasible to have the PLC as part of the safety related control system, but this must meet the appropriate requirements of an analysis required by EN 13849; it is generally considerably easier to avoid the PLC altogether.

Strategic Safety Systems Ltd., 8 The Highgrove, Bishops Cleeve, Cheltenham, GL52 8JA, UK
Phone: 01242 679713 Mobile 077680 11667
E-Mail: info@StrategicSafety.co.uk Web site: www.StrategicSafety.co.uk