ISSN 1041-9489

SAFETY BRIEF

June 1992 Volume 7, No. 3

Triodyne Inc.
Consulting Engineers and Scientists
5950 West Touhy Avenue Niles, IL 60714-4610 (708) 677-4730
FAX: (708) 647-2047

Safety Interlocks – The Dark Side

Frank B. Hall, P.E., J.D. *

Abstract

Every safety interlock brings to an interlock application its own risks which tend to offset the intended safety. The balancing of those risks against the safety afforded must always be considered in the ultimate decision of ***whether or not****, under all the circumstances of the intended application,* ***the safety device should be used at all****. Often the risks outweigh the safety benefits.*

This Safety Brief covers general observations on interlocks, the myth of the perfect interlock, design considerations in choosing an interlock, mechanisms of defeat, reasons for failure, the implications of false reliance on interlocks, regular verification of interlock integrity, redundant interlocks, and the probability of failed interlocks being repaired or replaced. It emphasizes the difference between primary and secondary protection. Machine elements and controls in a normal operating mode are defined and the energy relationships between them are illustrated. An objective of this paper is to enable readers to judge for themselves the effectiveness of interlocks and of various alternative safety measures.

GENERAL OBSERVATIONS ON INTERLOCKS

There is a present-day philosophy that attempts to dictate that all hazards shall be reduced by strictly technical means - the ultimate being to achieve the foolproof machine on which no one can be injured no matter what the operator does. The miraculous device that is invariably suggested for this purpose is the interlock.

Everyone who has struggled with the problem of trying to reduce machine hazards knows that even the most ingenious systems and devices have Achilles heels. Somewhere, somehow, the ultimate success or failure of the system or device will depend on people.

When programs focus solely on making a machine foolproof, they are insidiously harmful. They tend to neglect the training of operators and maintenance personnel in basic principles of safety practices and attitudes. To pursue blindly the ideal of the foolproof machine by the panacea of the interlock may in fact result in an increase of hazards. The machine with no moving parts, that instantly turns into foam rubber should anyone accidently run into it, still remains a technological dream.

The choice of the kind of interlock to use in a particular instance is a difficult, sophisticated engineering decision. The choice of whether or not an interlock should be used at all is often an even harder choice, calling for a consideration of basic principles. The choice is based fundamentally on whether or not the application permits use of primary protection.

It is almost impossible to define the term, "safety interlock." For instance, every limit switch used to sense position on an automatic machine is really an interlock. The presence sensing floor mat is also an interlock – with a different purpose. It might seem simple to distinguish the mat as having a "safety" purpose, and the other as having a programming purpose in the machine's cycle.

The distinction fails. Any switch can malfunction and some might cause "train wrecks" that in turn might injure personnel. Thus, perhaps every interlock might be traced through some set of consequences to show that it has a relationship to safety. A possible definition of the kind of interlock addressed here would be an interlock intended primarily to reduce risks. The definition is not satisfactory, but will have to serve for our purposes.

THE PERFECT INTERLOCK IS A MYTH

It should be recognized early that not only is a perfect interlock a myth, but it is almost certain that if a perfect interlock could be devised, it would be impractical to use. At least, one manufacturer of an interlock device apparently found it so. Let us look at his patents as an example:

U.S. 3,743,800, "Mechanical Safety Interlock for Covers of Explosion-Proof Electrical Housing." [2]

U.S. 4,031,340, "Defeater for Mechanical Safety Interlock for Covers of Explosion-Proof Electrical Housing."[12]

REASON FOR THE INTERLOCK
(What U.S. 4,031,340 says about U.S. 3,743,800)

"Where electrical circuit breaking devices, such as switches, etc., are located in an area in which explosive atmospheres may be present, provision must be made to prevent those circuit breaking devices from igniting the atmosphere and thereby causing an explosion. The conventional procedure is to enclose such devices in a case which will prevent any ignition which occurs within the case from propagating to the space outside the case. Such cases must, of course, have access openings so that the installer or a repairman can get at the electrical devices within the case. Such access openings are provided with covers."

"A common practice is to utilize an interlock between the electrical device within the case and the cover that will prevent the cover from being removed should the device be in switch closed position. Otherwise, it would be possible for a careless person to remove the cover and thereafter move the device to the switch open position, with the result being that the flame occurring within the case could easily propagate to the outside through the access opening from which the cover had been removed. An example of such a device will be found in U.S. 3,743,800."[12]

Now the manufacturer has to invent a ...*DEFEATER!*

REASONS FOR DEFEATING THE INTERLOCK

"It has been found that there are occasions where it is important that a serviceman, etc., be able to remove the cover while the electrical device within the housing is in switch closed position. For example, one or more large machines may be electrically connected to the box. It could, for example, be a machine involved in a continuous process which, if interrupted, would result in a prolonged restarting operation and loss of product in process. Shutting such machines down even briefly might be an expensive procedure. Yet, for some good reason the serviceman must have access to the interior of the housing. Also, the serviceman may have gas detectors available by which he can determine that an explosive atmosphere does not exist about the housing; and, therefore, a temporary removal of the cover to provide access to the interior of the housing without fear of causing an explosion. Even if he knew an explosive atmosphere existed, the experienced serviceman might know that with his knowledge and experience, work could safely be performed inside the box without the necessity of interrupting the electrical circuit."[12]

COMMENTS ON THE DEFEATER

"One solution to this problem might be to remove the safety interlock altogether. However, this would permit careless individuals, or individuals who did not have sufficient knowledge of the situation, to be careful about what they did to remove the covers. Thus the possibility of an explosion would remain. The solution provided by the present invention is to provide a defeater operable from the exterior of the housing to render the safety interlock ineffective so that the covers can be removed. The exterior, operable part of this defeater is inconspicuous. One not sufficiently knowledgeable to know about the interlock, why it was there, etc., would not recognize the defeater for what it was and therefore would not use it to obtain access to the interior of the housing. Instead, he would follow the conventional practice of turning the switch handle to the 'off' position to permit him to remove the cover."[12]

So the manufacturer who had produced this interlock device found his customers could not live with it and had to produce a "defeater" for it! *ANSI Z241.1* recognizes this need explicitly in paragraph 4.1.7.5 "Defeating Protective Devices," and in paragraph 4.1.7.4 "Troubleshooting with Power on." [1]

There are many situations analogous to that of the explosion proof electrical housing. Intentionally defeating an interlock is almost routine in troubleshooting. When this legitimate procedure is abused by intentionally defeating an interlock to facilitate production or operation, the fundamental weakness of the interlock becomes clear.

