

A brief Q&A tutorial guide for those concerned with:

- Providing a safer workplace
- Protecting workers from injury
- Reducing liability risks
- Eliminating the high indirect costs associated with worker injuries
- Meeting OSHA and ANSI safety guidelines
- Complying with the European Machinery Directive and CE Requirements



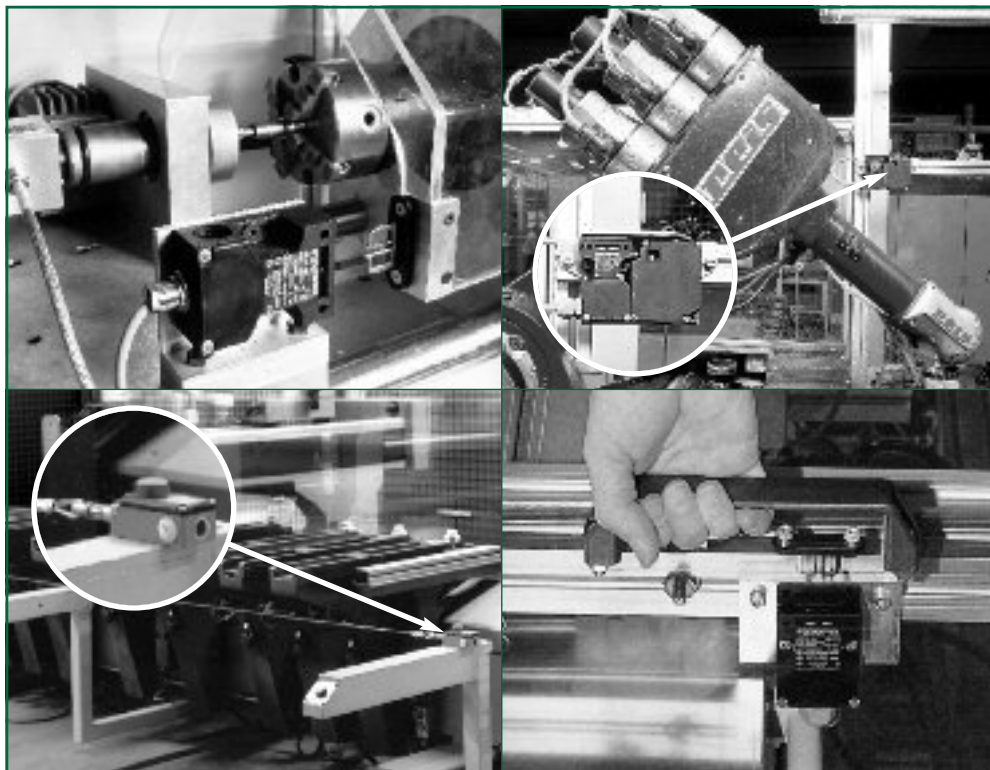
MAN-MACHINE SAFEGUARDING

Requirements & Techniques

For more than 60 years, Schmersal has dedicated itself to understanding man-machine safety hazards. Based on that experience, this handbook has been prepared. It represents a compilation of our responses to the most frequently-asked questions from people who are actively engaged in designing machine-guard systems. A complementary tutorial video is also available upon request.

The handbook concludes with a convenient condensed catalog of selected Schmersal interlock safety switches and controllers that satisfy a vast array of safety applications and challenges. Should you desire more detailed technical data, please write or call for these product catalogs.

TYPICAL SAFETY INTERLOCK SWITCH APPLICATIONS



INTRODUCTION

CHANGING MAN-MACHINE SAFEGUARDING RULES

Today worker safety is an issue of major concern to manufacturers worldwide. OSHA guidelines, more stringent ANSI standards, and the recently adopted European Machinery Directive (EMD) are evidence of the increased emphasis being given to employee safety in the workplace.

Selected reference standards and guidelines aimed at achieving heightened levels of safety include:

- American National Standards Institute
(ANSI) B11.19 2003
(ANSI) B11.20 2004
- OSHA 29 CFR 1910
- ISA S84.01
- ANSI/RIA 15.06-1999
- IEC 204 Part 1
- EN 292 Parts 1 & 2
- EN 954 Part 1
- European Union Machinery Directive (EMD)
89/392/EEC

Each establishes minimum safety requirements to which manufacturers and employers must comply. And each presents new challenges to the plant safety specialist and equipment designer... especially where safety guards ancillary to the production equipment's functional design are required. For example, ANSI Standard B11.19-2003 applies to *both* machine tool OEM's and *their* industrial users.

NEW SAFETY CONCEPTS AND TECHNIQUES

The goal of these new and emerging guidelines is to provide heightened levels of protection to machine operators, helpers, and maintenance personnel. Toward this goal they have embraced several new safety system concepts including:

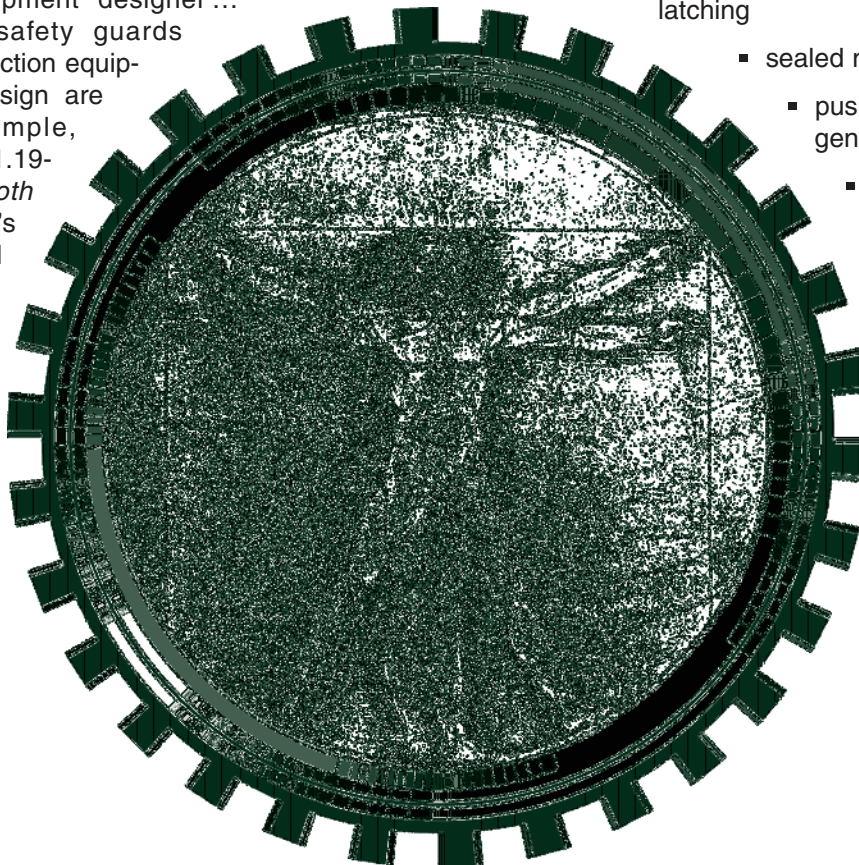
- positive-break contacts
- greater tamper-resistance
- positive-guided relays
- fault detection
- single component failure control reliability

Conventional limit switches, proximity sensors, magnet switches and other conventional position-sensing and control devices traditionally used as safety interlocks do not meet contemporary requirements. Consequently, when used in such applications, they are unsafe.

“SAFETY-SPECIFIC” COMPONENTS

New switches, sensors and controls have been designed specifically for safety applications. They include:

- keyed interlock switches
 - keyed interlock switches with solenoid latching
 - sealed non-contact sensors
- push/pull operated emergency cable-pull switches
- positive-break hinge switches
- positive-break limit switches
- positive-break safety edges
- safety controllers
- light curtains & beams
- laser scanners
- safety door handle systems



Each of these components is designed to overcome one or more of the limitations of conventional “non-safety” components, and help the safety specialist and equipment designers to better address their responsibility ... to ensure that machinery, built or purchased, does not expose the operators, helpers or maintenance personnel to hazards.

