Technical Paper

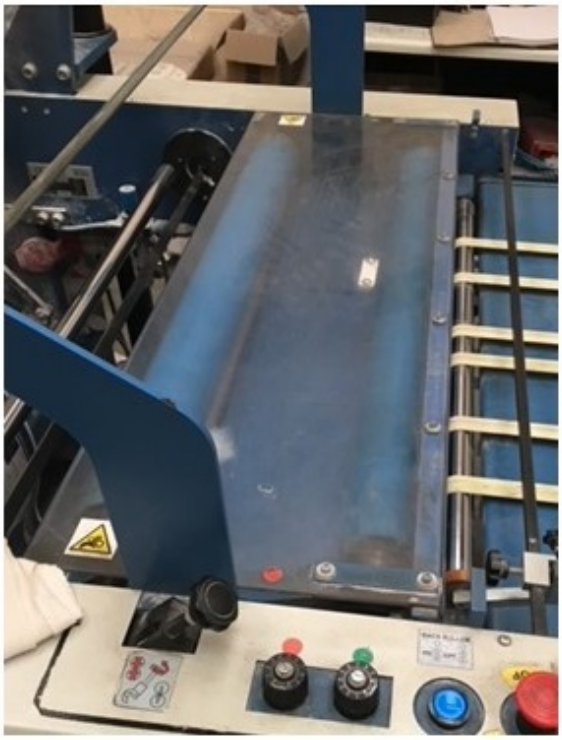
White Paper No. 47

Poor safety circuit design causes accident

Phil Chambers BSc, MIIRSM

Strategic Safety Systems

When you buy a machine, don't assume that it is reliably safe. This white paper discusses a small machine with a guard interlocked so that the machine should not run when it was open. However, the poor design of the electrical safety circuit allowed it to momentarily start when the operator had his hand in an in-running nip.



The accident occurred on a machine that applied a laminate film to printed paper. The left hand picture shows the guard closed and the right hand one shows it hinged to the right. Paper passes between the roller and the bed in the rightwards direction. The red arrow shows the in-running nip where the accident occurred.

A jam-up occurred with paper jammed under the right hand roller and the machine stalled. The operator opened the guard and its interlock should have prevented any powered movement. However, when the operator freed the jammed paper, the machine restarted and his finger was caught between the roller and the bed. He suffered severe bruising.

An investigation immediately after the accident verified that the interlock had not been overridden.

Cause of the accident

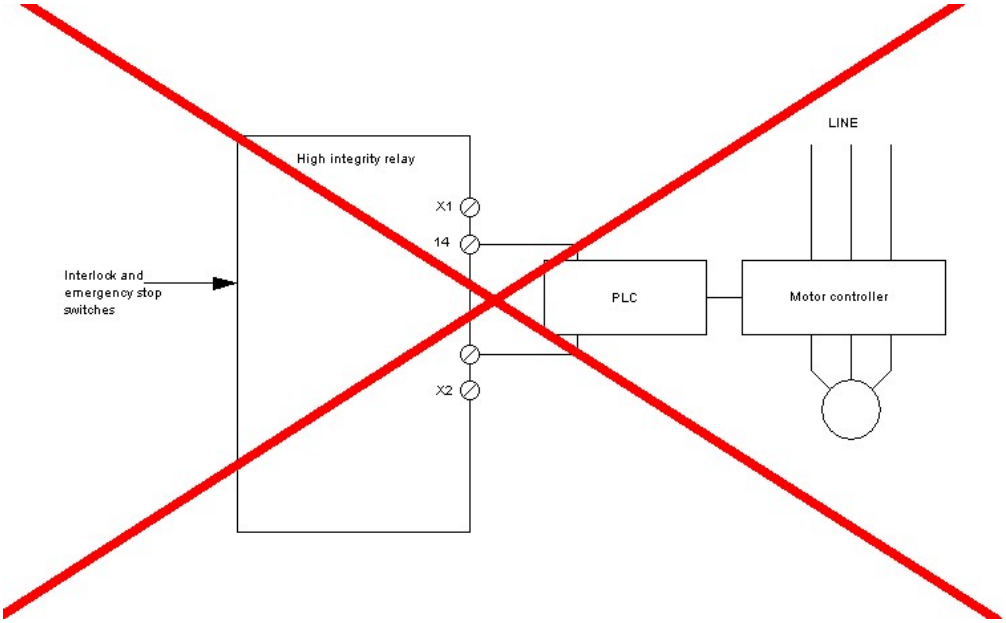
I was asked to investigate this machine further and my examination of the electrical circuit diagram showed that the interlock switch was purely an input to the PLC, which was a standard, non safety-rated type.

Because of this arrangement, there was no safety system that prevented spurious outputs from the PLC from causing the machine to run. What looks most likely is that when the machine stalled, the PLC sat waiting for its next signal; ie the machine was still live. When the operator cleared the jam, the PLC continued with its cycle. It was not until this cycle was complete that the PLC reacted to the open interlock switch.

Best safety circuit practice

It is essential that the safety circuit acts downstream of the PLC, unless a safety-rated PLC is used.

The diagram shown below shows how the reliability of a high integrity safety system (Pilz type safety relay, etc.,) can be entirely compromised by using it as a pure feed into a standard PLC. In my experience, I have seen this done several times by people who assume that PLCs have the same level of reliability as the safety relay.



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.

SSS White Paper 7 described safety related control systems in more detail.

http://www.strategicsafety.co.uk/pdf/WhitePapers/WhitePaper7-SafetyRelatedControlSystems.pdf

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