August 1999

Triodyne Inc.

A SAFETY JOURNAL HIGHLIGHTING CRITICAL SAFETY DEVELOPMENTS

SAFETY ALERT

ISSN 1097-7589

Vol. 1 No. 4

A New Interlock System

Movable Interlocked Barrier Guards With Motorized Openers for Testing

by Ralph L. Barnett * and Dr. Theodore Liber **

Abstract

A unique system is introduced for monitoring the viability of conventional position switch interlocks on movable barrier guards. At closely spaced intervals a test device motor causes the guard to open slightly to check if the interlock will change state in an attempt to interrupt control power to the protected machine. The machine will not in fact shut down during the testing phase because the interlock system will be isolated from the machine operating motor contactors during the test duration. Testing of a guard is annunciated just before and during the automatic testing phase. Any failures of an interlock or its testing system will also be annunciated until their causes are corrected. When a latching system is used in conjunction with the guard, a faulty interlock will cause the guard to be locked closed until it is convenient to effect a repair. Production is not interrupted because the interlock remains bypassed during this period. If an interlock is temporarily circumvented or if the interlock guard is sabotaged, the test device motor will not cause a change in state of the interlock during the test phase; again, system malfunction will be annunciated and/or the guard will remain latched and/or the machine will be shut down.

The proposed process provides the following advantages:

- A quantum leap in system reliability and safety is obtained using even the most ordinary "limit switch" type interlocks.
- The tamper-resistance of all known interlocks will be greatly enhanced; all popular forms of temporary interlock circumvention are eliminated.
- Long term sabotage which involves simultaneous guard removal and interlock bypassing is addressed for the first time; to defeat the proposed process involves the most outrageous restructuring of the control system.
- The system will safely endure adhesive environments that may cause interlock activators to stick in their "fail to danger" states.
- The monitored machine is almost never shut down nor production interrupted during or after the testing phase, even if mischief is uncovered.
- The testing of large numbers of interlocks will not expose the machines' electric power motors to the frequent restart demand associated with some conventional manual testing procedures.
- Without compromising safety, maintenance of even multiple interlock failures may be deferred until their repair is convenient.
- The assurance of working interlocks may enable OSHA to expand applications where maintenance is performed under "control stop" as opposed to the more elaborate "lock out."
- The design of the new test and monitoring system may be executed and implemented using straightforward hardware and software that are firmly entrenched technology.

I. Introduction:

An interlock may be used to indicate whether a barrier guard is open or closed or whether a mechanism is running or stationary. Interlocks are go/no go devices which monitor physical

* Professor, Mechanical and Aerospace Engineering, Illinois Institute of Technology, Chicago, and Chairman, Triodyne Inc., Niles, IL.

** Senior Science Advisor, Triodyne Safety Systems, L.L.C., Niles, IL.

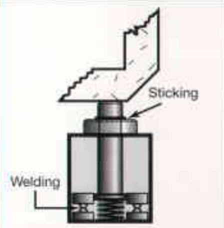
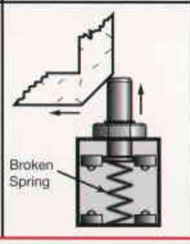
MACHINE GUARD CLOSED/SWITCH CLOSED	MACHINE GUARD OPEN/SWITCH OPEN	DESCRIPTION
		• Normally Open, Held Closed Contacts • Negative Mode Switch • Conventional Interlock • Single Channel Interlock • Movable Machine Guard Activating a Conventional Limit Switch with Spring-Disconnect Contacts

Figure 1 – Conventional Electrically Interlocked Barrier

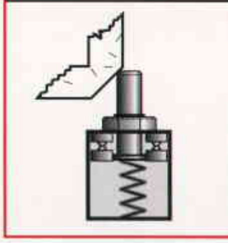
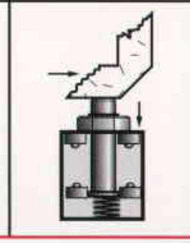
MACHINE GUARD CLOSED/SWITCH CLOSED	MACHINE GUARD OPEN/SWITCH OPEN	DESCRIPTION
		• Normally Closed, Held Open Contacts • Positive Mode Switch • Forced Disconnection • Single Channel Interlock • Movable Machine Guard Activating a Safety Interlock Switch with Positive-Opening or Positve-Break Contacts

Figure 2 – Positive Opening Safety Contacts

systems that exhibit simple dual conditions. They may operate electrically, mechanically, pneumatically, magnetically or with any combination of physical phenomena.

This paper is concerned with movable point of operation guards that are equipped with a single electrical interlock. The guards are typically hinged or sliding; they may be removable without tools such as hook-on or detented panels, or they may rotate into position like a pressure cooker lid. The interlocks are incorporated into the same control circuits as emergency stop devices where they may also instantly interrupt powered operation of the guarded machine.

A succinct statement of the design criteria for interlocked guards may be found in the 1993 European Standard entitled "Safety of machinery interlocking devices with and without guard locking - General principles and provisions for design"(Ref. 1):

3.2 interlocking guard (without guard locking) [3.22.4 of EN 292-1:1991]

Guards associated with an interlocking device, so that:

- the hazardous machine functions "covered" by the guard cannot operate until the guard is closed,
- if the guard is opened while the hazardous machine functions are operating, a stop instruction is given,
- when the guard is closed, the hazardous machine functions "covered" by the guard can operate, but the closure of the guard does not by itself initiate their operation.

3.3 interlocking guard with guard locking [3.22.5 of EN 292-1]

Guard associated with an interlocking device and a guard locking device so that:

- the hazardous machine functions "covered" by the guard cannot operate until the guard is closed and locked,
- the guard remains closed and locked until the risk of injury from the hazardous machine functions has passed,
- when the guard is closed and locked, the hazardous machine functions "covered" by the guard can operate, but the closure and locking of the guard do not by themselves initiate their operation.