Additionally, safety specialists and equipment designers have recognized:

- (1) the greater degree of protection the new devices offer
- (2) the importance of providing the greatest level of worker protection
- (3) the need to go beyond mere compliance with standards/guidelines to minimize their company’s liability exposure
- (4) their responsibility to ensure that equipment, built or purchased, must not pose hazardous conditions to the employees when operated.

These safety-specific components are available for review on our website at www.schmersalusa.com ... or ask for Catalog GK-1.

TOWARD A BETTER UNDERSTANDING

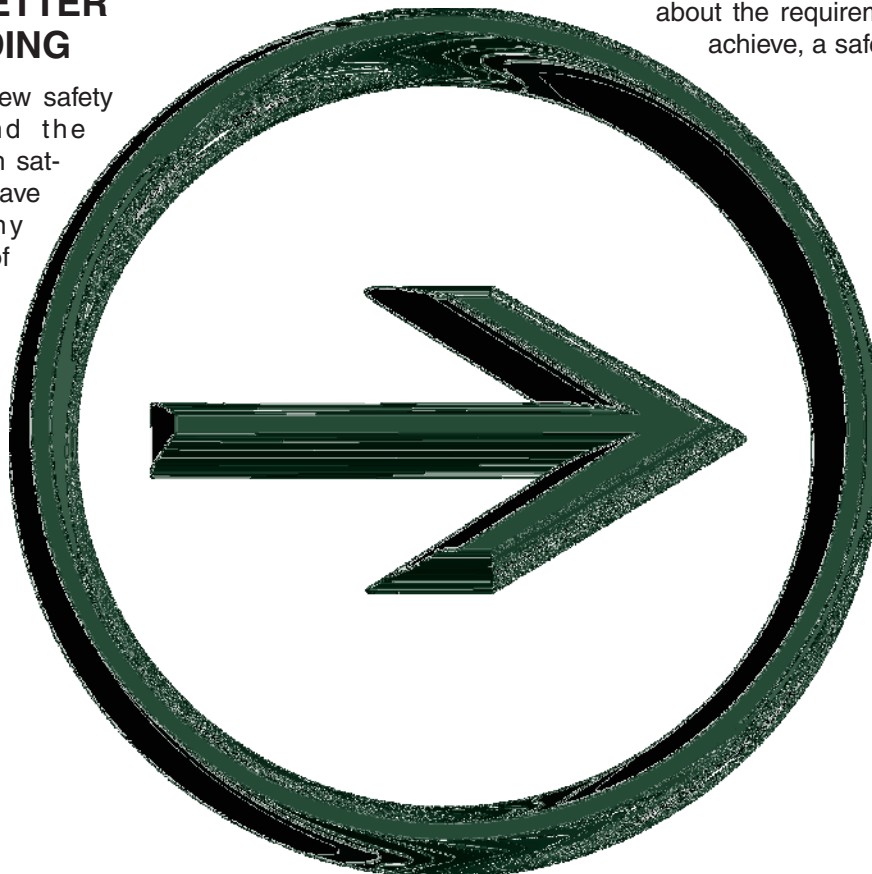
The emergence of new safety requirements, and the related devices which satisfy these criteria, have precipitated many questions. Typical of these are:

- What exactly are “positive-break” devices?
- What is “positive-mode” installation, and why is it safer?
- What are “fail-to-safe” devices?
- What are “positive-guided” contacts, and why are they recommended in safety circuits?
- How do I, the OEM or user, benefit from use of such safety devices?
- What is meant by “control reliability,” and how is it achieved?
- What is “risk assessment,” and how is it measured?

The answers to these, and other related questions, are the subjects of this brief booklet. We hope it provides you with:

- a better understanding of the current and emerging machinery safety requirements
- a basic understanding of the unique safety devices designed to meet these requirements
- a knowledge of the benefits to be derived from the use of such safety components.

And we hope it stimulates you to learn more about the requirements for, and ways to achieve, a safer workplace.



International symbol for Positive-Break contacts

TABLE OF CONTENTS

Topic	Page
I. Man-Machine Safeguarding Principles and Practices	5
II. Control Reliability	15
III. Risk Assessment	19
IV. Safety Standards, CE Marking and the European Machinery Directive ...	23
V. Safety Controllers	26
VI. Applications and Solutions	29

MACHINE GUARD CLOSED MACHINE GUARD OPEN

POSITIVE-BREAK NORMALLY-CLOSED CONTACTS
FORCED TO OPEN BY A NON-RESILIENT MECHANICAL MECHANISM.

Positive-Break Contacts

Safety Guard Closed Safety Guard Open

Contacts Closed Contacts forced open by non-resilient mechanical member

Positive-Mode Mounting

Actuator Gap Tolerance Normally-Closed Contacts (for monitoring) Normally-Open Contacts (for machine control)

Actuator Normally-Closed Contacts Open Normally-Open Contacts Closed

Positive-Guided Contacts

Starting Point

		Safety Category				
		B	1	2	3	4
S1	F1	P1	●	○	○	○
		P2	●	●	○	○
	F2	P1	●	●	○	○
		P2	●	●	●	○

Risk Assessment

I. Man-Machine Safeguarding Principles & Practices

1

Why should machine guard interlocks be “tamper resistant”?

Safety professionals recognize that, in many factories, workers often override or bypass safeguards intended to protect them from injury. Reported motivation includes real or perceived inconvenience, production incentives, familiarity with the equipment, or simply the challenge presented by the presence of the safeguard to be defeated.

Consequently, manufacturers are increasingly recognizing the need for, and their obligation to provide, safety interlocks which are not easily defeated/bypassed by the operator or maintenance personnel.

Additionally, safety standards-making groups encourage use of interlocks which are not easily defeated using simple, readily-available means (such as a paper clip, tape, rubber band, piece of rope, screwdriver, etc.).

For example, the American National Standards Institute’s (ANSI) B11.19-2003, Reference Standard for Safeguarding Machine Tools specifically requires:

- Barrier guards that protect against unauthorized adjustment or circumvention.
- Interlock devices that are not easily bypassed.
- Reduced liability

With the growing number of product liability cases, companies are recognizing the benefits of designing safety circuits with interlock devices that are difficult to defeat. To further reduce their liability exposure, firms are selecting only those devices that have been tested and certified for use in safety applications by a recognized, independent third-party agency.

Manufacturers are encouraged to surpass safety design expectations. As cited at a recent DESIGN NEWS seminar entitled “Product Liability — A Survival Kit for the 90’s”, jurors expect companies to go beyond mere compliance. They give greater benefit to firms who have designed their products with the latest state-of-the-art machine guarding safety devices.

2

What is meant by the term “difficult to defeat” when related to safety interlock switches in safety standards such as ANSI B11.19, ANSI B11.20, ANSI-RIA 15.02, OSHA 1910.212, et al?

“Difficult to defeat” is a subjective term related to workers’ propensity to override or bypass safety devices intended to protect them from injury. Colloquially it means that the relevant devices or systems cannot be defeated or bypassed using readily available means

(such as a piece of wire, tape, simple hand tool, etc.). It implies the basic safety interlock switch design serves as a deterrent to easily overriding or bypassing its intended function.

3

How is this requirement (“difficult to defeat”) being addressed by safety interlock switch manufacturers?

Safety interlock switch manufacturers are addressing this requirement by:

- Designing two-piece keyed interlocks which feature a geometrically-unique actuating key and associated operating mechanism which function together to deter “bypassing”.
- Designing “coded-magnet” sensors whose multiple reed contacts can only be actuated in the presence of a matched magnetic field array.
- Encouraging “positive-mode” mounting of single-piece interlock switches.

4

What are “positive-break” safety interlocks?

“Positive-break” safety interlocks are electromechanical switches designed with normally-closed (NC) electrical contacts which, upon switch actuation, are *forced to open by a non-resilient mechanical drive mechanism*. (Spring actuators are not considered positive-break mechanisms.)

One example of a “positive-break” safety interlock is shown in the photo below. This third-party certified and widely used safety switch features a two-piece construction: an electromechanical switching mechanism and a geometrically-unique actuator key.

A simple illustration of this design concept is shown in Figure 2.

The actuator key is typically mounted to a movable guard – such as an access door, protective grating, equipment hood, or plexiglass safety cover. When the guard is closed, the actuator mates with the electromechanical switching mechanism. Upon opening of the movable guard, the actuator key mechanically rotates a cam mechanism – *forcing the NC electrical contacts to open the safety circuit*.

