

II. Control Reliability

19

What is meant by “control reliability”?

“Control reliability” implies that the safety device or system is designed, constructed and installed such that the failure of a single component within the device or system

shall not prevent normal machine stopping action from taking place ... but shall prevent a successive machine cycle from being initiated.

20

How does this definition of “control reliability” relate to the European machinery safety requirements?

Safety systems which are “single component failure control reliable” meet the requirements of a Category 3

safety-related control system as defined by the harmonized European machinery safety standard EN954-1.

What are “positive-guided” or “force-guided” relays, and why are they preferred over conventional relays when designing safety systems?

Positive-guided relays feature N.O. and N.C. contacts which operate interdependently. For such relays, the N.O. and N.C. contacts can never be closed simultaneously. In the event one of the contacts welds closed, the other contacts cannot change state. For example, should one or more of the N.O. contacts weld/stick shut when closed, the N.C. contact(s) will remain open with a minimum gap of 0.5mm.

This unique feature is desirable in machine safety circuits where “fail- to-safe” and/or “single component failure control reliability” is desired. The positive relationship (interdependent operation) between N.O. and N.C. contacts permit self-checking/monitoring of the performance of these devices. Such relays provide a higher level of safety system integrity and reliability.

A simple illustration of the interdependent function of positive-guided contacts is shown in Figure 9.

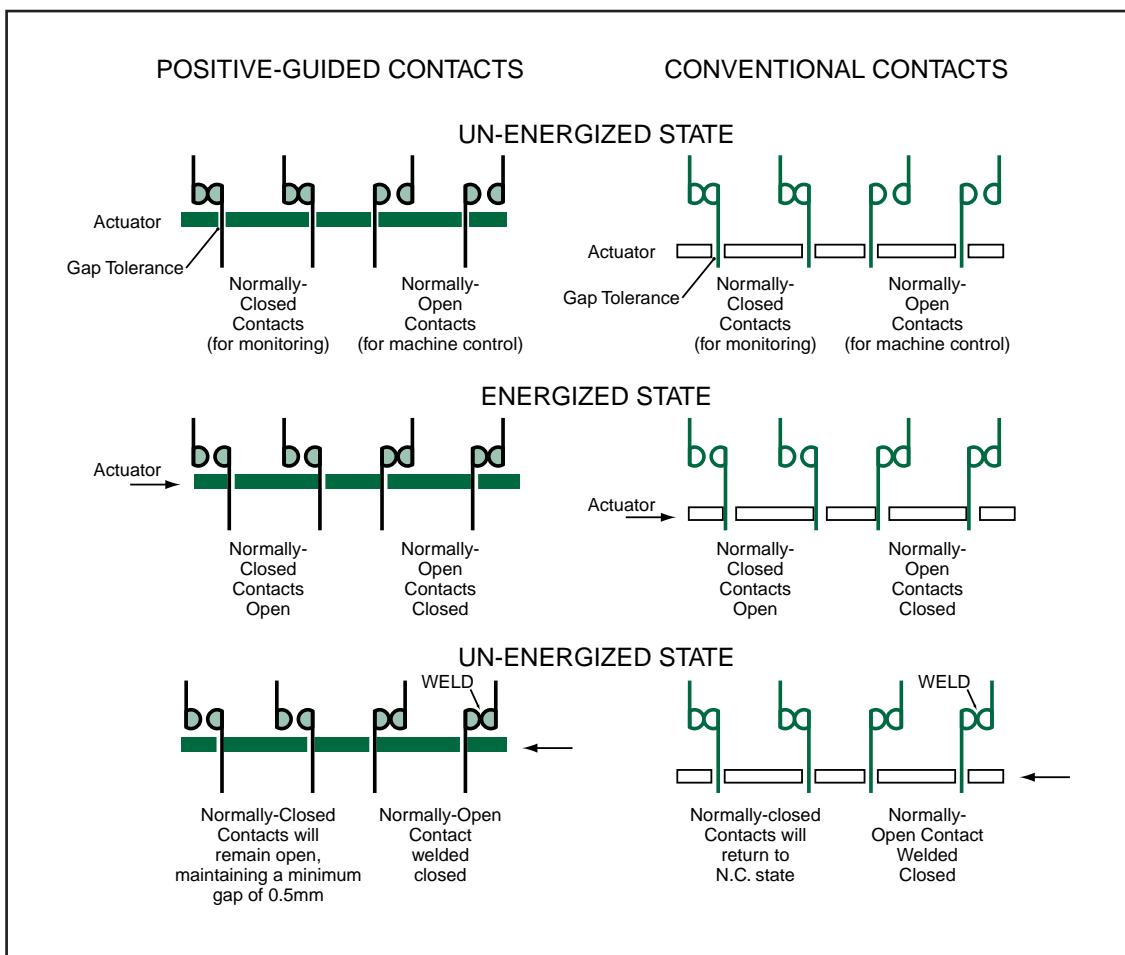


FIGURE 9
POSITIVE-GUIDED VS. CONVENTIONAL CONTACTS

22

What are “redundant” logic circuits, and what are their benefits in safety circuit applications?