3.4 control guard [3.22.6 of EN 292-1]

Guard associated with an interlocking device (with or without guard locking) so that:

- the hazardous machine functions "covered" by the guard cannot operate until the guard is closed,
- closing the guard initiates the hazardous machine function(s).

The so called "interlocking guard (without guard locking)" is the focus of this paper. Opening such a guard interrupts the power to a machine and eliminates the hazard before access to it is possible. The door guard on a microwave oven meets this condition. The condition is also met by mechanical systems where the separation distance between the hazard and the guard door is such that it takes longer for the operator to reach the hazard than it does for the hazard to disappear. Suitable braking devices may be used to rapidly terminate mechanical hazards.

II. Interlock Reliability

The conventional interlock or position switch is far and away the most often used concept for interlocking guards in the U.S. The construction of the doorbell switch provides an example of a conventional interlock; its concept is embodied in Figure 1. Interlock guards are primarily used to control risk-taking [Ref. 2]. Their presence fundamentally changes the man-machine interaction [Ref. 3] in the sense that a foreseeable number of people will misuse them as control devices in the same manner that the safety edges on elevator doors are purposely blocked to prevent door closure. Because a certain percentage of operators will transfer their personal vigilance to dependence on interlocks, safety demands that such devices be reliable.[1]

For commercial usage, the reliability of conventional position switch interlocks may be judged from a study involving the upper limit switches on hoists and cranes ranging in capacity from one-quarter to two tons. The study was first described in 1964 by the National Safety Council in the Fifth Edition of their Accident Prevention Manual for Industrial Operations [Ref. 4]: "During a 20-year period, one division of an automobile manufacturing company made 72,000 formal hoist inspections involving over 600

[1] Reliability: The probability that an item will preform a required function under stated conditions for a stated period of time.

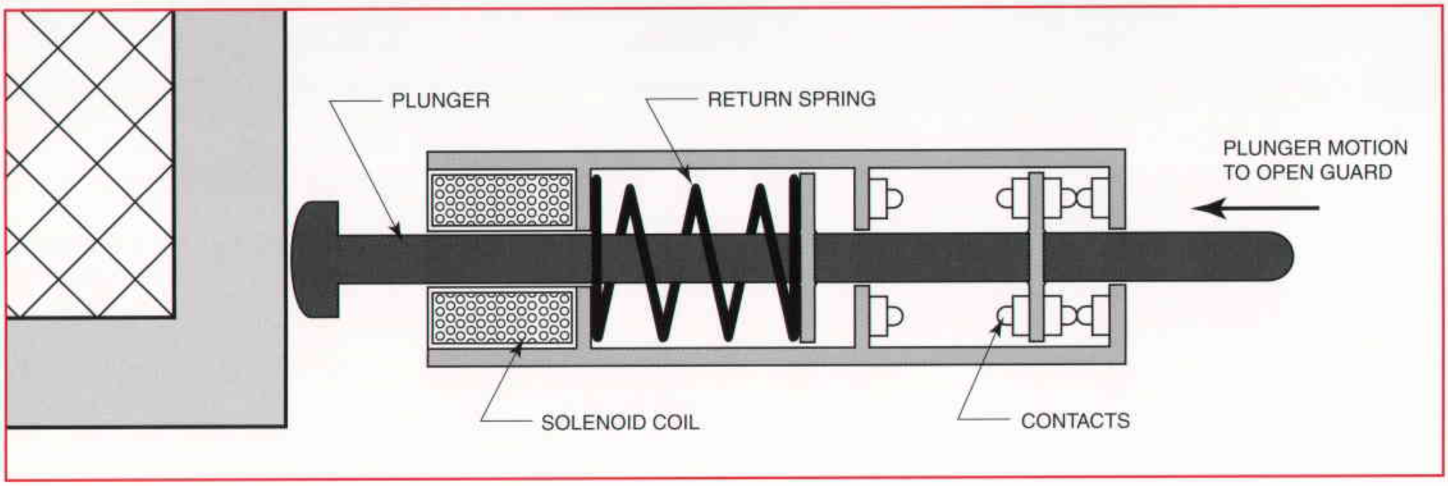


Figure 3 – Solenoid Activated Guard Opener (Shown at Rest with Guard Closed)

electric hoists and cranes. The inspections disclosed approximately 3,000 unsafe cables, 1,000 faulty brakes, and 1,000 defective limit switches." It can be seen by this study that the reliability of conventional limit switch interlocks is unacceptably low for safety applications. In a consumer setting, the National Highway Transportation Safety Administration (NHTSA) stated that vehicles built between August 1973 and 1975 must have either passive restraints or lap-shoulder belts in conjunction with a starter interlock. Such a system prevents the vehicle's engine from starting whenever the front-seat occupants' manual seatbelts are unfastened. Many consumers complained that the interlock system failed to operate effectively, i.e., it was not reliable. Thus, on October 27, 1974, President Ford signed a bill that prohibited starter interlocks. Four days later, NHTSA deleted the starter interlock regulation from the Federal Motor Vehicle Safety Standard 208.

To deal with the low reliability of conventional interlocks in safety applications in this country, most machinery manufacturers require that the interlocks be tested at the beginning of every shift. Either of the following two methods is used for manual testing:

Method 1. If a machine operates with all of the interlocked guards closed, one may stop the machine, successively prop open each guard, and attempt to start the machine. Clearly, if the machine remains benign all of the interlocks function in this static mode. This is a relatively fast procedure when two people conduct the tests; one at the control and one successively opening the barriers. Strict coordination must be maintained between the two testers or guards may be opened and closed so rapidly that they don't get tested, or a properly operating interlocked guard may accidently be closed during attempted start up which would result in the machine being turned on and a defective interlock falsely proclaimed.

Method 2. A guard opened on a running machine will shut down the motor if the interlock is functional. Restarting the machine and repeating the procedure for each interlocked barrier completes the test protocol. This testing method is more failure provoking than the static test because contacts are more difficult to break electrically when they are carrying current. Furthermore, if the contacts are vibrating they can continuously make and break the circuit and pass enough current through the interlock to sustain the motion of the motor. Interrupting power on a running machine is a more vigorous testing protocol than establishing the inability to start the machine.