For machine applications with residual motion after shut-down, key actuated interlocks are available with a solenoid latch – which, in conjunction with a time-delay, motion detector, position sensor or other machinery status monitor, can delay access to hazardous areas until safe conditions exist.

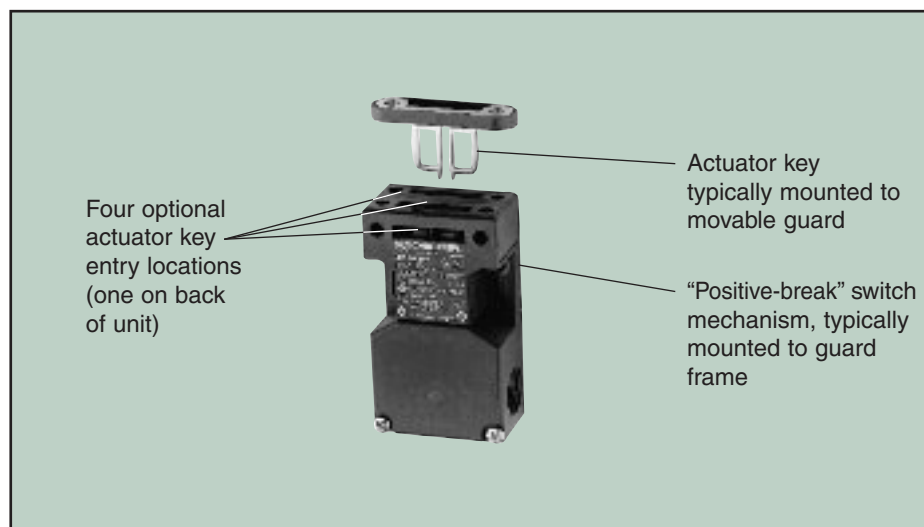
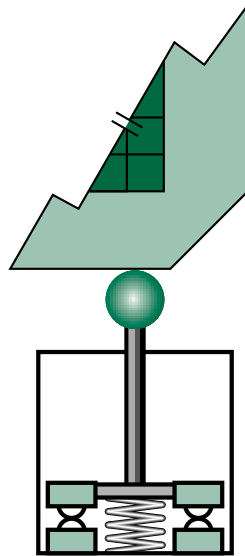
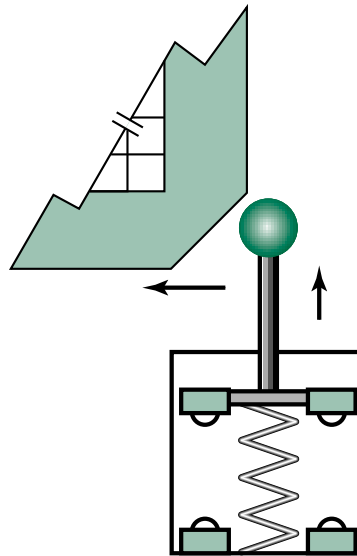


FIGURE 1

MACHINE GUARD CLOSED



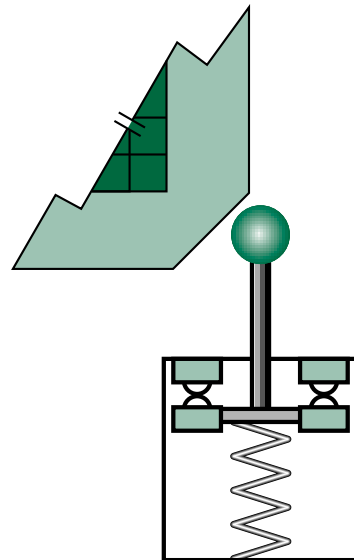
MACHINE GUARD OPEN



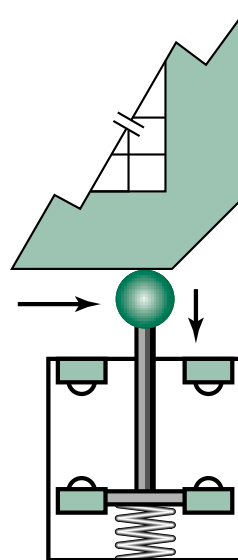
MOVABLE
MACHINE GUARD
ACTUATING A
CONVENTIONAL
LIMIT SWITCH
WITH
SPRING-DRIVEN
CONTACTS

CONVENTIONAL NORMALLY-CLOSED CONTACTS
OPEN BY RESILIENT MECHANICAL MECHANISM.
CONTACTS MAY NOT OPEN DUE TO SPRING FAILURE
OR WELDED CONTACTS.

MACHINE GUARD CLOSED



MACHINE GUARD OPEN



MOVABLE
MACHINE GUARD
ACTUATING A
SAFETY INTERLOCK
SWITCH WITH
POSITIVE-BREAK
CONTACTS

POSITIVE-BREAK NORMALLY-CLOSED CONTACTS
FORCED TO OPEN BY A NON-RESILIENT MECHANICAL MECHANISM.

FIGURE 2

Conventional versus Positive-Break Contacts

5

Are conventional electromechanical limit switches designed with “positive-break” contacts?

Conventional “limit” switches are typically designed to use a spring force to open normally-closed electrical contacts. Such designs are subject to two potential failure modes:

- Spring failure
- Inability of the spring force to overcome “stuck” or “welded” contacts.

When “actuated,” either situation may result in an unsafe condition due to failure to open normally-closed contacts. Consequently, such designs are not certified or recognized as suitable for safety applications.

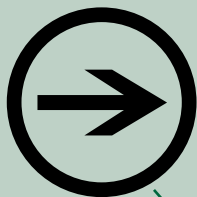
SCHMERSAL offers several “limit” switches designed with “positive-break” contacts in both snap-acting and slow-action models for use in safety applications.

6

How can I recognize “positive-break” safety interlock switches?

Devices which feature a “positive-break” design carry the following internationally-recognized (IEC) safety symbol:

These designs meet the international requirements established for such safety interlock switches.



Typically, the positive-break symbol can be found on products as part of product specification identification, as shown below.



FIGURE 3

7

What is meant by a “positive linkage” switch actuator, and why is it recommended for safety applications?

A “positive linkage” switch actuator is designed to eliminate possible slippage between the actuator and its

mounting shaft. Examples of such designs are pinned, square and serrated shafts (see Figure 4, below).

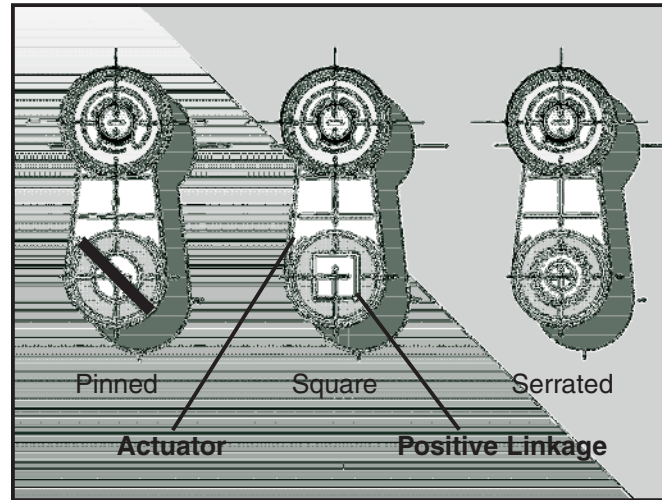


FIGURE 4

8

What is “positive-mode” mounting and why is it essential in safety applications?

“Positive-mode” mounting assures that an electro-mechanical safety interlock switch is positively-actuated when equipment or machinery shut-down is desired.

mechanical mechanism which forces the normally closed (N.C.) contacts to open is directly driven by the safety guard. In this mounting mode, opening the safety guard physically forces the N.C. contacts to open when the guard is open.