SOURCES OF HAZARDS ON ELECTRIC/ PNEUMATIC/HYDRAULIC-CONTROLLED MACHINES RESULTING FROM UNEXPECTED MOVEMENT

Movement results from energy applied deliberately or inadvertently. Injury can result if the movement is unexpected. Understanding the ways in which this can happen is facilitated by separating the area in which energy is controlled in the machine. There are seven areas involved and they are shown in Figure A as seven boxes. Each box shows one of the following elements of a machine in normal running condition.

1. Energy sources
2. Stored energy
3. Power initiators (Power controllers)
4. Power actuators (Converters from electric power or fluid power to mechanical power)
5. Movable machine elements
6. Secondary initiators
7. Manual operation of power initiators

ILLUSTRATIONS EXPLAINED

Figure A is an energy control chart, with numbering which applies to machine elements in subsequent Figures A1 through F.

Figures A1, A2-EM1 to A2-EM5 and A-3 to A7 are intended to be simple tutorials on electric and air/oil fluid circuits.

Figures B-F show energy relationships for Figure A. Note that Figure C shows stored energy hazard; Figure D offers maximum protection (primary protection!), being isolated from all energy sources and from stored energy.

Figure E shows secondary protection by interlock (defeated by malfunction); Figure F shows secondary protection (defeated by manual override).

Figures G and H show the manner of interlock *actuation*, by negative and positive modes, and how a machine is made unsafe by interlock malfunction.

Figure I defines the ways in which malfunctions may occur, i.e., permissive and preventive.

The next text identifies and defines machine elements, starting with movable elements that might cause injury and working back to the contributing factors. Numbers of elements as they are used in illustrations are shown in parentheses.

Movable Machine Elements (5) are clamps, brakes, elevating tables, conveyor belts, mixing paddles, augers, sealers, applied tools, drills, positioners, measuring devices, fans, pumps, compressors, slides, et cetera.

Power Actuators (4) are devices that convert electric power or fluid power (generic term for pneumatic or hydraulic pressure systems) to mechanical power. For example:

Electric:
Motors driving machine elements
Motors driving hydraulic pumps
Clutches engaging drives
Electromagnets

Pneumatic/hydraulic:
Motors driving machine elements
Cylinders, single and double-ended
Rotary power actuators

Initiators. From ANSI Z241.1: "2.27 Initiator. A device that causes an action of controls or power actuator." E.2.27. Initiator. Typical manual initiators are pushbuttons, foot switches, manual starters, hand valves and other valves with manual overrides. Typical non-manual initiators are limit switches, pressure switches, temperature-actuated switches, flow switches and cam actuated valves."

Air/oil initiators that directly control power are so designated, "power initiators (3)." Initiators that control power initiators are designated as secondary initiators (6). Perhaps an analogy will help. The bouncer in a tavern who physically throws the unwelcome guest out the door is a power initiator (3); the manager who signals the action by pushing the bouncer in the direction of the troublesome guest is a secondary initiator (6).

Because there are both electrical power and air/oil power, the initiators are also designated accordingly. Air/oil initiators respond by opening or blocking passages in valves, by changing pressure or volume of flow in the system. A directional valve, for instance, whose ports are connected to a cylinder can cause the cylinder rod to extend or retract - a power initiator (3). A smaller valve might operate that power valve by applying pressure to one end or the other of the power valve spool - a secondary initiator (6).

Electric power initiators (3) act to connect available line voltage to a motor, thus causing it to run; to an electromagnet to energize it; or to a clutch to engage it or disengage it. Thus, power is applied by the power initiator (3) to the power actuators (4).

The initiators that signal the power initiators are secondary initiators (6). Examples of secondary electric initiators are hand devices such as pushbuttons, hand valves, limit switches, interlocks, and automatically controlled outputs from relays or programmable logic controllers.

Thus, most power initiators (3) are controlled by other initiators which in turn are operated manually, by position, flow, pressure or other machine signals. These secondary initiators, which do not themselves control or apply power directly are secondary initiators, (6).

An example of a power initiator (3) is a magnetic motor starter (controller). It connects the motor (power actuator (4) to or disconnects it from the primary voltage. The START and STOP pushbuttons are *secondary initiators* (6) whose circuits cause (signal) the starter to operate, thus allowing indirect control of energy to the motor and causing it to drive a fan (5).

A directional valve (power initiators (3) controlling the flow of energy to a power actuator may in turn be controlled by electrical solenoids (*secondary initiators* (6). Often when the valve is large, instead of direct solenoids, it will be pilot-operated by a small directional solenoid valve. The small valve is a secondary initiator whose solenoids are even more remote *secondary initiators*. Sometimes the primary (power) valve and the pilot valve are incorporated in a single valve body.

Manual Operation of Power Initiators (7)

It is essential to understand that nearly all initiators, power or secondary, provide for manual actuation of the device. Unless primary protection is in effect there is no reliable way to stop signals (from secondary initiators) from reaching a primary initiator. And even if you could, there is no way to prevent someone from *manually* actuating the power initiator (7).

For manual actuation, sometimes a tool is required; sometimes a button is provided. A detent feature is often present. *This is also significant as a safety consideration!* Not only can an attempted secondary protection be overridden manually, but an initiator left by accident in a detented (other than normal) position can cause an unexpected movement when power is restored.