Both testing methods are time consuming and both expose the testers to an unguarded running machine when faulty interlocks are encountered. The second method is not prone to sequencing errors; however, the frequent motor restarting when testing large numbers of guards will compromise large horsepower electric motors.

Experience has shown that testing of interlocks is rarely undertaken. When it is, and the testing reveals an interlock that will not shut off the machinery, (fail to danger), the requirement to immediately shut down the machine and fix or replace the interlock is commonly violated. Unfortunately, the fault is not annunciated or displayed.

A new approach to enhancing the reliability of single mechanical interlocks was officially introduced into the European Community in 1988. The effects of reasonably foreseeable failure modes were either eliminated or minimized. For example, Figure 1 indicates three recurring failure scenarios that involve contact welding, actuator sticking, and broken springs. These conditions are particularly vexing and lead to "fail to danger" modes where contacts remain closed and the protected machines continue to run after their guards are opened. To overcome these faults, the European Community replaced the spring disconnect mechanism with a force disconnect mechanism as shown in Figure 2. This positive mode operation will

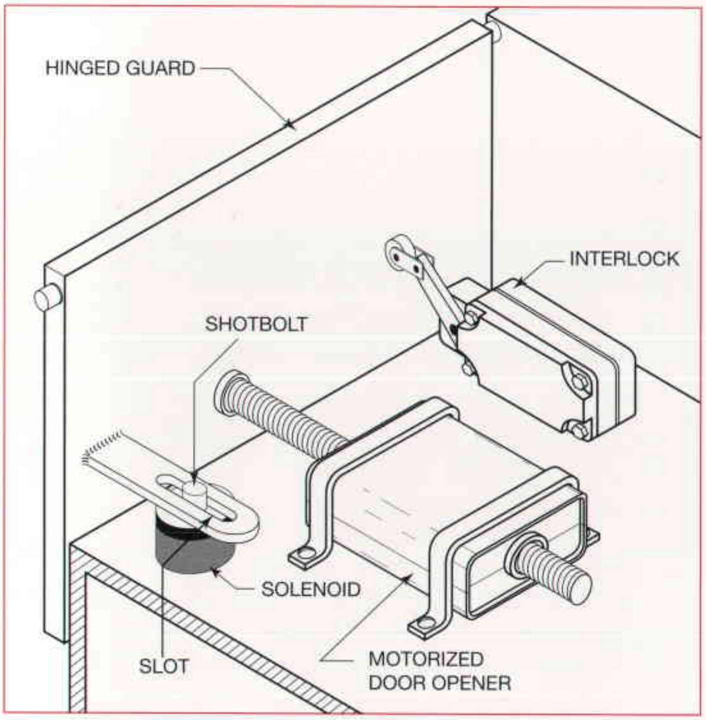


Figure 4 – Solenoid Actuated Shotbolt, Motorized Door Opener and Interlock

either break the contacts when the guard is opened or will interfere with the opening of the guard itself.

In addition to safety interlocks, the composition of a safety interlock system may include transformers, relays, circuit monitors, control modules, interconnected wiring, motor contactors, zero speed switches, timers, door locks, solenoids, fuses, reset buttons and programmable logic controllers. Europeans use five levels of safety interlocking to satisfy requirements arising from risk assessments of candidate machines. The relative risk levels take account of injury severity, frequency of exposure to hazards, probability of avoiding the hazards, and likelihood of occurrence if a safety control system fails. Reliability hardening and complexity of the interlock systems naturally increase with the danger level. For example, reliability may be enhanced with large safety factors, quality control, diversity, redundancy, proven technology, and preventive maintenance. [Ref. 5]. As the danger level increases there is a concomitant increase in testing, self-checking, and monitoring requirements.