Safe “Positive-Mode” Mounting (Figure 5)

When mounted in the positive-mode, the non-resilient

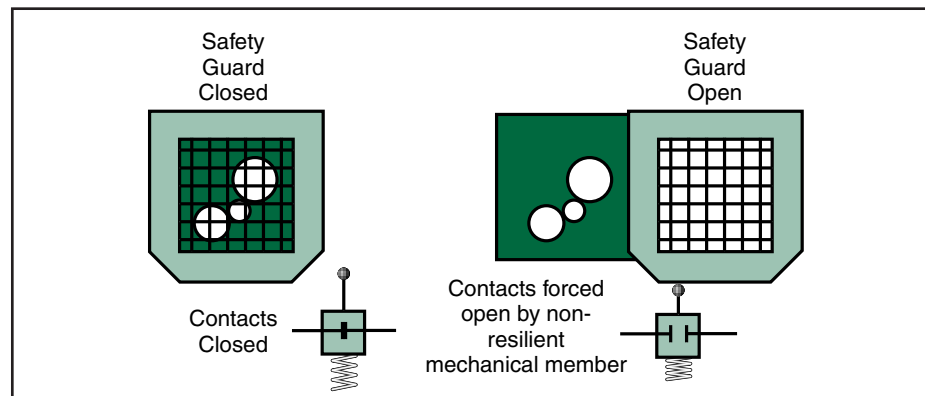


FIGURE 5
POSITIVE-MODE INSTALLATION

Unsafe “Negative-Mode” Mounting (Figure 6)

When mounted in the “negative-mode,” the force applied to open the normally-closed (N.C.) safety circuit contacts is provided by an internal spring. In this mounting mode the N.C. contacts may not open when the safety guard is “Open.” (Here welded/stuck contacts, or failure of the contact-opening spring, may result in exposing the machine operator to a hazardous/unsafe area of the machinery.)

Positive-mode installation is especially important when using single-piece safety interlock switches. This installation mode takes full advantage of the device’s “positive-break” design — using the *external* force applied by the safety guard to open the N.C. contacts.

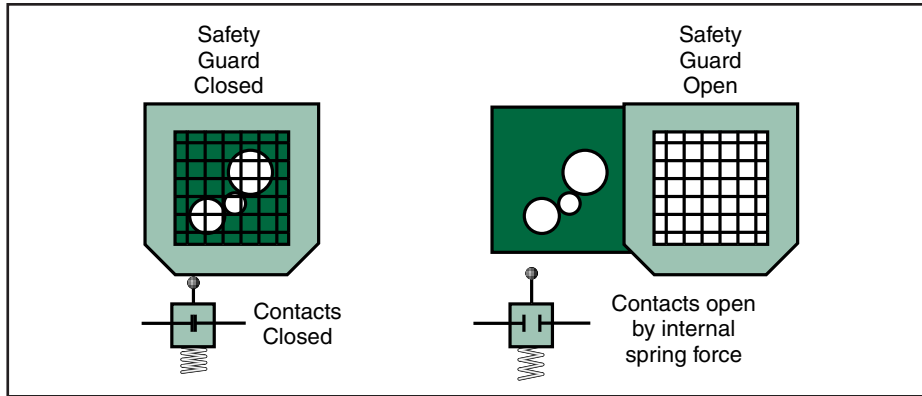


FIGURE 6
NEGATIVE-MODE INSTALLATION

9 What are the risks of installing single-piece, safety interlock switches in the “negative mode”?

When mounted in the “negative-mode” (see Figure 6 above), single-piece safety interlock switches can be easily defeated/circumvented by the operator ... often simply by taping down the switch actuator when the safety guard is open.

In addition, spring-driven, normally-closed contacts can fail to open due to sticking, contact welding, or a spring failure.

Under such circumstances the operator or maintenance personnel may be exposed to an *unsafe or hazardous condition*.

Consequently, where possible, two-piece, key-actuated, tamper-resistant safety interlocks are recommended. These devices are designed to be difficult to defeat, while providing the assurance of safety circuit interruption inherent with “positive-break” interlock switch designs.

10

What are “self-checking,” “redundancy,” and “single-fault tolerance”?

Self-Checking: The performing of periodic self-diagnostics on a safety control circuit to ensure critical individual components are functioning properly. Faults or failures in selected components will result in system shut-down.

Redundancy: In safety applications, redundancy is the duplication of control circuits/components such that if one component/circuit should fail, the other (redundant) component/circuit will still be able to generate a stop signal. When coupled with a “self-checking” feature, a safety circuit component failure, or component failure within the safety circuit monitoring module or safety relay module,

will be automatically detected and the machine shut down until the failure is corrected.

Single-Fault Tolerance: A safety circuit is considered to be single-fault tolerant if no foreseeable single fault will prevent normal stopping action from taking place.

Rugged, “fail-to-safe,” safety circuit controllers (often called safety relay modules) are also available that incorporate the above features to satisfy the “control reliability” requirements of existing domestic and international safety standards.

11

Are cable-pull switches acceptable for use in E-Stop circuits?

OSHA and the European safety standards permit use of cable-pull switches in E-Stop circuits provided they:

- (1) Operate whether the cable is pulled or goes slack (e.g. breaks or is cut).
- (2) Feature positive-break NC contacts.
- (3) Must be manually reset before the controlled equipment can be restarted.

In addition, European Norm EN418 requires that the switch latch at the same time that the contacts change state.

SCHMERSAL offers a variety of cable-pull switches that meet both EN418 and the OSHA guidelines. These are complemented by several safety circuit controllers and safety relay modules designed expressly for use in E-Stop circuits.

12

Are reed switches recommended or acceptable in safety circuits and, if so, under what conditions?’

Reed switches may be used as interlocks in safety circuits provided:

- they are designed to be actuated by a specific (coded) magnetic-field array matched to the switch’s reed-array pattern.
- they are used in combination with a safety controller capable of periodically checking the integrity and performance of the reed switch contacts.

One such combination is shown in Figure 8, below.

Coded-magnets are required to actuate the sensor, thus making it difficult for the operator or maintenance personnel to “defeat” or “bypass.”

The safety controller features multiple safety relays with positive-guided contacts, redundant control circuits, and self-diagnostics that check safety system operation. In

the event of a component or interconnection wiring failure in the safety circuit, or in the safety circuit controller, the unit will shut down the system in a “safe” state.

Note: Reed switches used without an approved safety circuit controller do not satisfy safety requirements. Reed switches are susceptible to sticking due to power surges, shock, or vibration.

Additionally, reed switches tend to fail in the “closed” position. This failure mode cannot be addressed by using a fuse. To ensure reliability of a safety circuit using reed-type switches, use of a safety controller is required. Depending upon the application, it is also recommended that they feature two independent contacts to permit dual-channel monitoring.

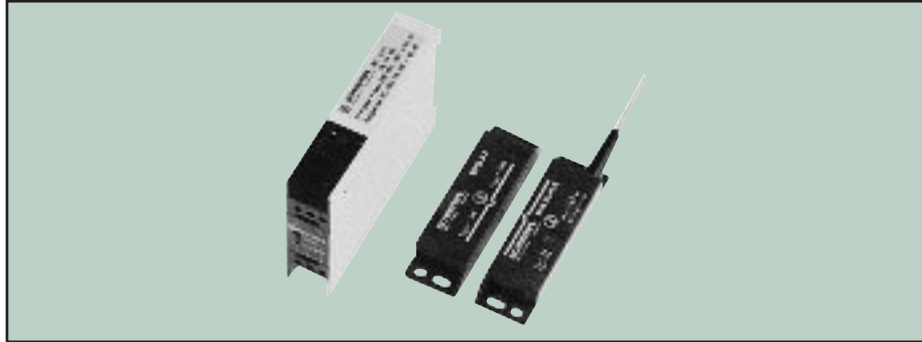


FIGURE 8

13

What is meant by “controlled access”?

“Controlled access” generally refers to a movable machine guard that is designed such that it can only be opened under specific conditions. Typically such movable guards restrict access to an area of a machine which continues to present a hazard to the operator immediately upon the removal of power. In these situations opening of the guard is prevented until the hazardous condition has abated.

This is usually achieved by a solenoid-latching interlock switch controlled by a motion detector, position sensor, time-delay or other machine-status monitor which releases the interlock (allowing the operator to open the guard) only after safe conditions exist.

14

What is “diverse redundancy,” and how does it heighten the reliability of a safety circuit?