The prevention of an unexpected machine movement during servicing or maintenance requires that no energy reach a power ac-

1

ENERGY SOURCES

A machine may have any one or any combination of the following:

COMPRESSED AIR
PNEUMATIC POWER

Disconnect from machine by a shutoff valve.

HYDRAULIC POWER

Hydraulic pump driven by electric motor.
Disconnect switch controls energy to motor.

A.C. or D.C.
ELECTRIC POWER

Disconnect switch shuts off power to machine

7

MANUAL OPERATION OF POWER INITIATORS

6

SECONDARY INITIATORS

ELECTRIC:
- Pushbuttons
- Limit switches
- Flow switches

AIR or OIL:
- Pilot valves
- Hand valves
- Solenoid valves

MALFUNCTIONS:
- By-passing shorts

MANUAL OVERRIDE of secondary initiators

3

POWER INITIATORS (CONTROLLERS) such as:

MAGNETIC STARTERS for starting and stopping electric motors

PNEUMATIC or HYDRAULIC POWER VALVES

All of the above operated by secondary initiators.

2

STORED ENERGY (Such as potential and kinetic energy)

Stored throughout machine but lumped here for convenience. Energy might be stored in 1, 3, 4, 5 or 6.

(Elevated parts, springs in compression or in tension, parts still rotating.)

Air or oil under pressure in hose, tanks, or accumulators.

4

POWER ACTUATORS

Convert electric power or fluid power to mechanical power

Examples: Motors, brakes, clutches, cylinders, rotary units

5

MOVABLE MACHINE ELEMENTS

Driven by Power Actuators

Pulleys, clamps, presses, transfer slides, rotators. Movement in general.

Figure A - Energy control chart of electric/pneumatic/hydraulic-controlled machine. Relationships among elements are shown in Figures B through F.

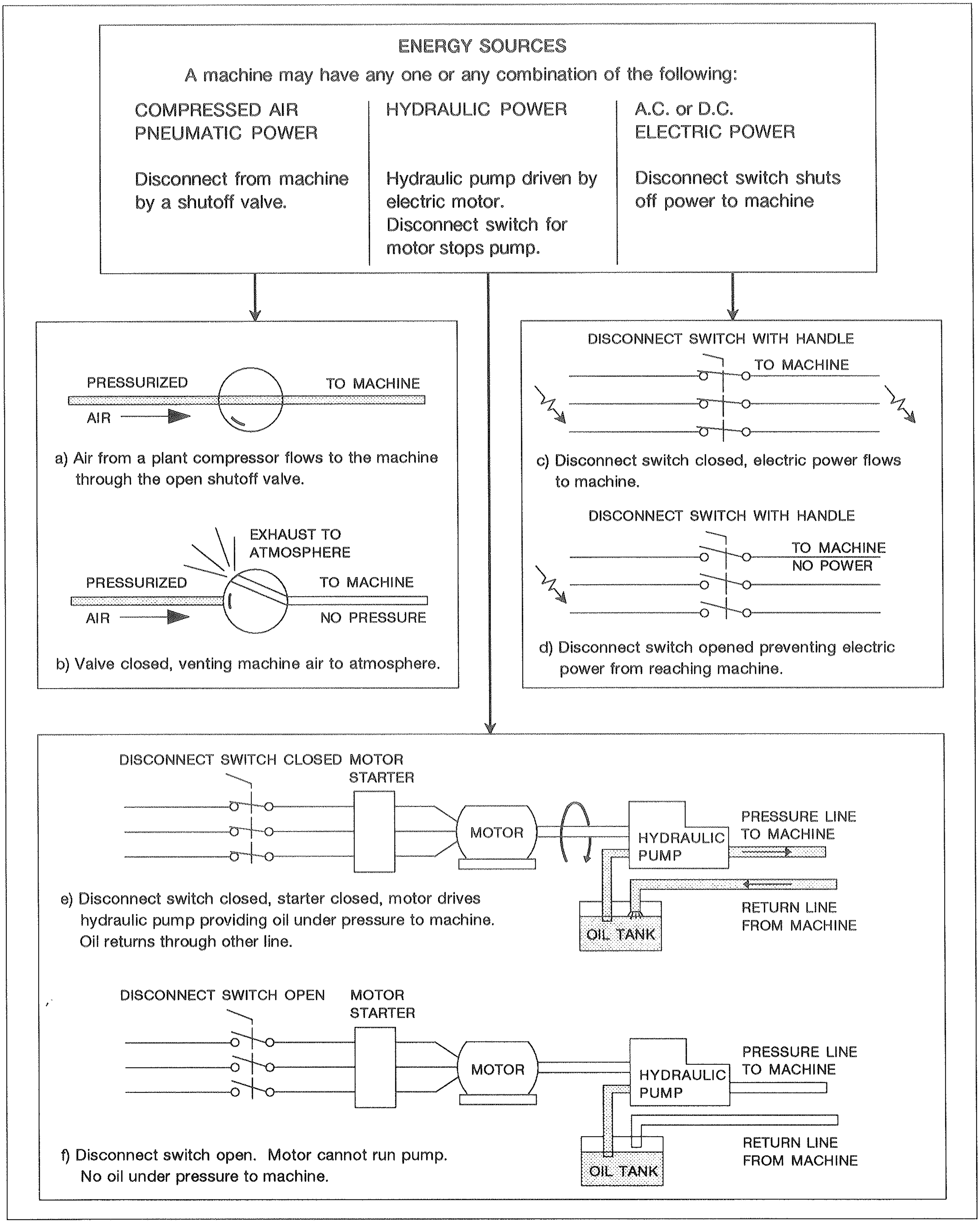


Figure A1 - Detailed examples of three common energy sources (See Figure A Box 1).

tuator. If the energy source is isolated from the machine and locked out, then none of the power initiators can have any effect. The actuators are then unable to produce a movement (Figure D). This is called *primary protection* and is required either by OSHA lockout/tagout [3] or by Zero Mechanical State[1].

