SELECTED MACHINE SAFEGUARDING TERMINOLOGY

Authorized Output: an output from a safety controller's positive-guided relays (used to "authorize" or "enable" a machine's start circuit when safety system conditions exist). Also known as "safety output."

Automatic Reset: a safety controller reset circuit that automatically resets the safety controller when safe system conditions (no system faults) exist. A manual reset button is optional.

Auxiliary output: a non-safety related contact closure or semiconductor output primarily used for signaling component or system status to a PLC, audible alarm or visual indicator (such as a stack light). Also called a "signaling contact" or "auxiliary monitoring contact".

ANSI (American National Standards Institute): an association of industry representatives who, working together, develop safety and other technical standards.

Auxiliary monitoring contact: See "auxiliary output".

BG (Berufgenossenschaft): an independent German insurance agency whose legislative arm recommends industry safety practices. One of many "notified bodies" authorized to certify that safety products comply with all relevant standards.

CE (Conformité Europeéne) mark: a symbol (CE) applied to finished products and machinery indicating it meets all applicable European Directives. For electrical and electronic "finished products", such as a safety relay module, these include the Low Voltage Directive and, where relevant, the Electromagnetic Compatibility (EMC) Directive.

Coded-Magnet Sensor: a two-piece position sensor consisting of an array of reed switches and a multiple magnet array-actuating element. Such devices will only deliver an output signal when the reed switch element is in the presence of a matched, multiple-magnetic field array. Coded-magnet sensors cannot be actuated using a simple magnet. Hence they are far more difficult to defeat/bypass than a simple magnetic switch or proximity sensor.

Control Reliability: A term applied to safety devices or systems which are designed constructed and installed such that the failure of a single component within the device or system does not prevent normal machine stopping action from taking place…but does prevent a successive machine cycle from being initiated.

CSA (Canadian Standards Association): an independent Canadian testing and standards-making organization similar to Underwriters Laboratories (UL) in the U.S. "CSA-certified" products meet relevant CSA electrical and safety standards.

Declaration of Conformity: a manufacturer's self-certified document, signed by a highly-positioned technical manager, which lists all the Standards and Directives to which a product conforms. A Declaration of Conformity is mandatory for all CE-marked products, and for machine components which, if they fail, could lead to a dangerous or hazardous situation on a machine.

Defined Area: a predetermined area scanned by a light beam within which the presence of an opaque object of specified minimum size will result in the generation of a control signal.

Direct-Action Contacts: See "positive-break" contacts.

Diverse Redundancy: the use of different components and/or different microprocessor instruction sets written by different programmers in the design and construction of redundant components/circuits. Its purpose is to increase system reliability by minimizing the possibility of common-mode failure (the failure of like components used in redundant circuits).

Dual-Channel Safety System: a safety control system characterized by two inputs; each connected to one of two independent safety circuits. Dual-channel systems are typically capable of detecting interconnection wiring faults such as open circuits, short-circuits and ground faults. As such they provide a higher level of safety than single-channel systems.

E-Stop (Emergency Stop): the stopping of a machine by actuation of an "emergency stop" switch (such as a safety interlock switch, emergency push button switch, rope-pull switch, foot switch, or other actuating device.

European Machinery Directive (EMD) 2006/42/EC: a set of machine safety design requirements which must be satisfied to meet the Essential Health and Safety standards established by the European Economic Community. This Directive, and other relevant European Directives (such as the Low Voltage Directive, EMC Directive, et al) must be satisfied for the machine to bear the CE mark.

Fail-to-Danger: a component or system failure which allows a machine to continue operating, exposing personnel to a hazardous or unsafe condition.

Fail-to-Safe: "Fail-to-Safe" safety devices are designed such that a component failure causes the device/system to attain rest in a safe condition.

Fault Detection: the monitoring of selected safety system components whose failure would compromise the functioning of the safety system. The detection of such failures is known as "fault detection." Examples are:

- a short-circuit in the safety circuit's interconnection wiring
- an open-circuit in the safety circuit's interconnection wiring
- a welded contact in the safety controller's positive-guided relays
- an open machine guard

Fault Exclusion: the ability to minimize known possible component failures ("faults") in a safety system by design criteria and/or component selection. Simple examples of "excluded faults" are:

- The use of an overrated contactor to preclude the possibility of contact welding.
- Design of a machine guard such that the safety interlock switch actuator cannot be damaged.
- Selection of a suitable safety interlock switch.
- Use of positive-break safety interlock switches together with a self-monitoring safety relay module, such that the possibility of a contact weld resulting in the loss of the safety function is eliminated.