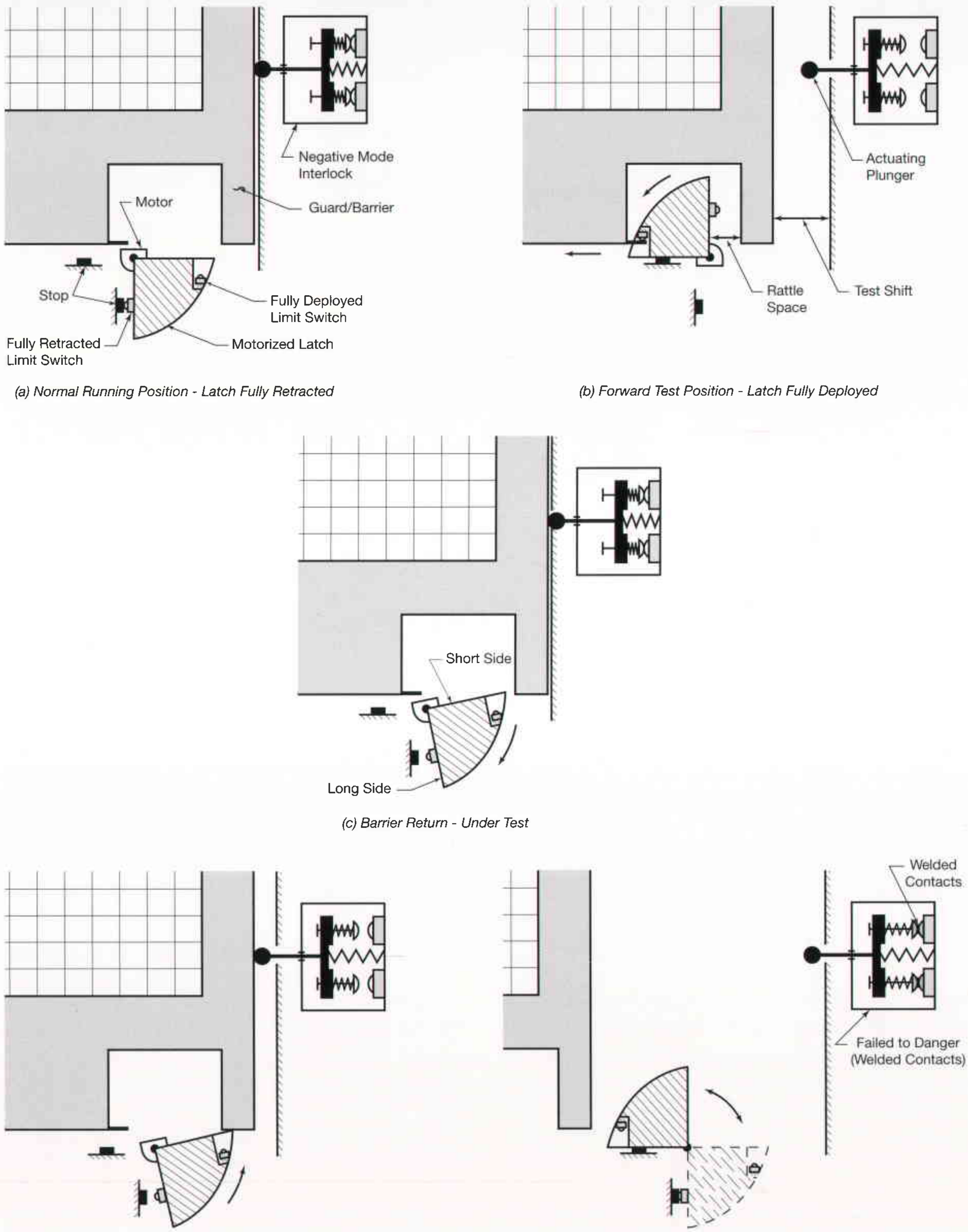
Almost every component of a high reliability interlock system is checked and monitored. Some are checked continuously; others are scrutinized at regular intervals or during operation. It is extremely important to point out that an interlock cannot be completely checked without opening its corresponding guard. The interlock has two states and each must be examined independently; one when the guard is closed and the other when the guard is open. Advanced systems take advantage of every functional guard opening to check the guard's interlock and the associated system. "Check the interlocks daily or at the start of each shift" continues to be the most popular interlock admonition. Enforcement of this testing ritual is always challenging because of the time and effort required for machinery with multiple guards. For high reliability applications, the British have designed circuits that enforce the opening and closing of the guard and hence the guard switches to provide a pre-start check after switch-on of the power supply, [Ref 6]. Whenever a faulty interlock is encountered its replacement is expected before operations are resumed. The advanced interlock systems enforce this replacement by disabling the machinery.

In 1999, Barnett and Liber were granted a patent that introduced processes which provide the next generation of interlocking technology. The heart of the new system consists of a motor or a powered shifter that will open a guard just enough to activate its interlock. Opening and closing an interlock automatically at regular time intervals allows the interlock to be checked by monitoring whether it changes its state. By selecting short time intervals between tests, for example five minutes, the interlocking reliability of even inexpensive interlock devices can be made to approach 100%. At worst, an operator cannot be exposed to a faulty interlock for more than the selected testing interval. Figure 3 illustrates a solenoid activated plunger that may be used to open a sliding guard. Contacts are shown that will indicate the extreme forward and rearward positions of the plunger.

Testing of a guard is annunciated just before and during the automatic testing phase. During this test the interlock function is bypassed so that the machine will not shut down. Production is not interrupted during the testing and the machinery motors are not repeatedly turned on and off. In the more elementary versions of the concept, operator protection during the testing phase is furnished by the annunciating and/or display system which admonishes against entering a guarded space during testing. This active protection may be replaced by a passive latching device which locks the guard in protective position during testing. An old-fashioned solenoid operated shotbolt may be deployed during the testing phase; such a device is illustrated in Figure 4. A slot in the latch plate may be observed that allows the guard to be moved for testing without unlatching the shotbolt. The slot allows the hinged guard to be moved manually or through the use of the motorized door opener.

The presence of a latch enables one to maintain the guard in a locked position when a faulty interlock is detected. Consequently, continuous passive safeguarding is provided. Indeed, the interlock need not be repaired when its "fail to danger" propensity is identified. Maintenance may be delayed until convenient; production continues undisturbed.

open to continue →→



(a) Normal Running Position - Latch Fully Retracted

(b) Forward Test Position - Latch Fully Deployed

(c) Barrier Return - Under Test

(d) Guard Ajar - Under Test

(e) Barrier Open or Removed - Under Test

Figure 5 – Combination Motorized Door Opener and Latch System

It is straightforward to design the motor/shifter devices so that they will lock the guards during both the testing phase and during those periods where faulty interlocks are present. Figure 5 shows a schematic representation of a combination motorized door opener and latch system. In the first illustration, Figure 5a, a conventional interlocked barrier is shown with a rotary latch in the fully retracted position. If the machine and interlock are functional, the machine may be operated with the hazard space fully protected. Opening the barrier will immediately interrupt