Stored Energy (2)

Both the OSHA lockout and ZMS procedures require that stored energy be isolated, reduced or otherwise controlled. Stored energy includes potential or kinetic energy stored in the movable element itself (for example, the kinetic energy of a rotating part with large inertial energy or the potential energy of an elevated part that might descend if not blocked). Energy stored in surge tanks, accumulators or even in distended hose or from an extender cylinder under a gravity load, must be prevented from reaching an actuator.

Realize that Figure C does *not* represent ZMS or OSHA lockout even though energy from the source has been locked out. Stored energy (2) may still be present. Figure D does represent ZMS and OSHA lockout/tagout.

Note that primary protection consists not only of the lockout or shutoff of primary energy, but also the lockout, shutoff or reduction of stored energy. See Figure D, which shows stored energy reduced.

An attempt to attain primary protection without the added prevention of stored energy is dangerous. See Figure C.

ENERGY SOURCES:
ELECTRICALLY POWERED MACHINES
(EXAMPLES OF FIGURE A BOXES 3, 4, 5 AND 6)

To make information in this paper more accessible to those who have had to forego the fun of dealing with things technical in order to pursue the exhilaration of the law or the heady satisfaction of managing affairs commercial, this section presents basic technical principles through example.

Box 1 (Energy sources) can be explained pictorially by the sketches (a) through (f) in Figure A1.

Boxes 3, 4, 5 and 6 are shown in Figure A2 which is an example of a magnetic starter (3) controlling an electric motor (4) driving a conveyor belt (5). The magnetic starter (M) with its contacts on the I-bar is an example of Box 4 Power Initiators. The magnetic starter is represented as an E-structure of magnetic steel laminations with a coil of wire around its middle leg. Below it an I-bar of steel is suspended and normally drops away from the E-structure by gravity - that is, it drops away when the structure is not magnetized by current passing through the coil.

The I-bar is called the armature and carries four sets (M1, the "holding" contact, M2, M3, and M4, the power contacts) of some conductive bars that close across contacts when the I-bar is magnetically attracted to the E-structure. When M2, M3 and M4 close, power is connected to the motor which then drives the conveyor belt.

In Figures A2 and A3, we are going to illustrate the action of the circuit that controls the magnetic starter. Example of Box 6: Secondary Initiators: Let us put a magnifying glass on the secondary initiators section of Figure A2 and A3. See Figure A2-EM1. The wires are numbered 1 through 5. Dashed lines represent non-conductive parts that are mechanically supported by the device. Each pushbutton or contact has a spring (not shown) to restore it to the position of A2-EM1 after it has been actuated and released.

For instance, the interlock contact between 1 and 2 opens if the door beneath it is opened by sliding it downward. Should the STOP button between 2 and 3 be depressed momentarily, its contacts will open but as soon as it is released, its spring will close it again. When the START pushbutton is depressed to close the circuit between 3

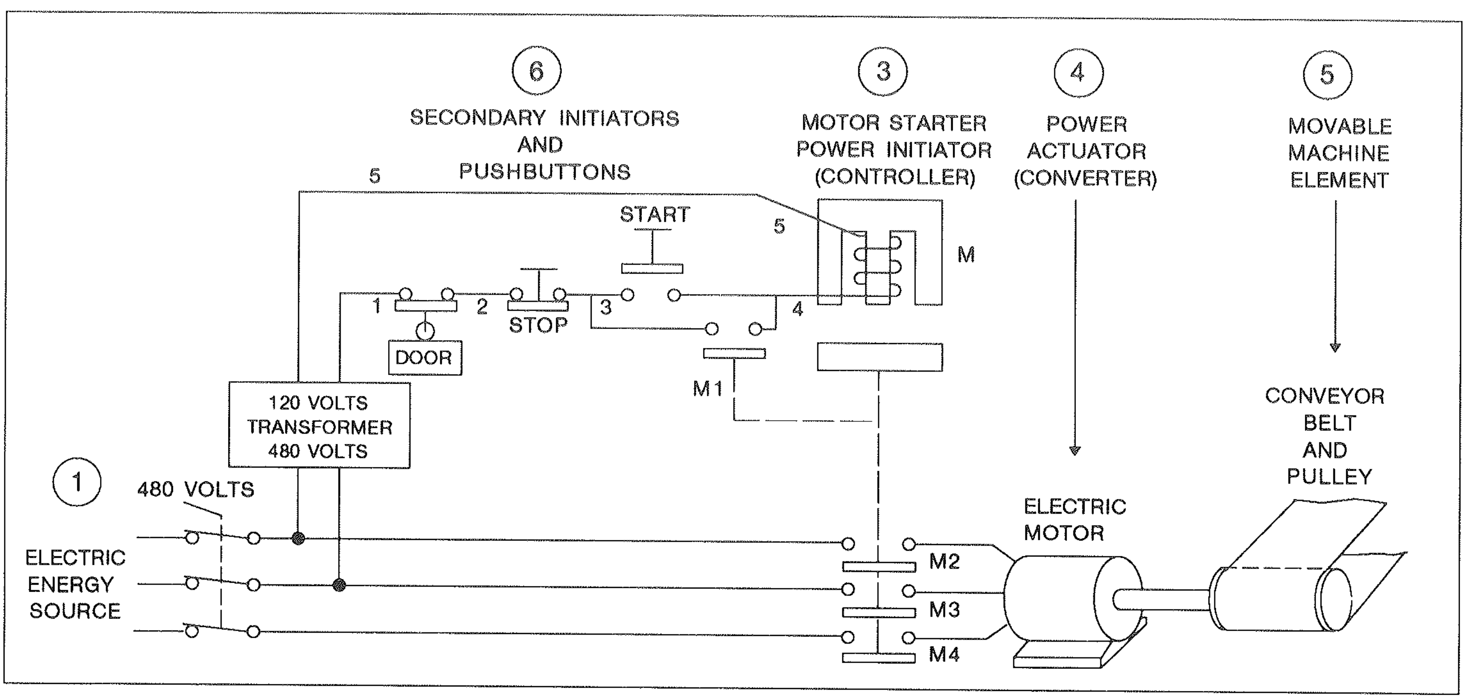


Figure A2 - Electromagnetic operation of a motor starter, motor, and driven conveyor (not energized).