“Diverse redundancy” is the use of different types of components and software in the construction of redundant circuits/systems performing the same function. Its use is intended to minimize or eliminate failure of redun-

dant circuits and components due to the same cause (“common-cause” failure). Such designs serve to increase the functional reliability of the safety circuits and systems.

15

Why are safety interlock switches and safety controllers required?

For machinery builders who export to the European Union, the use of such components designed expressly for machine guarding safety systems is mandated by the requirements of the European Machinery Directive and the need to comply with relevant safety standards. These requirements include:

- Use of interlock switches that feature positive-break normally closed contacts.
- Use of interlock switches or machine guarding position sensors, which are tamper-resistant/difficult to defeat.
- (Where risk level dictates) the need to monitor the integrity of the safety circuit components and its interconnection wiring to ensure the system will function properly when called upon to do so.

For machinery builders selling in the U.S., the use of such components is encouraged by the safety guidelines and standards of the Federal government and several industry standards-making groups including:

- OSHA (Occupational Health & Safety Administration)
- ANSI (American National Standards Institute)
- UL (Underwriters Laboratories)
- ISA (Instrument Society of America)
- SAE (Society of Automotive Engineers).

16

As an OEM, what are the benefits of using positive-break and tamper-resistant interlocks in safety applications?

Proper selection and installation of safety interlocks which have been *tested and certified by an approved, independent safety testing body* benefits the equipment manufacturer by:

- Providing greater protection from injury for machine operators, maintenance personnel, set-up and other user personnel.
- Satisfying international safety regulations ... a must for U.S. equipment manufacturers who wish to export to the European Economic Community.

- Enhancing product marketability.
- Satisfying safety standards and guidelines against which manufacturer's responsibility, in the event of an injury, is judged.
- Reducing liability risks.
- Minimizing insurance claims/costs.

17

As an “in-plant” user, what are the benefits of using positive-break, and/or tamper-resistant interlocks in safety applications?

Proper selection and installation of such safety interlocks which have been *tested and certified by an approved, independent testing body* benefit the in-plant user by:

- Providing greater protection from injury for machine operators, maintenance personnel, and other employees.
- Reducing liability risks.
- Minimizing insurance claims/costs.
- Satisfying safety standards and guidelines against which employer responsibility, in the event of an injury, is measured.
- Reducing the indirect costs associated with worker injury (e.g. lost production, loss of skilled workers, reduced productivity due to employee stress, etc.)

18

What are the benefits of using SCHMERSAL safety interlock switches and related controls?

While SCHMERSAL is not the only manufacturer of such devices, there are a number of factors which favor your consideration. These include:

- (1) All SCHMERSAL safety interlocks have been third-party tested and certified to meet relevant directives — all are CE-compliant.
- (2) Each can be provided with a Declaration of Conformity.
- (3) Each has been designed expressly for safety applications to meet the requirements of ANSI, OSHA and the European Machinery Directive.
- (4) SCHMERSAL's individually-coded keyed interlocks (AZ16zi, AZ17zi, and AZM170zi) provide the highest level of tamper resistance.
- (5) SCHMERSAL's safety interlocks and related controllers have been proven in thousands of installations worldwide.
- (6) SCHMERSAL's microprocessor-based Series AES safety controllers feature integrated systems diagnostics which, using a visual colored LED display pattern, help identify the type of system fault that has occurred and its location (to minimize downtime).
- (7) SCHMERSAL's safety controllers are easily integrated with their more than 200 “positive-break” interlock switches and coded-magnet sensors to achieve any desired safety level. And, they are also compatible with other manufacturers' safety-approved components.

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.

21

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.

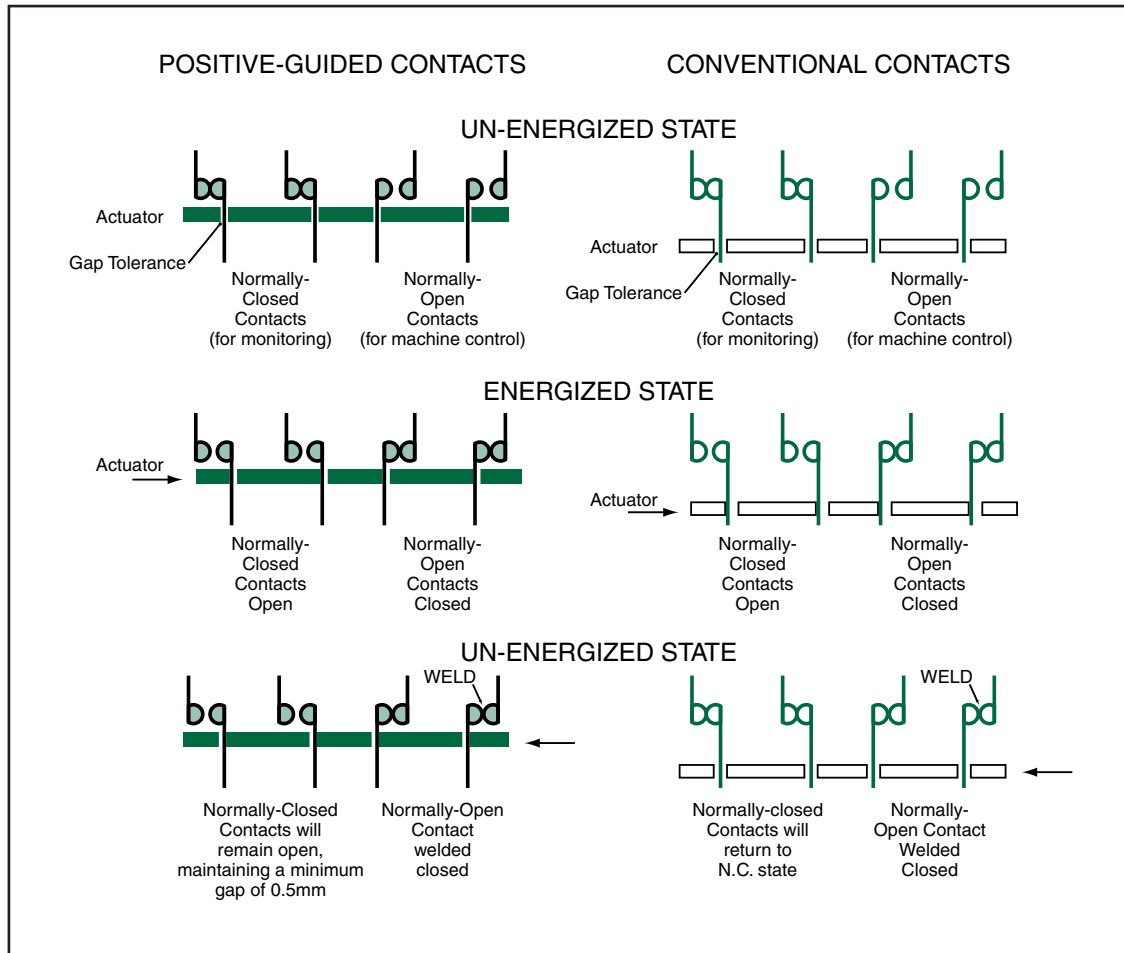


FIGURE 9
POSITIVE-GUIDED VS. CONVENTIONAL CONTACTS

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 B11.19-2003 Machine Tool Safeguarding...

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

Annex C: Performance of safety-related function(s)

"Control reliability is not provided by simple redundancy. There must be monitoring to assure that redundancy is maintained. Control reliability uses monitoring and checking to determine that a discernable component, module, device or system has failed and that the hazardous motion (or situation) is stopped, or prevented from starting or restarting. Control reliability ensures that a failure of the control system or device will not result in the loss of the safety-related function(s)."

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.

III. Risk Assessment

26 What is “risk assessment”?

Various machines present different types of hazards and risks to the operator and/or maintenance personnel. Risk assessment is a systematic means of quantifying these

risk levels in order to determine the scope of the required safety system needed to protect personnel from possible injury.

27 How do I go about assessing the risk level presented by a machine or manufacturing process?

Different machines and processes have different levels of relative risk. Determining this relative risk level involves evaluating four major factors. These include:

- (1) Severity of the potential injury.
- (2) Frequency of exposure to the potential hazard.
- (3) Possibility of avoiding the hazard if it occurs.