The elimination of such faults are generally 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 machine's safety system. However, each "fault exclusion" must be identified, justified, and documented in the Technical File submitted to satisfy the European Machinery Directive.

Feedback Loop: an auxiliary input on a safety controller designed to monitor and detect a contact weld in the primary machine-controlled device (e.g. motor contactor, relay, et al) having positive-guided contacts.

Force-Guided Contacts: See "Positive-Guided Contacts".

Fixed Barrier Guard: See "Hard Guarding".

Guard: a barrier that prevents entry of an individual's hands or other body parts into a hazardous area.

Hard Guarding: the use of screens, fences, or other mechanical barriers to prevent access of personnel to hazardous areas of a machine. "Hard guards" generally allow the operator to view the point-of-operation.

Hazardous Area: an area of a machine or process which presents a potential hazard to personnel.

Interlock: an arrangement in which the operation of one device automatically brings about or prevents the operation of another device.

Interlocked Barrier Guard: a fixed or movable guard which, when opened, stops machine operation.

Machine Primary Control Element (MPCE): an electrically powered component which directly controls a machine's operation. MPCE's are the last control component to operate when a machine's motion is initiated or stopped.

Machine Secondary Control Element (MSCE): a machine control element (other than an MPCE) capable of removing power from the hazardous area (s) of a machine.

Manual Start-Up Test: a term applied to safety controllers designed such that at least one of the system's interlocked machine guards must be manually-opened and closed (after applying power) before machine operation is authorized. All SCHMERSAL'S even numbered Series AES microprocessor--based safety controllers (e.g. AES 1136, AES 1146, AES 1156, AES 3366, et al) are designed to require a manual start-up test.

Manually-monitored Reset: a safety controller reset circuit requiring the presence of a discrete "trailing-edge" signal (24V to 0V) to activate the controller's authorized outputs. A reset button is mandatory.

Muting: the ability to program a monitoring and/or control device to ignore selected system conditions.

Negative Mode Mounting: the mounting of a single-piece safety interlock switch (e.g. a limit switch) such that the force applied to open the normally closed (NC) safety contact is provided by an internal spring. (See Figure 1.)
In this mounting mode the NC contacts may not open when the safety guard is "open". Here welded/stuck contacts, or failure of a contact-opening spring, may result in exposing the machine operator to a hazardous/unsafe area.

When mounted in the "negative-mode", single-piece safety interlock switches can be easily circumvented/defeated by the operator…simply by taping down the switch actuator when the safety guard is open.

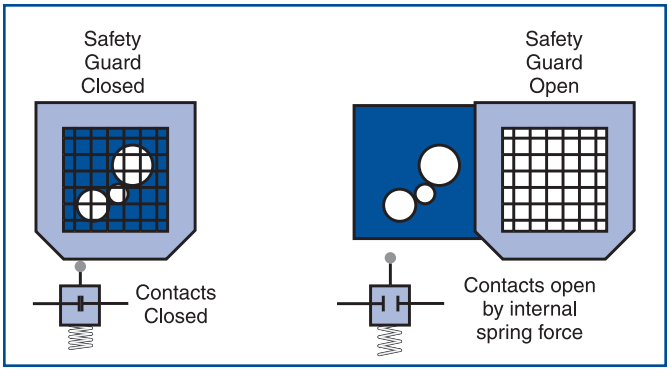


Figure 1
NEGATIVE-MODE INSTALLATION

OSHA (Occupational Safety Health Administration): a U.S. Department of Labor Federal agency responsible for monitoring and regulating workplace safety. OSHA enforcement may reference their own regulations, as well as those of other industry standards-making groups (e.g. ANSI, NFPA, UL, et al).