Figure A2 - EM1

Basic magnetic circuit with interlock, STOP and START pushbuttons.

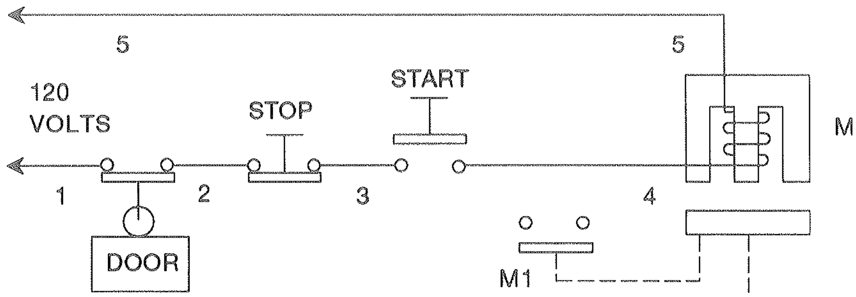


Figure A2 - EM2

Circuit opened by both STOP button depressed and interlock switch deactuated because of open door. Even though START button is closed, no current flows, therefore no magnetic effect.

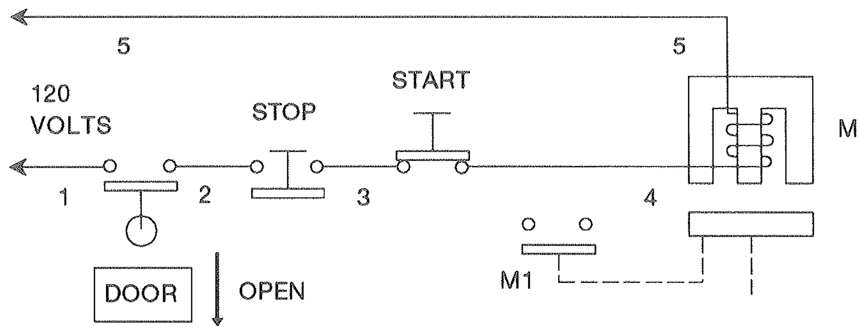


Figure A2 - EM3

START button closes circuit, current flows through coil producing magnetic effect.

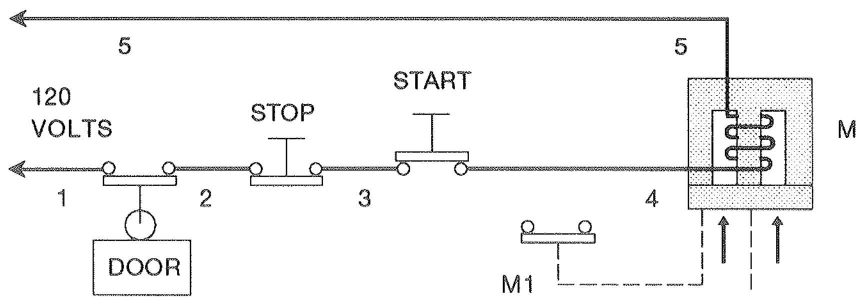


Figure A2- EM4

Wires "a" and "b" connect M1 in parallel with START. Same effect as EM3 but START button can now be released because M1 takes its place. See EM5.

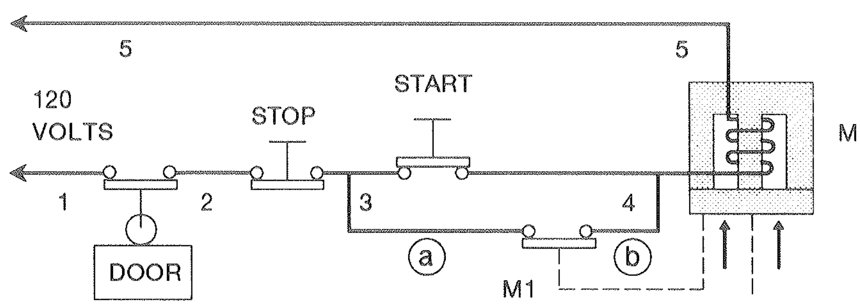
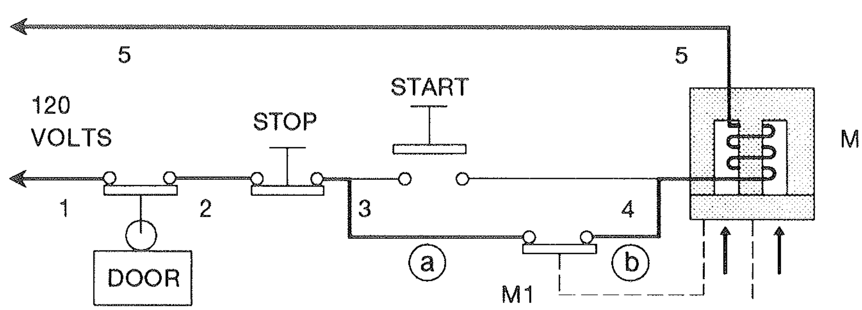


Figure A2 - EM5

Magnet remains until power is lost or interlock or STOP button interrupts current.



and 4, as soon as it is released, its springs will open the contact again (A2-EM2).