One approach provides guidelines for risk assessment based upon five defined levels of risk. These levels range from the lowest risk (level B) in which the severity of injury is slight and/or there is relatively little likelihood of occurrence, to the highest risk (level 4) in which the likelihood of a severe injury (if the safety system fails) is relatively high.

This particular method is depicted in Figure 10, in which the following qualitative definitions apply:

- S: Severity of potential injury
 S1: slight injury (bruise)
 S2: severe injury (amputation or death)
- F: Frequency of exposure to potential hazard
 F1: infrequent exposure
 F2: frequent to continuous exposure
- P: Possibility of avoiding the hazard if it occurs (generally related to the speed/frequency of movement of hazard point and distance to hazard point)
 P1: possible
 P2: less possible

For further details of the above, the reader is referred to the EN 954-1 (Safety of Machinery: Principles for the Design of Related Control Systems).

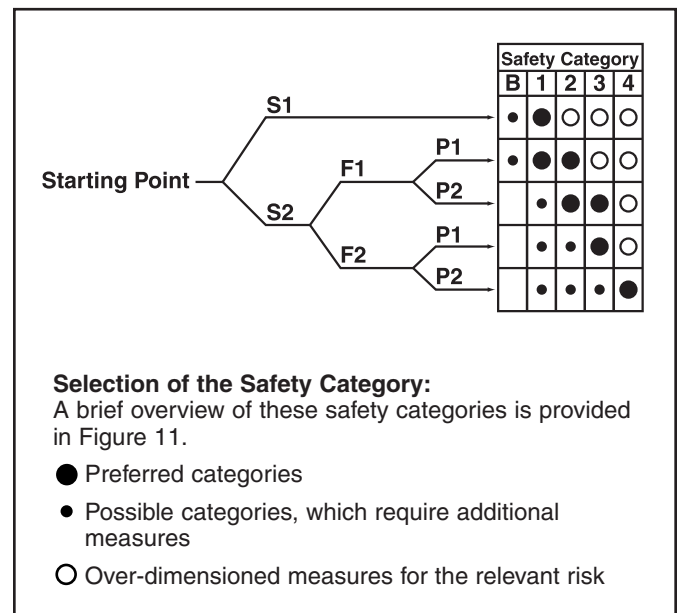


FIGURE 10

Another methodology is outlined in ANSI’s Technical Report B11.TR3. This guideline suggests a “task-based” review of potential hazards by both the equipment designer and the ultimate end-user.

28

What are the defined levels of *relative risk* for machinery within which the *safety system* should be designed?

The European harmonized standard, EN954-1 (Safety of Machinery — Design of Safety Related Control Systems), outlines five relative levels of risk associated with the operation/maintenance of machinery. The greater the possibility and/or severity of injury, the

greater the requirements are on the design and integrity of the machine safety systems.

In general, these levels of risk are defined as follows:

Safety Cat.	General Safety System Requirements	General Safety System Behavior	Safety Cat.	General Safety System Requirements	General Safety System Behavior
B	Safety system designed to meet operational requirements and withstand expected external influences. (This category is usually satisfied by selecting components compatible with the application conditions ... e.g. temperature, voltage, load, etc.)	A single fault or failure in the safety system can lead to the loss of the safety function.	3	Safety system must meet the requirements of Category B. In addition the safety control system must be designed such that a single fault will not lead to the loss of the safety function. And, where practical, the single fault will be detected. (This requires redundancy in the safety circuit monitoring module and the use of dual-channel monitoring of the input and output devices such as machine guard interlock switches, E-stop pushbuttons, safety relays, etc.)	Here a single fault or failure in the safety system will not lead to the loss of the safety function and, where possible, will be detected.
1	Safety system must meet the requirements of Category B, but must use "well-trying" safety principles and components. "Well-trying" principles and components include those which: <ul style="list-style-type: none"> ▪ avoid certain faults ... e.g. short circuits. ▪ reduce probability of faults ... e.g. over-rating selected components, over-dimensioning for structural integrity. ▪ detect faults early ... e.g. ground fault protection. ▪ assure the mode of the fault ... e.g. ensure an open circuit when it is vital that power be interrupted should an unsafe condition arise. ▪ limit the consequences of the fault. 	A single fault or failure in the safety system can lead to the loss of the safety function. However, the use of "well trying" safety principles and safety components results in a higher level of safety system reliability.	4*	Safety system must meet the requirements of Category B. In addition the safety control system must be designed such that a single fault will not lead to the loss of the safety function and will be detected at or before the next demand on the safety system. If this is not possible, then the accumulation of multiple faults must not lead to the loss of the safety function. (This also requires redundancy in the safety circuit and the use of dual-channel monitoring of the input and output devices such as machine guard interlock switches, E-stop pushbuttons, safety relays, etc. Here the number of allowable faults will be determined by the application, technology used, and system structure.)	Here a single fault or failure in the safety system will not lead to the loss of the safety function, and it will be detected in time to prevent the loss of the safety function.
2	Safety system must meet the requirements of Category B. In addition the machine shall be prevented from starting if a fault is detected upon application of machine power, or upon periodic checking during operation. (This suggests the use of a safety relay module with redundancy and self-checking. Single-channel operation is permitted provided that the input devices ... such as machine guard interlocks, E-stop pushbuttons, et al ... are tested for proper operation on a regular basis.)	Here, too, a single fault or failure in the safety system can lead to the loss of the safety function between the checking intervals. However, periodic checking may detect faults and permit timely maintenance of the safety system.	<p>*Category 4 safety requirements are usually associated with extremely high-risk applications. Since general machine design practice respects classic safety hierarchy, in which most machine hazards are either:</p> <ul style="list-style-type: none"> ▪ designed out, ▪ guarded against (if they cannot be designed out), and, ▪ (as a last resort) warned against, <p>Category 4 requirements may arise relatively infrequently.</p>		

FIGURE 11

29

Which of these risk category safety system requirements is consistent with OSHA and ANSI's requirement for a "control reliable" safety circuit?

Within the above defined levels of risk, a Category 3 safety system would satisfy OSHA and ANSI's requirement for a "control reliable" safety circuit. Here use of an appropriate fail-to-safe, safety controller in combination with one or more safety interlock switches and/or coded-magnet sen-

sors will meet the single component failure detection and system shutdown criteria, while preventing a successive machine cycle from being initiated when a fault is detected.

30

How can the safety system requirements, and the requirement for machine safety system "control reliability," be satisfied?

Machine safety system control reliability can be achieved through use of:

- Safety components which feature fail-to-safe design.
- Electromechanical safety interlocks which feature positive-break N.C. contacts.
- Use of safety relays which feature positive-guided contacts.

- Use of self-checking safety controllers.
- Use of redundant monitoring/checking circuits and related safety system components.

The selection of these components will, of course, be a function of the application and its level of risk assessment. SCHMERSAL has available an *applications and safety circuit wiring handbook* to serve as a reference for selecting, designing and wiring the appropriate safety circuit for a given level of risk assessment.

31

Are safety controllers needed when addressing Category 1 or 2 safety system requirements?

Category 1 and 2 safety system requirements can be achieved without the use of safety controllers. However, this requires very careful design of the safety control circuit and a thorough understanding of the standards relat-

ed to the Machinery Directive. Use of a safety circuit controller ensures meeting Category 1 and 2 requirements without a time-consuming study of the machine control system.

32

How common are Category 4 safety system requirements and how can they be satisfied?

Category 4 safety system requirements are typically associated with extremely high-risk applications in which:

- (a) The severity of a potential injury is extremely high (e.g. amputation or death).
- (b) The employee/operator is exposed to the hazard highly frequently or continuously.
- (c) There is little possibility of the employee/operator avoiding the hazard.

Classic safety hierarchy states that dangers should be:

- (1) designed out;
- (2) guarded against, if they cannot be designed out; and then
- (3) (as a last resort) warned against.

Since this classic safety hierarchy reflects general machine design practice, few machines present Category 4 risk conditions.

When Category 4 safety requirements are encountered (that is, when the safety control system must be able to detect any single fault, or provide multiple fault tolerance, without loss of the safety function), it is important to remember these define the performance requirements of the overall safety system ... not of the individual components. (This, of course, is true for all safety categories ... not only Category 4.)