“Control reliability” implies that the safety device or system is designed, constructed and installed such that the failure of a single component within the device or system shall not prevent normal machine stopping action from taking place ... but shall prevent a successive machine cycle from being initiated. To achieve this, safety controllers are typically designed with dual logic circuits, each of which can provide safety circuit checking/monitoring. These functionally-equivalent logic circuits cross-monitor each other, as well as checking the safety circuit for component failures, short circuits, open circuits, etc.

Since these controllers detect faults in the safety circuit components and interconnection wiring to effect machine shutdown, such “redundant” self-monitoring circuits enhance safety system reliability. In so doing they

provide a higher level of safety for the machine operator and maintenance personnel.

To heighten the integrity and reliability of these units, SCHMERSAL engineers have had each of the redundant logic circuit microprocessors programmed by a different software specialist ... thus reducing the probability of a simultaneous logic-circuit malfunction due to a programming error.

Use of such safety controllers, in combination with safety interlock switches, tamper-resistant coded-magnet switches, and emergency cable-pull switches enables control engineers to achieve the “single component failure control reliability” required by OSHA, ANSI, and international machine guarding safety standards/guidelines.

23

What characterizes “fail-to-safe” operation?

“Fail-to-safe” safety devices are designed such that a component failure will cause the device to attain rest in a safe condition. This term is generally applied to electronic safety interlock systems using non-mechanical presence or position sensors (such as reed switches, proximity

switches, et al) and/or safety controllers. Such controllers are often designed to feature redundancy, self-diagnostics, and positive-guided contacts.

24

Why should I upgrade or enhance my current safety interlock or safety barrier design?

Heightened awareness and concern for worker safety has, and is, precipitating compelling reasons for such upgrades or enhancements. These are embodied in a variety of industrial safety standards and guidelines against which machinery manufacturers' and users' level of responsibility and degree of liability are measured.

Several of these current and emerging standards and guidelines are listed under references at the end of this booklet. The following excerpts are provided simply to illustrate the importance and need to consider providing new or improved safety systems.

OSHA Guidelines

OSHA 1910.212 "General Requirements for all machines": "One or more methods of machine guarding shall be provided to protect the operator and other employees from hazards... The guarding device shall be in conformity with any appropriate Standards thereof..."

OSHA 1910.5 "Applicability of Standards": "Any Standard shall apply according to its terms to any employment and place of employment in any industry even though particu-

lar Standards are prescribed for the industry..."

OSHA 1910.6 "Incorporation by Reference": "The Standards of agencies of the U.S. Government, and organizations which are not agencies of the U.S. Government which are incorporated by reference in this part, have the same force and effect as other Standards in this part..."

ANSI B11.19-1990 Machine Tool Safeguarding...

4.1.1.4: "The employer shall ensure that barrier guards are installed, maintained, and operated so as to protect against unauthorized adjustment or circumvention..."

5.5.1 "Control Reliability": When required by the performance requirements of safeguarding, the device, system, or interface shall be designed, constructed and installed such that a *single component failure* shall not prevent normal stopping action from taking place..."

1.3.1 and 1.3.2: The grace period for OEM's to conform with new safeguards was Feb. 1991. Employers (industrial users) were required to bring existing safeguards into conformance by March, 1994.

25

What is "fault exclusion" and how does it affect safety circuit design?

In selected situations the occurrence of known possible component failures ("faults") can be minimized by the safety system design or component selection. Simple examples are:

- (1) the use of an overrated contactor to preclude the possibility of contact welding.
- (2) design of a machine guard such that the interlock switch actuator cannot be damaged.

- (3) use of positive-break safety interlock switches together with a safety controller, such that the possibility of a contact weld resulting in the loss of the safety function is eliminated.

The elimination of such faults are a compromise between the technical safety requirements and the theoretical probability of their occurrence. Design engineers are permitted to exclude such faults when constructing the machinery's safety system. However, each "fault exclusion" must be identified, justified, and documented in the Technical File submitted to satisfy the European Machinery Directive.