Whenever electrical current passes through a simple coil of wire, a magnet is formed. When the current ceases, the magnetic field collapses. When the coil is formed around a structure of magnetic steel, the magnetic effect is concentrated and requires less current.

Thus, when the START pushbutton is pressed, the circuit is complete without any open sections and current passes through the coil of the E-structure. It becomes magnetic, attracts the I-bar with its contacts and remains magnetic as long as the current flows (A2-EM3).

In A2-EM4 and A2-EM5, we have rewired the circuit by adding wires "a" and "b." Contact M1 has thus been wired in parallel with the START pushbutton.

Because you do not want to have to keep your finger on the START pushbutton to keep the motor running, you must get something to substitute for the START pushbutton. Remember the contact M1 that closes when the I-bar is attracted to the E-structure? By connecting it in parallel with the START pushbutton by means of wires a and b, it closes at the same time (A2-EM4), and when the START pushbutton is released, the current continues to flow, maintaining the magnet (A2-EM5).

The conditions in A2-EM5 are identical to those shown in Figure A3, except that the START pushbutton has been released. It was necessary to press the START pushbutton only *momentarily* in order to keep the motor running. Any interruption of the current by sliding the door down and thus opening interlock contact or by pressing the STOP pushbutton *momentarily* will immediately result in the motor and conveyor stopping. A2-EM5 followed by the open contacts shown in A2-EM2 result in Figure A2-EM1.

Additionally, if there is a power outage, the conveyor and motor will stop and, when the power is restored, the motor and conveyor will NOT restart automatically. Thus, after a power outage when power is restored, machines on this kind of control do not start unexpectedly again. Compare this to a power outage in your home when all the lights go out. When power is restored, the lights go back on. Suppose you were using an electric lawnmower. It would stop but when the power was restored, the mower would start again because it is on a maintained contact switch.

ENERGY SOURCES: PNEUMATIC/ HYDRAULIC-POWERED MACHINES

Figure A Box 1 is explained in detail by Figure A1. The sketches (a) through (f) are intended to be self-explanatory. A short description, however, about pneumatic (compressed air) and hydraulic systems may be helpful.

Compressed air is usually provided through the plant from large compressors and a practical working pressure is 65 to 75 psi (pounds per square inch). The cylinders that must work with this pressure get very large when heavy forces must be available. Another characteristic is that there is no "tank" line, since the exhaust air can simply be released to the atmosphere.

When forces required are very large, hydraulic operation is favored because the actuators can then be smaller. Usually the source of hydraulic pressure will be a hydraulic pump at the machine, driven by an electric motor. When you want to stop the hydraulic pressure, you simply stop the drive motor and lock it out.

Commonly systems are run at under 1500 psi. Systems up to 5000 psi are not rare, and pose a special type of hazard. If a pinhole hose leak develops, you do not look for it by touch or you may get a sudden injection that will blow up your arm like an automobile tire. The exhaust oil cannot be released to the atmosphere like exhaust air, but is directed back to the tank by a tank line.

Hydraulic systems have many strange and mysterious ailments caused by internal leak-

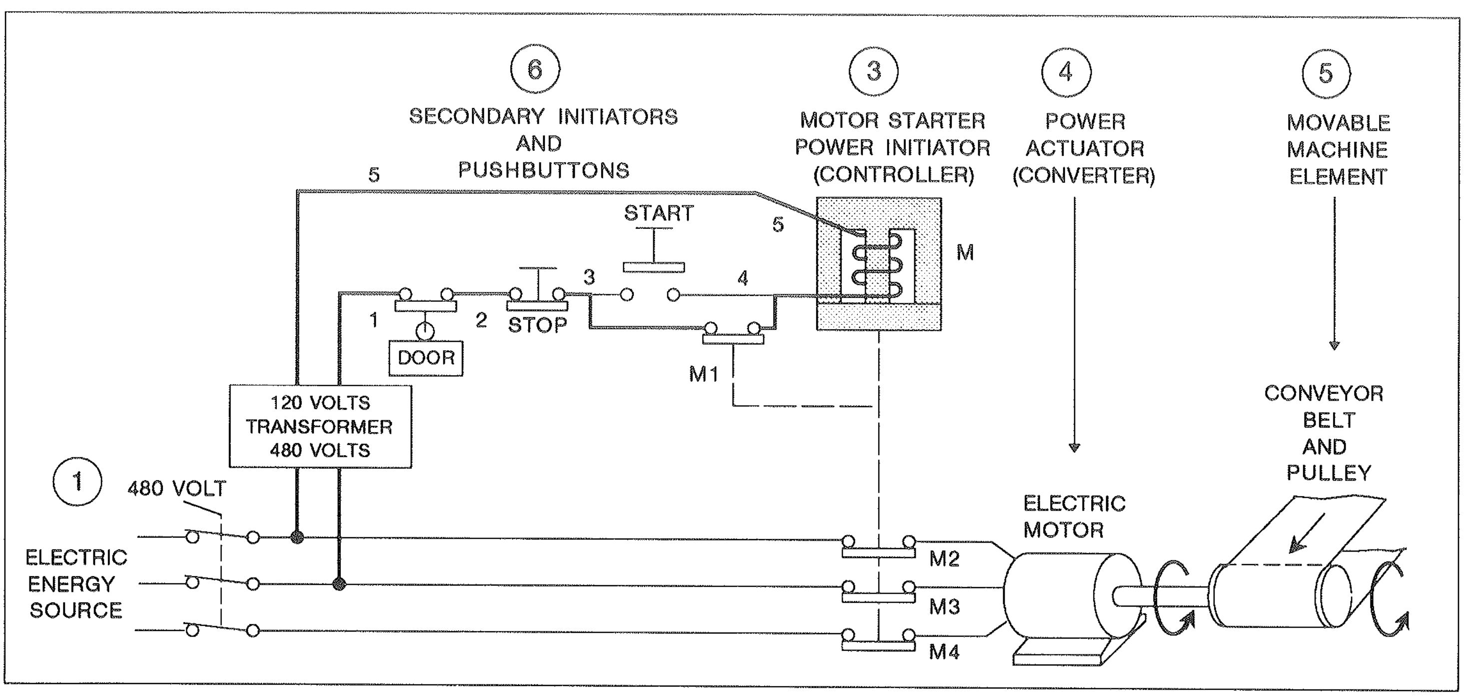


Figure A3 - Electromagnetic operation of a motor starter, motor, and driven conveyor (energized).

age of valves and other components when they become worn. Backpressure caused by pipes too small for discharge quantities sometimes results in weird symptoms that enliven the working day of the design engineer.