In this “system” context, it is clear that safety system component selection and design for equipment assessed as a Category 4 risk will be dictated by the number of faults the system can tolerate without loss of the safety function. Hence the appropriate safety system components are application-specific, requiring a thorough understanding of the operation of the machinery and its control system.

Use of a safety controller rated at Category 4 does not, in itself, assure the overall *safety system* meets this level of performance requirements.

IV. Safety Standards, CE Marking and the European Machinery Directive

33

What is the “CE” mark and what does it mean?

The “CE” mark (for Conformance Europeene) is a symbol applied to finished products and machinery which meet applicable European Directives. For electrical and electronic “finished products,” these include the Low Voltage Directive and, where relevant, the Electromagnetic Compatibility (EMC) Directive.

The CE mark on a machine indicates that the machine as a whole conforms to the requirements of the European Machinery Directive (EMD). The EMD states that the machine must comply with the Essential Health & Safety requirements and the EMC.

34

Does the CE mark on a safety interlock switch, coded-magnet sensor, safety controller or other finished product intended for use in a safety circuit signify the product is safe?

No, the CE mark is not a safety mark. It simply serves to advise European customs officials that the product meets all applicable European Directives, allowing it to be placed

on the European Economic Market Area (The European Union and the countries of Iceland, Liechtenstein and Norway).

35

Are third-party approvals needed to apply the CE mark to safety components?

Third-party examination by an approved, independent testing agency or notified body is required for some safety components. Specific products include light curtains, safety mats, and two-hand controls. In addition some countries, such as Germany, require third-party certification for safety circuit controllers.

For most other safety components (such as interlock switches, coded-magnet sensors, limit switches, et al) self-certification by the manufacturer is acceptable. Despite this liberty, as policy SCHMERSAL has all of

their safety products certified by an independent third party (such as the BG).

Whether third-party or self-certified, all CE-marked components must be documented by a Declaration of Conformity. This document, signed by a highly positioned technical manager (e.g. Director of Engineering, et al), lists all standards and directives to which the product conforms. In addition, component manufacturers must maintain technical files documenting test results, etc.

36

Are machine guarding safety interlock switches and related safety control products subject to CE-marking?

SCHMERSAL considers all of their safety interlock switches, sensors and related control accessories as products requiring mandatory CE-marking. Consequently these products are designed to meet the EMC

and Low Voltage Directives as required. The CE-marking on SCHMERSAL's products affirms their compliance with these applicable Directives.

37

Since CE-marking of safety products is (for most items) a self-certification process, how can a user be assured "CE-marked" products truly meet relevant European Directives?

Users of CE-marked products have three vehicles of assurance at their disposal. These include an EC Declaration of Conformity, EC Type-Examination, and Type-Certification (Technical Report). Each of these is described below.

EC Declaration of Conformity

The Declaration of Conformity is mandatory for all products that are CE-marked. It is also mandatory for machine components which, if they fail, could lead to a dangerous or hazardous condition on the machine. These mandates are defined in the European Machinery Directive, and must be issued by the manufacturer for all products that are CE-marked.

This document, signed by a highly-positioned technical manager (e.g. Director of Product Development, Director of Research, Head of Engineering, et al), lists all the Standards and Directives to which the product conforms. It is a self-certification procedure normally undertaken by the manufacturer.

All SCHMERSAL safety products have a Declaration of Conformity document according to the European Machinery Directive mandates.

EC Type-Examination

This is a third-party examination conducted by an approved, independent testing agency/notified body (such as the BG in Germany), and is compulsory for selected safety equipment. Here the product is investigated to confirm that it conforms to all the Standards and Directives listed in the Declaration of Conformity.

The examination procedure, the definition of an approved independent testing agency/notified body, and the types of safety equipment for which this examination is mandatory is defined in the European Machinery Directive. (Specific products for which an EC Type-Examination is mandated include light curtains, safety mats, and two-hand controls. In addition the German authorities include safety circuit controllers as requiring such testing.)

This examination may only be conducted once, by one approved body, whose findings are then valid for the entire European Economic Community.

All SCHMERSAL safety controllers are so tested and certified. And each can be supplied with an "EC Type-Examination Certificate" issued by a recognized, approved body/notified body.

Type Certification (Technical Report)

This is similar to the EC Type-Examination, but is not compulsory. Here the product is investigated by an approved independent testing laboratory (usually by a notified body) to confirm that it conforms to all the Standards and Directives listed in the Declaration of Conformity. This examination may be carried out in as many countries and as often as required.

All SCHMERSAL safety products not covered by an EC Type-Examination certificate (such as our electro-mechanical safety interlock switches) have been so tested and certified. And each can be supplied with a "Type Certificate" issued by a recognized, notified body (e.g. BG, TÜV).

38

To what type machines does the European Machinery Directive apply?

The European Machinery Directive applies to all machinery that is powered and has moving parts. Excluded are manually-powered equipment, motor vehicles, medical

machinery and other special equipment ... some of which is regulated by other legislation under European Community Directives.

39

Who is responsible for certifying that an affected machine complies with the “essential health and safety requirements” embodied in the European Machinery Directive?

For most classes of machines, the affixing of the CE mark to demonstrate compliance with relevant European Directives is a self-certification process. For the most dangerous types of machines (Schedule 2, Annex IV of the European Union Machinery Directive, such as presses, sawing machines, manually-loaded injection/compression plastics molding machines and others listed in this Schedule), certification must be done by a recognized, independent, third party (known in Europe as a “notified body”). A list of notified bodies is available from

The Official Journal of the European Communities, U.S. Contact, UNIPUB; Lanham, MD.

While self-certification of many machines is legally acceptable, many machinery buyers prefer purchasing machines which have been evaluated and certified by independent, recognized third parties. This preference, in some cases, has been precipitated by sale of self-certified machines which were found to not meet relevant Directives.

40

What are “Consensus Standards,” and how do they relate to OSHA guidelines?

“Consensus Standards” are those industry standards developed by groups of professionals representing a cross-section of firms within that industry. Examples are standards prepared by ANSI (American National Standards Association), ISA (Instrument Society of America), ASME (American Society of Safety Engineers), SAE (Society of Automatic Engineers) and RIA (Robotics Industry Association). These standards provide safety guidelines for machinery designers and users.

OSHA specifically requires that guarding devices at the point-of-operation be in conformity with any appropriate standards (which include any OSHA or “industry consensus standards”). Hence OSHA may cite such consensus standards as a basis for their findings and enforcement.

V. Safety Controllers

41

What are “safety controllers” and what are their functions?

Safety controllers (such as SCHMERSAL’s SRB and AES Series) are connected between machine guarding interlock/E-Stop switches and the machine’s stop control elements (such as a motor contactor or control relay).

These controllers contain dual, self-checking safety system monitoring circuits and positive-guided output relays. Each is designed to monitor faults in the safety system’s interlock/E-Stop switches, the safety circuit interconnection wiring, and their own internal monitoring circuits and output relays.

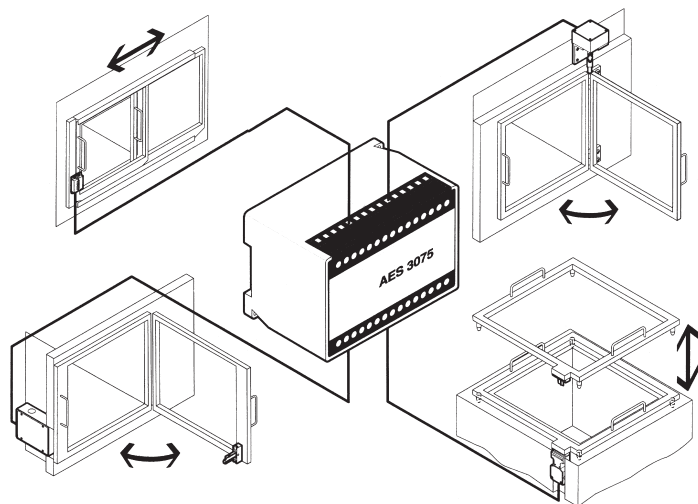
Detection of a fault in the machine’s safety circuit or of an open machine guard, disables the module’s output signal(s) facilitating machine stoppage, and/or prevents the restarting of the machine until the fault has been corrected.