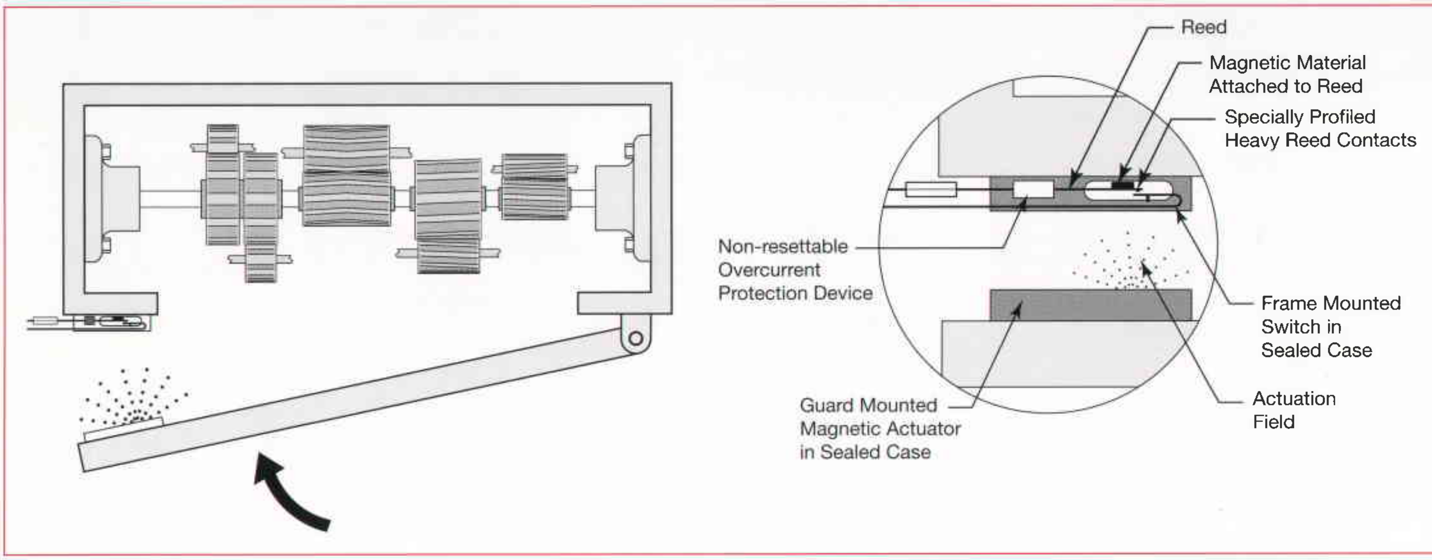


Figure 6 – Magnetic Reed Switch

powered operation; permission to restart is granted upon reclosing. The machine will not restart until a start command is given. If the interlock "fails to danger" or if it is circumvented, the machine will operate when the door is opened. The position of the latch is communicated to the machine's control unit by the "fully retracted" latch limit switch. As shown in Figure 5c, one side of the latch is long and the other short.

To test the interlock, the motorized latch is rotated 180° counterclockwise as shown in Figure 5b. This action shifts the guard to the left away from the interlock's actuating plunger. During this test phase the barrier is locked against opening; there is a rattle space. The test shift plus the rattle space provide a gap at the right side of the guard. The gap must not allow entry of a hand; otherwise, a fixed barrier strip must be mounted to the frame to enclose the gap. The fully deployed status of the latch is communicated to the machine's control unit by the "fully deployed" limit switch. During this test phase, an operating interlock will change state; if not, its faulty "fail to danger" status will be annunciated and/or displayed. Further, the latch will remain fully deployed to keep the barrier locked in its protective position. During this test phase the interlock's circuitry is bypassed to maintain the operating condition of the machinery. Because the guard is locked closed, the machine may continue to run safely in this state until it is convenient to repair the interlock. If the motorized latch is operating correctly, the command to deploy the latch will result in breaking the "fully retracted" contact and in making the "fully deployed" contact. Failure of either or both actions casts doubt upon the efficacy of the automatic test system. Under these circumstances the machine may be programmed to shut down and continuously annunciate and display the status of the test system. To avoid shutting the machine down, the control unit may be programmed to bypass the automatic test system and to introduce a manual test protocol with suitable instructions and warnings. The manual test program may be reinforced by shutting down the machinery when the test intervals are too long.

If the interlock passes the first test phase where the latch is fully deployed, the latch is then rotated clockwise into its fully retracted position. As illustrated in Figure 5c, this action causes the barrier to move to the right into its fully closed position. The second test phase begins as the barrier pushes against the actuating plunger. This gives the interlock an opportunity to change state from open (off) to closed (on). Failure to change state implies that the interlock failed to danger during or after the first test phase. This status is annunciated and displayed and the latch is rotated counterclockwise into its locking position where it resides until repairs are made. The viability of the test system is reestablished by insisting that the second test phase cause the breaking of the "fully deployed" contact and the making of the "fully retracted" contact.

Every motor/latch design may manifest special failure modes that must be accommodated. Because the systems generate a large amount of feedback data it is usually simple to safeguard the failure modes, e.g., motors may be switched to forward/off/reverse, latches may or may not be fully retracted or fully deployed, and interlocks are go or no/go. This information may be used to warn and instruct, shut down the machine, lock the barrier closed, or switch to manual testing protocols.

Returning to the motor/latch design characterized in Figure 5, a special condition arises when the barrier is left ajar. This condition is depicted in Figure 5d where the guard is found to interfere with the full deployment of the latch during phase one testing. The motor forward command followed by breaking of the "fully retracted" contact indicates that the test motor is working. Because the "fully deployed" contact is not made, one cannot depend on the barrier shifting or on the latch moving into its locking