In hydraulics or pneumatics, the power initiator (3) is usually a directional valve. As you can see in Figure A4, the valve consists of a body with a hollow interior into which fits a special sliding spool. When not controlled or actuated in any way, this particular valve is caused by springs at each end to assume a centered position. Here the result is to block all passages. One of the advantages of this valve is that if control power were lost, the valve would simply stop all motion.

HOW the spool is moved to either of the other two positions is not shown but will be discussed. It can be moved manually by means of a rod at each end, extending outside the valve body. It could be moved by putting a solenoid (a magnet operated by a coil) on each end rod. The actuating rods are then moved by simply closing an electric circuit to the desired solenoid to work its rod. The actuating force would come from the magnet, causing a rod to move rather than causing contacts to be closed. See A2-EM1thru A2-EM5 and picture a rod on the I-bar instead of contacts.

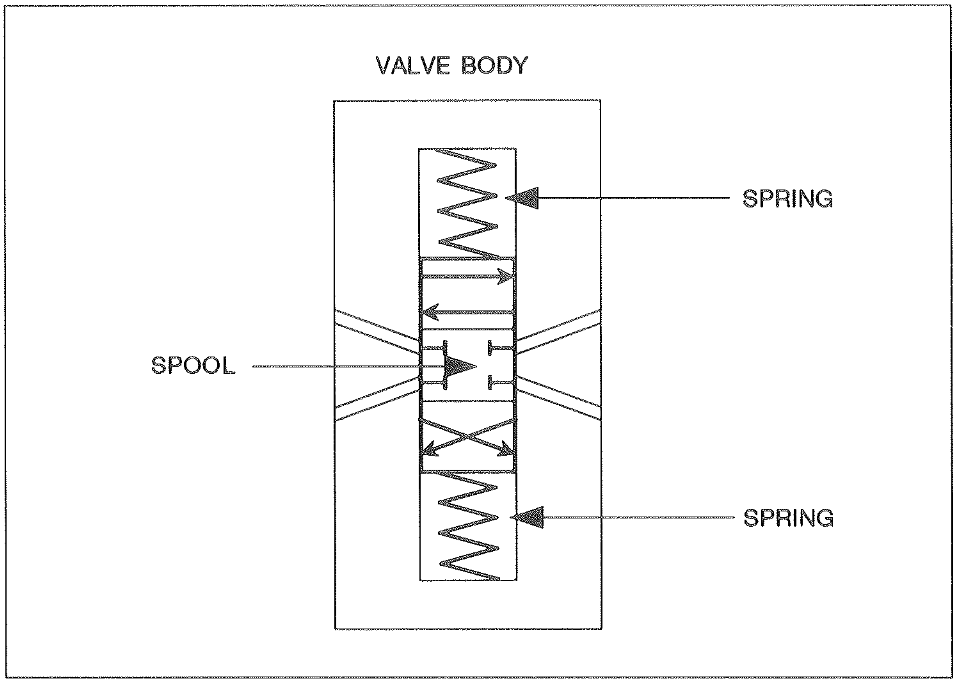


Figure A4- Basic directional valve parts.