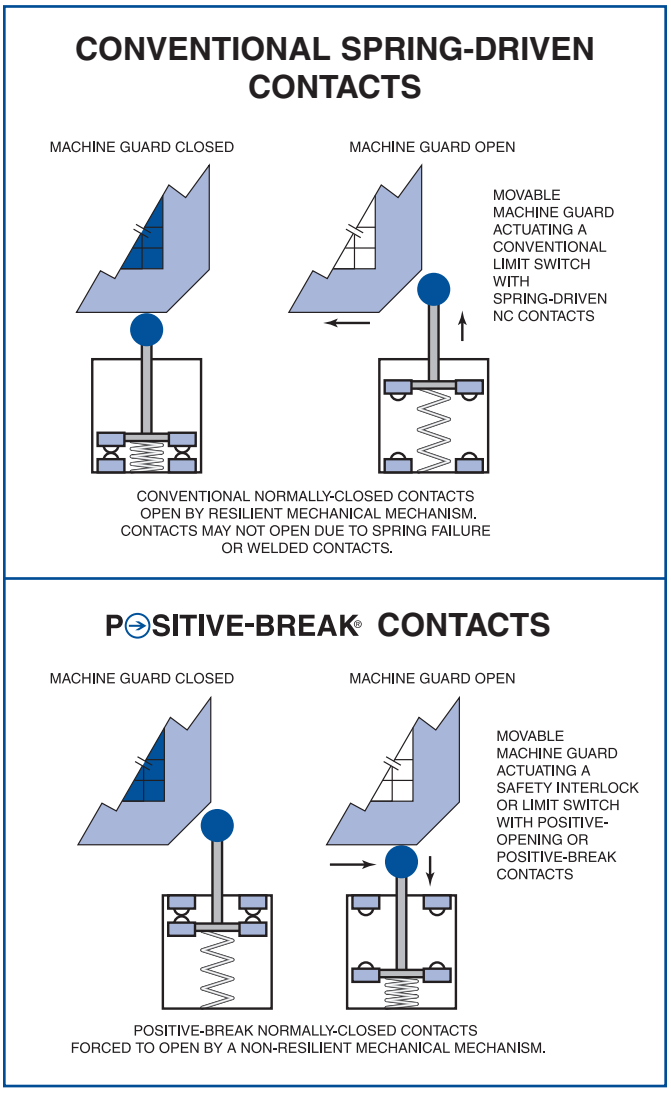


Figure 2
CONVENTIONAL VERSUS POSITIVE-OPENING CONTACTS

Performance Level: outlined in EN ISO 13849-1, a required level of safety for SRPCS. Designated PL_a through PL_e.

Point-of-Operation: the area(s) of a machine where material or the workpiece is positioned and a process is performed.

Point-of-Operation Guarding: a device or guard installed at the interface between the operator and the point-of-operation which is intended to protect personnel from hazardous areas.

Positive-Break Contacts: normally-closed (NC) contacts which, upon actuation, are forced to open by a non-resilient mechanical drive mechanism. Also called "positive-opening" or "direct-action" contacts. (See Figure 2.)

Positive-Guided Contacts: Normally-open (NO) and normally-closed (NC) contacts which operate interdependently such that the NO and NC contacts can never be closed at the same time. They are designed such that if one of the contacts welds/sticks closed,

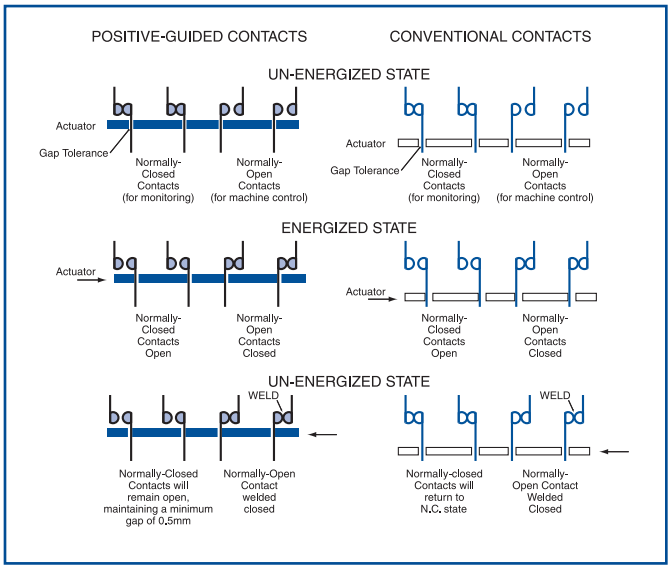


Figure 3

the other contacts cannot change state. (See Figure 3.) The interdependent operation between NO and NC contacts permits self-checking/monitoring of the functioning of relays and contactors featuring positive-guided contacts. Hence they are desirable in machine safety circuits where "fail-to-safe" or "control reliability" is desired. Also called "force-guided contacts".