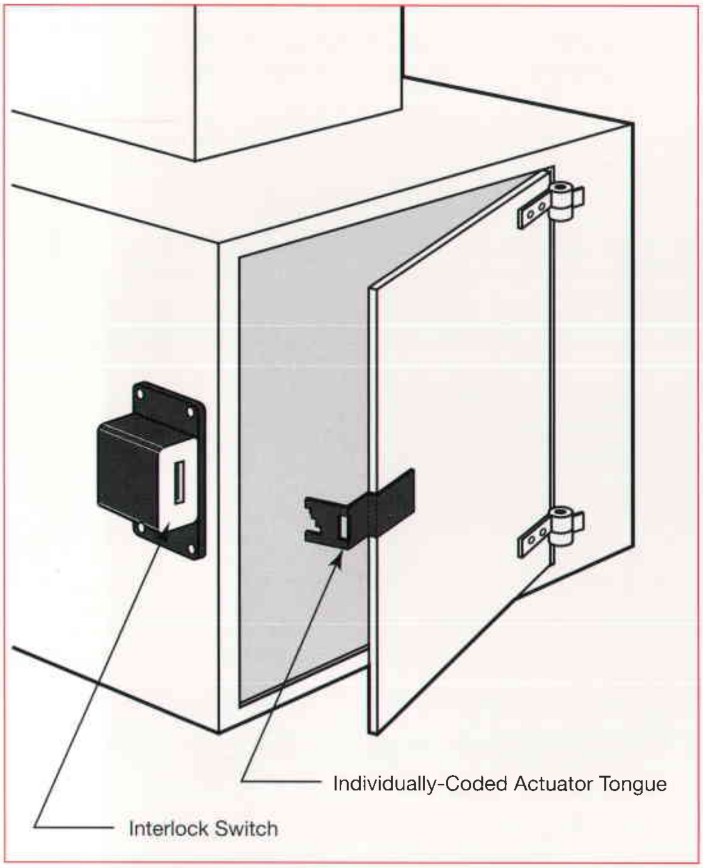


Figure 7 – Coded Mechanical Tamper-Resistant Interlock

mode. Note that a faulty "fully deployed" contact provides the same information under normal working conditions. So does a failure of the test motor in between its two extreme positions. Uncertainty in the test system may be handled by shutting down the machine. As previously described, the automatic testing system may be bypassed and manual testing can be required every eight hours to maintain the running status of the machine. Annunciators and displays may be used to communicate the questionable performance of the test system. Under these conditions one cannot depend on the automatic locking of the barrier in its protective position.

With a properly functioning interlock, an open barrier shuts the machine down together with the automatic test system. However, a "fail to danger" fault will allow a barrier to remain open while the machine is running and the test system is functioning. This situation is depicted in Figure 5e where the latch is rotated into its forward or deployed position during its first test phase. The test will detect the "fail to danger" fault of the interlock. Furthermore, because the barrier has been opened or removed, the "fully deployed" limit switch contacts are not closed. This means that the barrier cannot be locked automatically even though the latch will remain fully deployed against its physical stop. The previously described countermeasures may all be used; machine shut down, continuous annunciation and display, and manual testing. In addition,

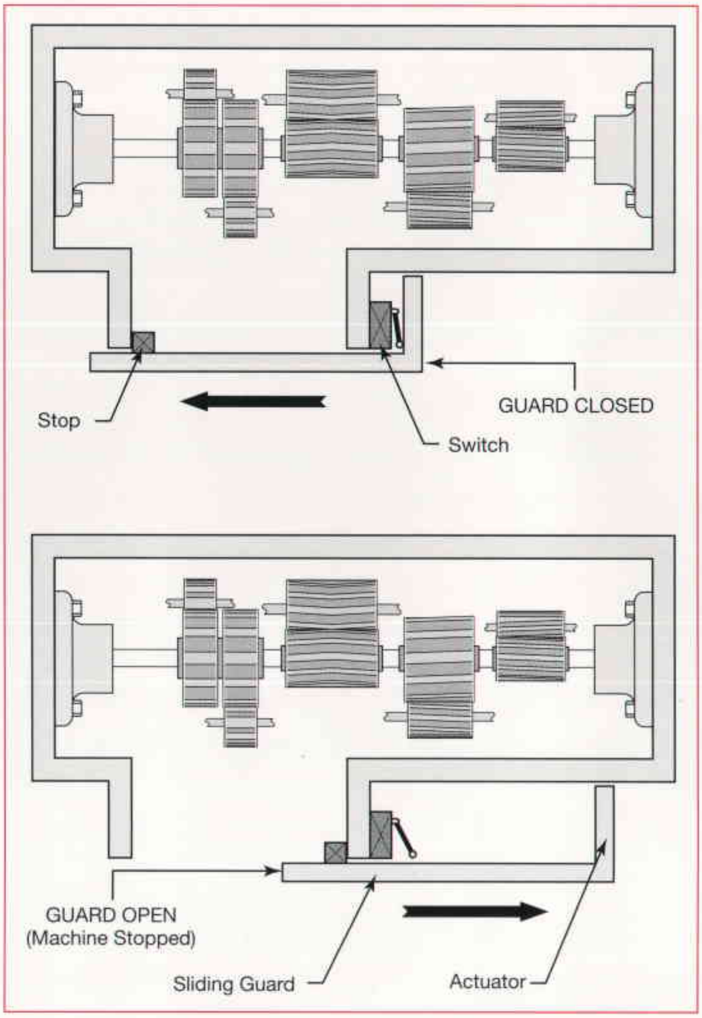


Figure 8 – Guard Covering Switch

the barrier may be manually shifted to its protective position where it can be locked by the latch and remain locked until the interlock is repaired.

III. Tamper Resistance

The circumvention of interlocks takes two forms; temporary bypassing and long term sabotage. Such acts arise when dynamic troubleshooting requires that machines be operated with open guards. Sometimes bypassed interlocks are not restored after a maintenance routine and occasionally interlocked guards are completely removed in an attempt to increase production, improve visibility or create a less stressful working profile. To maintain production, it is not uncommon to override faulty interlocks that create nuisance shutdowns or prevent machine operation.

The safety integrity of interlocks depends in part on their tamper resistance. This subjective property has not been quantified nor standardized by the safety community. That is not to say that it hasn't been addressed. For example, the American National Standard Institute's standard ANSI B11.19-1990, Reference Standard for Safeguarding

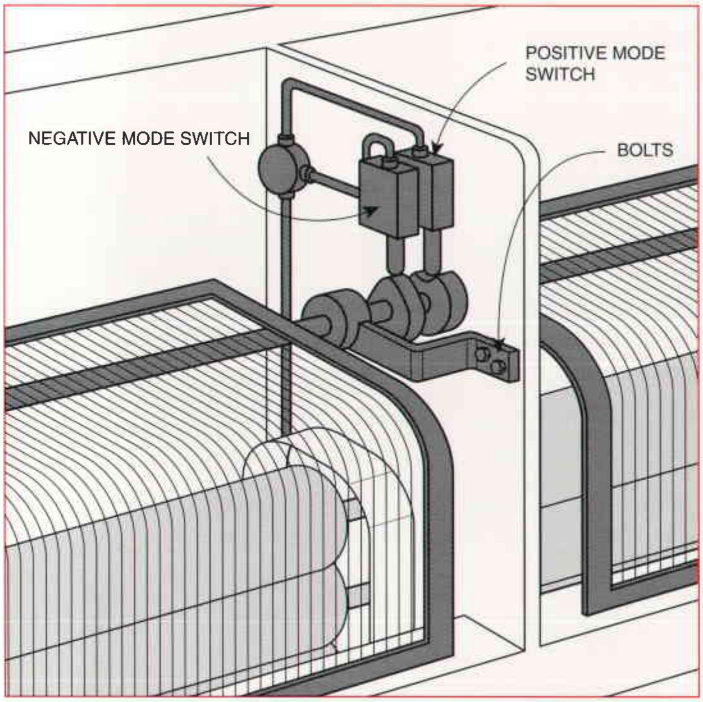


Figure 9 –Two Opposite Mode Position Switches

Machine Tools specifically requires:

- Barrier guards which protect against unauthorized adjustment or circumvention,
- Interlock devices which are not easily bypassed.

The security of interlocking systems is likewise addressed by the British Standard Code of practice for Safety machinery, BS5304:1988, paragraph 9.5.3. Virtually all manufacturers of sophisticated interlocks deal with the problem of tamper resistance.

To circumvent conventional position switch interlocks the activator arms or stems may be tied, taped or wedged into the closed (running) position. This can generally be accomplished in a matter of seconds. Systems embracing multiple interlocks can be bypassed by jumping over the interlock contacts in the circuit wiring; industrial electricians can accomplish this in a matter of minutes. There is a family of non-contact (non-mechanical) actuation devices that have become popular interlocks. They operate via magnetic or electronic fields as exemplified by the magnetic reed switch in Figure 6. An actuation magnet is attached to the guard and the switch body is mounted on the machine frame. A closed guard brings the field into close proximity with the reed supported magnetic material which deflects the reed and causes contacts to close within the sealed case. These interlocks may be defeated by opening their associated guards and placing an ordinary magnet on the reed switch.

The European Community approaches the problem of tamper resistant interlocks by minimizing the motivation for bypassing them and by making defeat more difficult. The level of required hardening and the need for human intervention are revealed during required risk assessment studies. The use of coded actuators increases the difficulty of bypassing the interlocks. The coding may be incorporated magnetically, electrically, mechanically, or optically. For example, the magnetic field used in the reed switch illustrated in Figure 6 can be uniquely configured so that the reed will not respond to arbitrary magnets. The mechanical actuator tongue in Figure 7 has been individually coded and matched to the switch mechanism. The common method for defeating coded interlocks is to remove the coded actuator from the guard and join it to the interlock switch mounted on the frame.

The Europeans also control tampering by “hiding” the interlocks. They do this by physically obstructing or shielding the interlocking devices while the guards are open as illustrated in Figure 8. The determined risk taker can always jumper the interlocks out of the control circuit. Removing the mounting screws on positive mode interlocks is the method used at most machinery trade shows for bypassing interlocked guards so that the mechanisms can be viewed.

Tamper resistance is an intrinsic characteristic of the Barnett/Liber interlock system. Whenever a motorized guard is opened, the associated interlocks are expected to change states. If a change does not occur because actuators are tied down or the interlocks are jumpered out of the circuits, the system annunciates a malfunction and/or the guard is latched until the system is restored to its normal configuration. If desired, the logic can be set to shut down the machine. It should be noted that the motorized guard opener enables one to achieve extremely high levels of tamper resistance even when using the least expensive and most easily defeated interlock devices.

IV Comments

Most interlocks, and especially those considered in this paper, are integrated into the control systems of the protected machinery. Because of this ANSI standard B11.19-1990, 5.5 requires that they exhibit “control reliably”; to wit, “...the device, system or interface shall be designed, constructed and installed such that a single component failure within the device, interface or system shall not prevent normal stopping action from taking place but shall prevent a successive machine cycle...” Clearly the conventional interlock fails this requirement decisively, e.g., a broken spring, welded contacts or a sticking actuator will each cause the interlock to fail to danger.

The concept of motorized door openers is based on the notion that “the proof of the pudding is in the eating.” The door opener replicates the action of an operator trying to gain access to the guarded space. In the case of a light curtain, the equivalent testing involves breaching a light screen with a probe. If the safeguards do not protect under test conditions, they clearly will not protect during production.

Various testing protocols are available for machines with multiple guards. For example, all guards may be tested simultaneously or sequentially. The optimum testing intervals may be different for various guards; longer intervals produce less wear on the interlock system components.

Conventional redundant protection of guards using multiple positive mode or negative mode interlocks or a combination of these devices such as shown in Figure 9, cannot be manually tested. If a machine shuts down when a guard is opened it is possible that only one interlock is operable and the rest are faulty. The Barnett/Liber system can operate using a single motorized door opener and a single latch. Each interlock is individually monitored when the door is forced open. A faulty interlock results in annunciation and/or guard latching until the fault is corrected.

The reliability of the interlocked guard illustrated in Figure 9 is enhanced by redundancy; loss of protection only occurs in the unlikely event of simultaneous failure of the interlock devices. Reliability is also improved by diversity; i.e. the use of position switches that operate in opposite modes. Notice that if the bolts loosen and drop the cams relative to the switches, the positive mode interlock will never shut off the machine. The negative mode switch will provide the required protection.

Latches are currently available that remain locked without solenoid activation. A push lock release button energizes the solenoid only when guard opening is required. This prevents guards from swinging open whenever a control stop button is pressed. It also means that the latch solenoid is not left energized for long periods which can cause efficiency loss. The latching capability may be used to purposely bypass an errant interlock while maintaining safety by locking the guard in place. For security reasons it may be desirable to keep the guard locked. When a power failure occurs, the latching logic may be designed to hold all the guards in a locked position.

From a reliability point of view it is very significant that there are many mature manufacturers of interlock systems with hardware ranging from the simple to the sophisticated. [Ref. 7, 8, 9, 10, 11, 12] The motorized guard opener concept provides enhanced reliability for all available systems. This implies that less elaborate devices may be substituted for sophisticated hardware without compromising safety.