In addition to detecting open guards and/or actuated E-Stop switches, safety controllers are capable of detecting the following types of safety system faults:

- Guard monitoring switch/sensor failure

- “Open-circuit” in interconnection wiring
- “Short-circuit” in interconnection wiring
- “Short-to-ground” in interconnection wiring
- Welded contact in controlled output device
- (such as positive-guided motor contactor)
- Failure of safety controller’s positive-guided relay(s)
- Fault in safety system monitoring circuit
- Insufficient operating voltage.

Some microprocessor-based safety controllers, such as SCHMERSAL’S AES Series, also feature integrated system diagnostics with visual LED outputs which indicates fault type and location — thus minimizing machine downtime.



Safety controllers detect and locate system faults. Units are available for use with guard interlock switches, non-contact safety sensors, safety edges, light curtains, E-stops and emergency cable-pull switches to satisfy a broad range of application requirements.

42

Why should safety controllers be used with safety interlocks/E-Stops?

Safety controllers increase the reliability of the machine guarding safety system. Their ability to detect safety cir-

cuit faults, and shut down the machine until the fault is corrected, greatly heighten the safety level.

43

What is the difference between a single and dual-channel safety controller, and when should each be used?

A single-channel safety controller is capable of accepting only one (normally-closed) input. When used in safety circuits they are unable to detect a short-circuit failure in the interconnection wiring, or a failure of the monitored input to change state.

A dual-channel safety controller is capable of accepting two inputs; one to each of its two, redundant self-monitoring safety circuits. When used in safety circuits they are typically capable of detecting interconnection wiring faults (such as short-circuits, open circuits, and ground faults) or a failure of one of the monitored input(s) to

change state. As such they provide a higher level of safety than single-channel units.

Single-channel safety controllers are suitable for relatively low levels of risk assessment (e.g. EN 954-1 Safety Categories B, 1 and 2). Dual-channel units are appropriate when designing “control reliable” safety systems — that is, systems in which a single component failure will not prevent normal machine stopping action from taking place, but will prevent a successive machine cycle from being initiated (e.g., EN 954-1 Safety Categories 3 and 4).

44

How do I decide which safety controller to use?

Safety controller selection is usually based on:

- (1) the type of inputs being monitored (e.g. E-Stops, interlock switches, light curtains, coded-magnet sensors, et al).
- (2) the number of inputs being monitored.
- (3) the number and type of outputs required from the safety controller (e.g. number of parallel outputs from the module’s positive-guided relays and the number of auxiliary/signaling outputs).

- (4) the need/desire to monitor the integrity of the positive-guided contacts in the controlled output device (e.g. motor contactor, control relay, et al).
- (5) the type of safety controller reset desired.
- (6) the level of safety desired (this is usually determined by a structured risk assessment).

These application parameters will normally narrow, and simplify, the choice of a safety controller to one or two units.

45

When is it necessary to design a safety system to satisfy the requirements of EN 954-1 Category 4?

Category 4 safety requirements are usually associated with extremely high-risk applications. Consequently the safety system needed to satisfy these conditions can be quite complex and costly.

Since general machine design practice respects classic safety hierarchy, most extremely high-risk hazards — that is:

- (a) those which the operator cannot avoid
- (b) those in which the operator is exposed frequently or continuously, and
- (c) those which could result in serious injury, amputation or death

are designed-out during machine development or are guarded against (if they cannot be designed-out).

Consequently for most applications it is generally not necessary to incur the cost/complexity of Category 4 safety system design. Many low-risk situations can be satisfied by safety systems that meet the requirements of Category B, 1 or 2 as defined by EN 954-1.

In most higher-risk situations, a suitable safety system (and one which meets ANSI's requirement for "control reliability") can be achieved with a system designed to meet the Category 3 requirements of EN 954-1.

When needed, Category 4 requirements can be satisfied by proper selection from SCHMERSAL's wide range of CE-compliant safety interlocks and related safety controllers.

VI. Applications and Solutions

46

What are some of the applications in which positive-break and tamper-resistant safety interlocks are used?

Positive-break and tamper-resistant safety interlocks are inherently safer alternatives to conventional industrial components such as:

- (Non-safety) electromechanical limit switches
- Inductive proximity switches
- Snap-acting position switches (without positive-break)
- Uncoded reed switches
- Hall-effect sensors
- Magnetic position switches
- Photoelectric sensors

Such conventional industrial sensors/switches are not recommended for safety applications.

For increased safety and reduced liability, only components which have been tested and certified for safety applications by an independent, recognized safety commission/agency are recommended.

Typical applications for these safety interlocks include:

- Metal cutting machine tools
- Metal forming machine tools
- Grinding machines
- Woodworking machinery
- Packaging equipment
- Printing presses
- Stamping/punch presses
- Textile machinery
- Material handling/conveyor lines
- Forging equipment
- Crushing machines
- Sawing systems
- Robot work-cell enclosures
- Emergency trip-wire systems
- Assembly equipment

The contents of this booklet represent a brief overview of selected current international and U.S. machine guarding safety standards and guidelines affecting machinery builders and users. The material presented is intended to inform the reader of some of the current and emerging safety issues which may need to be considered.

Due to the booklet's brevity, and to the diversity of applications which may be affected, we strongly encourage consulting with official regulatory bodies and relevant safety standards/guidelines.

Toward this goal a partial listing of selected references has been provided. We trust this brief tutorial was of value and that it encourages further investigation.

REFERENCES

The following are some of the current and emerging safety standards and guidelines which may affect your equipment design and its use.

- Occupational Health & Safety Administration, Code of Federal Regulations, Part 1910 (OSHA 29 CFR 1910).
- ANSI Technical Report B11.TR3:2000, Risk Assessment and Risk Reduction — A guide to estimate, evaluate and reduce risks associated with machine tools.
- ANSI Standard B11.19-2003, Safeguarding Reference for B11 Machine Tool Safety Standards
- ANSI Standard B11.20-2004, Safety Requirements for Construction, Care, and Use of Machine Tools — Manufacturing Systems/Cells.
- ANSI-RIA 15.06-1999, Safety Requirements for Industrial Robots & Robot Systems.
- ISA S84.01: Safety Instrumented Systems
- EN292, Parts 1 & 2 — Safety of Machinery, Basic Concepts, General Principles of Design
- IEC 204, Part 1, Electrical Equipment of Industrial Machines (1992)
- European Machinery Directive (EMD) 89/392/EEC Essential Health & Safety Requirements Related to the Design & Construction of Machinery
- EN 954, Part 1, Safety of Machinery — Principles for the Design of Safety Related Control Systems
- EN 1088: Safety of Machinery-Interlocking Devices With and Without Guard Locking.

FREE SAFETY VIDEOS

For information about ordering any of these videos, please call your local SCHMERSAL Sales Representative or stocking distributor. For their name and telephone number, click onto our web site: www.schmersalusa.com, or contact SCHMERSAL at our headquarters:

660 White Plains Road
Suite 160
Tarrytown, NY 10591
Tel: 914-347-4775
Fax: 914-347-1567



Video I. Man-Machine Safeguarding: Principles & Practices

What are current OSHA regulations and ANSI standards for machine safety? How do they affect you? How can they be satisfied? These and other questions are answered in this comprehensive 15-minute tutorial video. Covers vital topics such as types of machine hazards, types of movable machine guards, risk assessment, redundancy, positive-break contacts, tamper-resistance, positive-guided relays, safety controllers, fault detection and control reliability.

Video II. Man-Machine Safeguarding: Problems & Solutions

What type of approved safety components are available to satisfy ANSI, OSHA and CE requirements? How do they work? For what type applications is each best suited? These and other questions are answered in this comprehensive 15-minute tutorial video. Presents and explains a wide variety of machine guarding safety components including keyed interlock switches (with and without solenoid-latching), hinged safety interlock switches, emergency cable-pull switches, coded-magnet sensors, safety edges, safety limit switches and safety controllers.

Video III. Safety Controllers: Applications & Selection

What are safety controllers? What is their function? Where/when are they used? These and other questions are answered in this focused 19-minute tutorial video. In addition it presents an easy-to-use, application-based selection methodology to aid in the choosing of an optimum safety controller to meet specific application conditions, safety control categories, and control reliability requirements.