Positive Linkage: a term applied to roller lever, rocking lever and other switch actuating members designed such that the integrity of the linkage between the actuator and the shaft is heightened (beyond a set screw on a smooth shaft) by its mechanical design. Examples of positive-linkages are pinned, square and serrated shafts. (See Figure 4.)

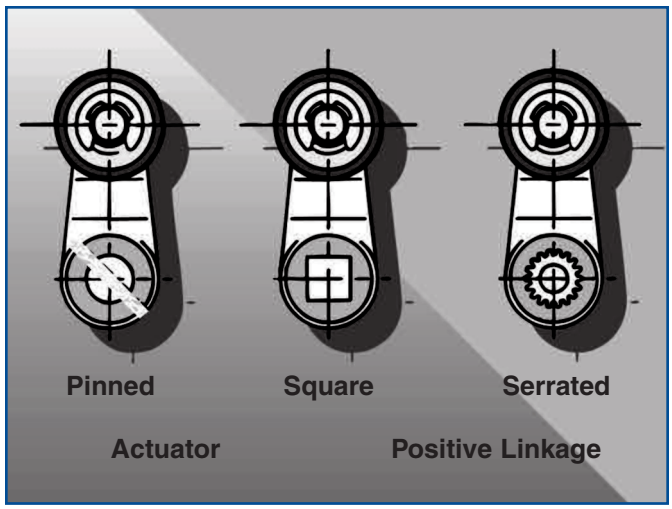


Figure 4

Positive-Mode Mounting: the mounting of a singe-piece safety interlock switch (e.g. a limit switch) such that the non-resilient mechanical mechanism which forces the normally-closed (NC) contacts to open is directly driven by the interlocked machine safety guard. In this mode (as opposed to "negative-mode mounting") the safety guard physically forces the NC contacts to open when the guard is opened. (See Figure 5.)

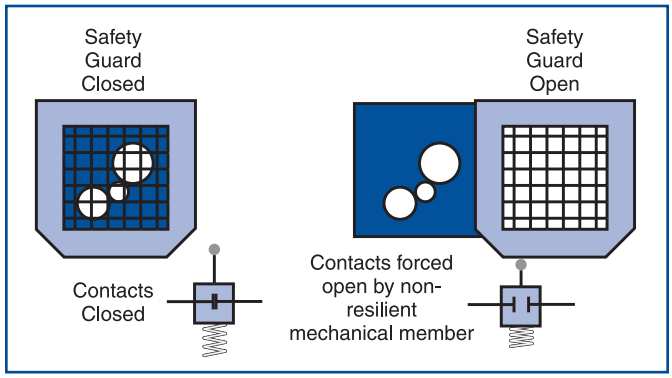


Figure 5

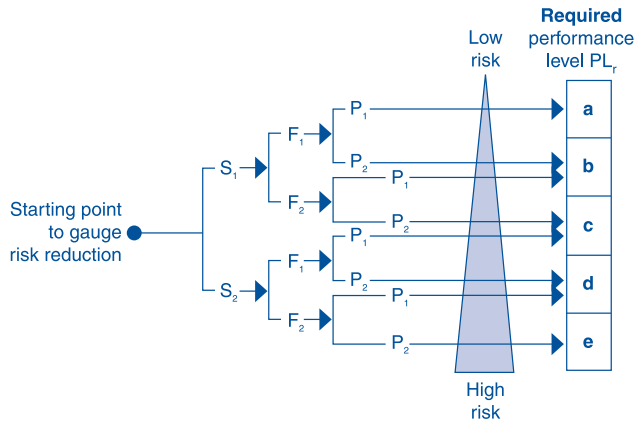
Positive-Opening Contacts: See "Positive-Break Contacts".

Push/Pull Operation: a term applied to emergency rope-pull switches designed to actuate when the rope/trip-wire is pulled and when it is pushed (goes slack). Such rope-pull switches provide a higher level of safety than units which only actuate when the trip-wire/rope is pulled.