Generally, OSHA will not allow interlocks to be substituted for lockout/tagout as a maintenance protocol. [Ref. 13] On the other hand, for routine adjustments or routine cleaning, control shut off is sometimes accepted. The high level of reliability associated with the moving guard opener concept may extend the range of scenarios where lockout procedures can be abandoned.

Control interlocking is the most commonly used method of interlocking and may be used with or without guard locking (as distinguished from our latching). The interlock contacts are incorporated in a safety related control system (SRCS) which is the subject of European Standard prEN 954-1, "Safety related parts of control systems." This standard describes five categories for benchmarking and describing the performance of SRCS's. The highest category, Category 4, is generally used in the most critical safety situations. Its requirements may be summarized as follows:

- Use of well tried safety principles.
- Safety related parts of machine control systems and/or their protective equipment, as well as their components, shall be designed, constructed, selected, assembled and combined in accordance with relevant standards so that they can withstand the expected influence.
- The system shall be designed so that a single fault in any of its parts does not lead to the loss of safety function.
- The single fault is detected at or before the next demand on the safety function. If this detection is not possible then an accumulation of faults shall not lead to a loss of safety function.

  Note 1: Multiple faults caused by a common cause or as inevitable consequences of the first fault shall be counted as a single fault.

  Note 2: The fault review may be limited to two faults in combination if it can be justified; but, complex circuits (e.g. microprocessor circuits) may require more faults in combination to be considered.

Commenting on Category 4 requirements, one of the leading manufacturers of interlocks, Scientific Technologies Inc. [Ref. 14], has stated,

> "Category 4 requires that the safety system function is still provided even with an accumulation of undetected faults. The most practicable way of achieving this is to employ continuous or high frequency monitoring techniques. This is not feasible with most mechanical or electro-mechanical components (e.g. mechanical switches, relays, contactors) such as are used in interlocking and emergency stop systems."

The proposed system for automatic motorized testing of interlocked guards may be programmed to monitor interlocks with sufficient frequency to achieve Category 4 status.

A detailed treatment of the notions introduced in this paper may be found in the United States Patent No. 5, 870,317 by Ralph L. Barnett and Theodore Liber.

References

1. "Safety of machinery - Interlocking devices with and without guard locking - General principles and provisions for design," EN 1088 draft European Standard. Brussels, European Committee for Standardization, May 1993.

2. Barnett, Ralph L., "Interlocked Barrier Guards: Risk-Taking Philosophy," Triodyne Safety Bulletin, v. 7 #4 (September 1998).

3. Barnett, Ralph L., Gene D. Litwin and Peter Barroso Jr., "The Dependency Hypothesis (Part I)," Triodyne Safety Brief, v. 2 #3 (November 1983).

4. Accident Prevention Manual for Industrial Operations, 5th Edition. Chicago, National Safety Council, 1964, p. 18-1.

5. Barnett, Ralph L., "The Doctrine of Manifest Danger and Its Relationship to Reliability, Preventive Maintenance and Fail-Safe Design," Triodyne Safety Brief, v. 8 #1 (September 1992).

6. "British Standard Code of Practice for Safety of Machinery," BS 5304:1988. British Standards Institution, 1988. p. 11-12.

7. Engineering Guide to Machine & Process Safeguarding. STI part number 99276-0010. Fremont, CA, Scientific Technologies Inc., 1998-99.

8. Machine Guarding Safety Products. Catalog AZ-6R2. Hawthorne, NY, Schmersal Safety Interlock Switches.

9. Machine Safety Products. P/N 98500, Minneapolis, MN. Banner Engineering Corporation, 1998-99.

10. Factory Automation Products. Catalog No. GC SFC1 9/96/70M. Schaumburg, IL, Omron Electronics, Inc.. Safety-door Lock Switch, D4BL.

11. Allen-Bradley Sensors and Allen-Bradley Industrial Controls. Publication C-111. Milwaukee, WI, Allen-Bradley Company, Inc., March 1995. pp. 3-22, 1-20.

12. MICRO SWITCH Sensing and Control, Industrial Switches and Sensors. Freeport, IL, Honeywell Inc., April 1997. p. D38.

13. "Selection and use of work practices," 29 CFR 1910.333. Washington, DC, Occupational Safety and Health Administration, as published in the Code of Federal Regulations Title 29, Part 1900 to 1910.999, revised as of July 1, 1998, pp. 852-853.

14. Engineering Guide to Machine & Process Safeguarding. STI part number 99276-0010. Fremont, CA, Scientific Technologies Inc., 1998-99. p. A37.

SAFETYALERT

August 1999 **Vol. 1 No. 4**

AFFILIATED COMPANIES

Triodyne Inc.
5950 W. Touhy Ave.
Niles, IL 60714-4610
Phone: (847) 677-4730
FAX: (847) 647-2047
E-mail: infoserv@triodyne.com
Web: http://www.triodyne.com

Triodyne Safety Systems, L.L.C.
5950 W. Touhy Ave.
Niles, IL 60714-4610
Phone: (847) 677-4730
FAX: (847) 647-2047

Triodyne Fire & Explosion Engineers, Inc.
2907 Butterfield Road
Suite 120
Oakbrook, IL 60521-1176
Phone: (630) 573-7707
FAX: (630) 573-7731

Institute for Advanced Safety Studies
5950 W. Touhy Ave.
Niles, IL 60714-4610
Phone: (847) 647-1101

Alliance Tool & Manufacturing, Inc.
91 East Wilcox Street
Maywood, IL 60153-2397
Phone: (708) 261-1712
FAX: (708) 345-4004

Triodyne-Wangler Construction Company, Inc.
5950 W. Touhy Ave.
Niles, IL 60714-4610
Phone: (847) 647-8866
FAX: (847) 647-0785

Editor: ***Paula L. Barnett***

Illustrated and Produced by
Triodyne Graphic Communication Group