Redundancy: the duplication of control circuits and/or components such that if one component/circuit should fail the other (redundant) component/circuit will ensure safe operation.

Risk Assessment: a systematic means of quantifying the relative level of danger different types of machine hazards present to the machine operator and/or maintenance personnel. This assessment is usually done in the early stages of the machine's design to permit such hazards to be designed-out or alternatively determine the scope of the safety system needed to protect personnel from possible injury. One approach suggested in EN ISO 13849-1 is summarized in Figure 6.

Figure 6



Selection of the Required Performance Level (PL_r)

Here the safety category is determined by the following parameters:
- S Severity of injury
  - S1 Slight injury
  - S2 Serious injury
- F Frequency and/or exposure time to the hazard
  - F1 Seldom to quite often
  - F2 Frequent to continuous
- P Possibility of avoiding the hazard
  - P1 Possible under specific conditions
  - P2 Scarcely possible

Safeguarding: protecting personnel from hazards using guards, barriers, safety devices and/or safe working procedures.

Safety Controller: an electronic and/or electromechanical device designed expressly for monitoring the integrity of a machine's safety system. Such controllers are designed using positive-guided (force-guided) relays. Depending upon the model, SCHMERSAL's safety controllers are capable of detecting the following types of potential safety system faults:

- Machine guard(s) open
- Guard monitoring switch/sensor failure
- Interconnection wiring "open circuit"
- Interconnection wiring "short circuit"
- Interconnection wiring "short-to-ground"
- Welded contact in controlled output device
- Failure of one of the safety controller's positive-guided relays
- Fault in the safety controller's monitoring circuit
- Insufficient safety controller operating voltage

Upon detection of a system fault, the safety controller will initiate a "machine stop" command and/or prevent the restarting of the machine until the fault has been corrected. The "stop" command may be immediate or time-delayed depending upon the model safety controller selected.

Safety Enable: (See “Authorized Output.”)

Safety Interlock Switch: a switch designed expressly to safely monitor the position of a machine barrier guard. Such switches typically feature positive-break contacts and are designed to be more tamper-resistant than conventional position/presence-sensing switches.

Safety Output: (See “Authorized Output.”)

Safety Relay: an electromechanical relay designed with positive-guided contacts.

Self-Checking: the performing of periodic self-diagnostics on the safety control circuit to ensure that critical individual components are functioning properly.

Self-Monitoring: see “Self-Checking”.

Single-Channel Safety System: a safety control system characterized by one safety interlock switch whose normally-closed contact is the sole input to a safety controller or a motor contactor. Such systems are unable to detect a short circuit failure in the interconnection wiring and are only recommended for addressing Safety Categories B, 1 and 2 (see “Risk Assessment”).

Solenoid-Latching Safety Interlock Switch: a two-piece safety interlock (actuating key and switch mechanism) whose design prevents the removal of the actuating key until released by an integral latching solenoid. Solenoid latching is typically controlled by a time-delay, motion detector, position sensor or other control components.

Stop Categories:

“0” Requires immediate removal of power from the controlled devices.

“1” Allows for a time delay up to 30 seconds for removal of power. This is commonly used with drive systems where immediate removal of power may result in a longer stop time.

SRPCS: Safety Related Parts of Control Systems — (sub)systems which perform a safety function.

Tamper-Resistant: a term applied to safety interlock switches referring to their relative ability to be defeated or bypassed using simple, readily available means such as a screwdriver, paper clip, piece of tape or wire, etc. Switches and sensors designed expressly for use as machine guard safety interlocks are designed to be more “tamper-resistant” than conventional switches/sensors (e.g. proximity switches, reed switches, conventional limit switches).

Time-delayed Authorized Outputs: a safety controller’s authorized outputs whose activation is delayed (up to 30 seconds) to satisfy Stop Category 1 requirements.

Trailing-edge Reset: (See “Manually-monitored Reset.”)

Two-Hand Control: a machine control system which requires “simultaneous” use of both of the operator’s hands to initiate a machine cycle.

UL (Underwriters Laboratories): an independent testing and standards-making organization. UL tests products for compliance to relevant electrical and safety standards/requirements.