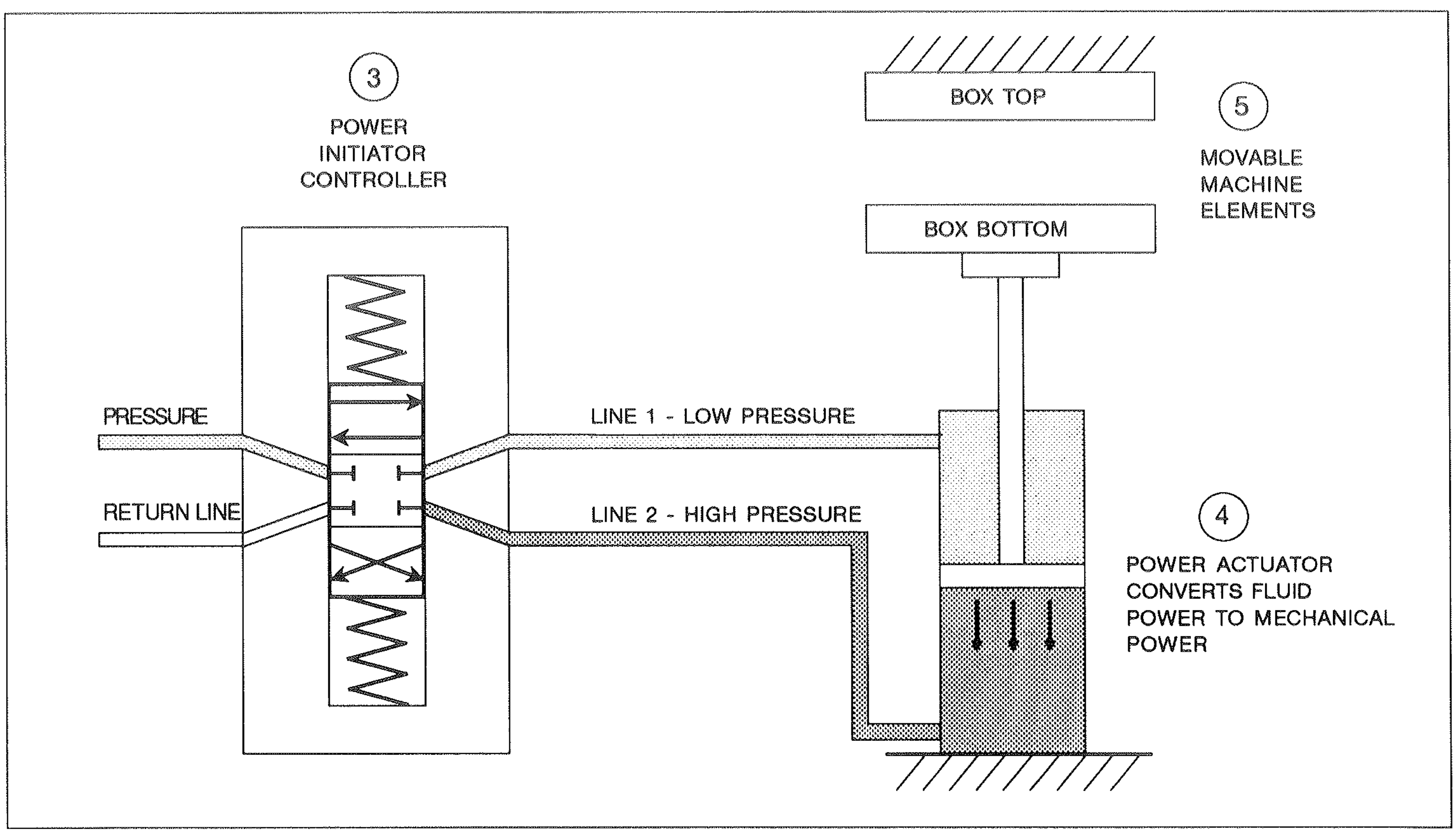


Figure A5 - Machine element stopped. Elevation of heavy box equals stored energy.

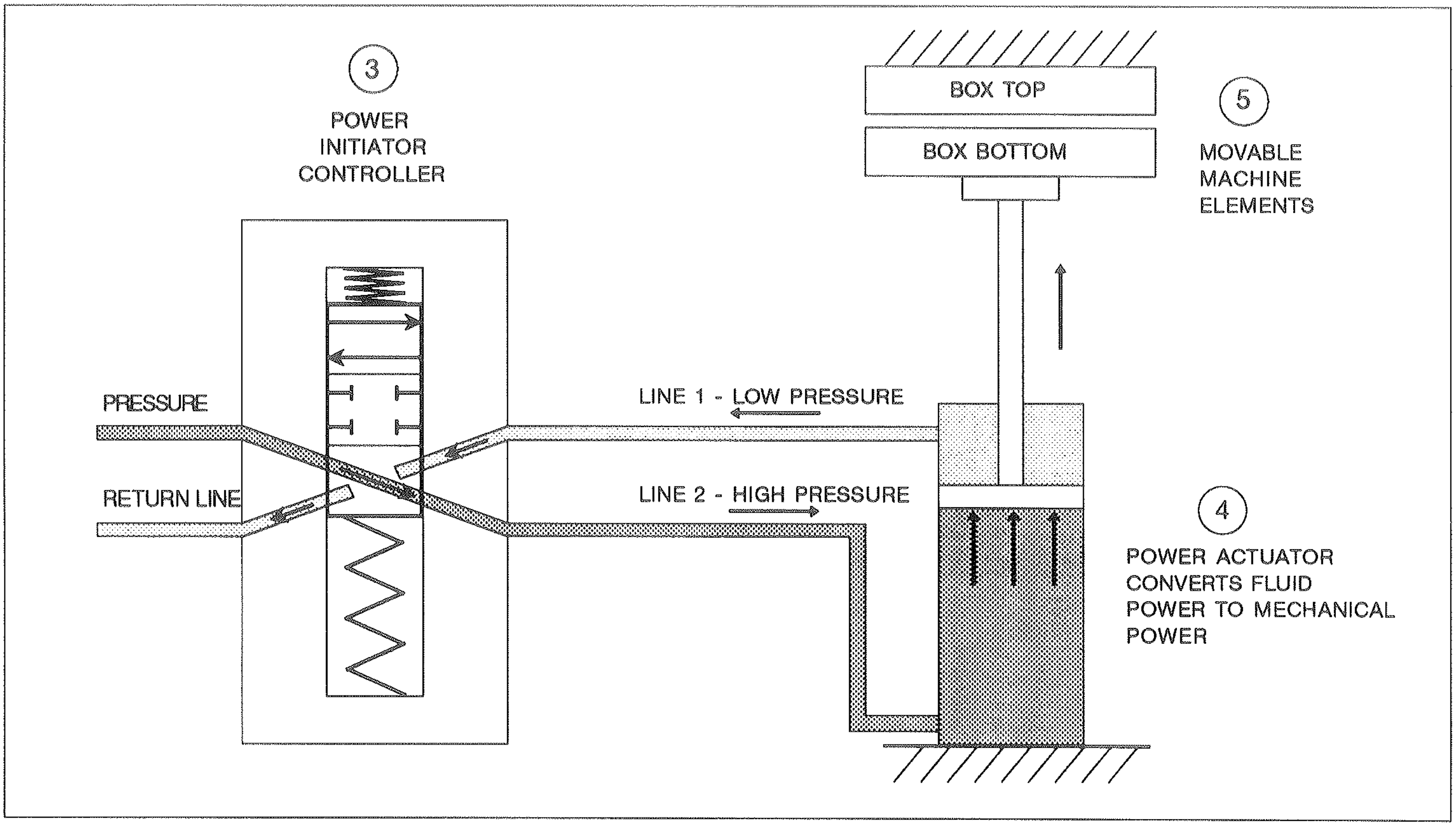


Figure A6 - Valve spool position directs oil under pressure to blind end of cylinder, extending cylinder rod and raising box bottom.

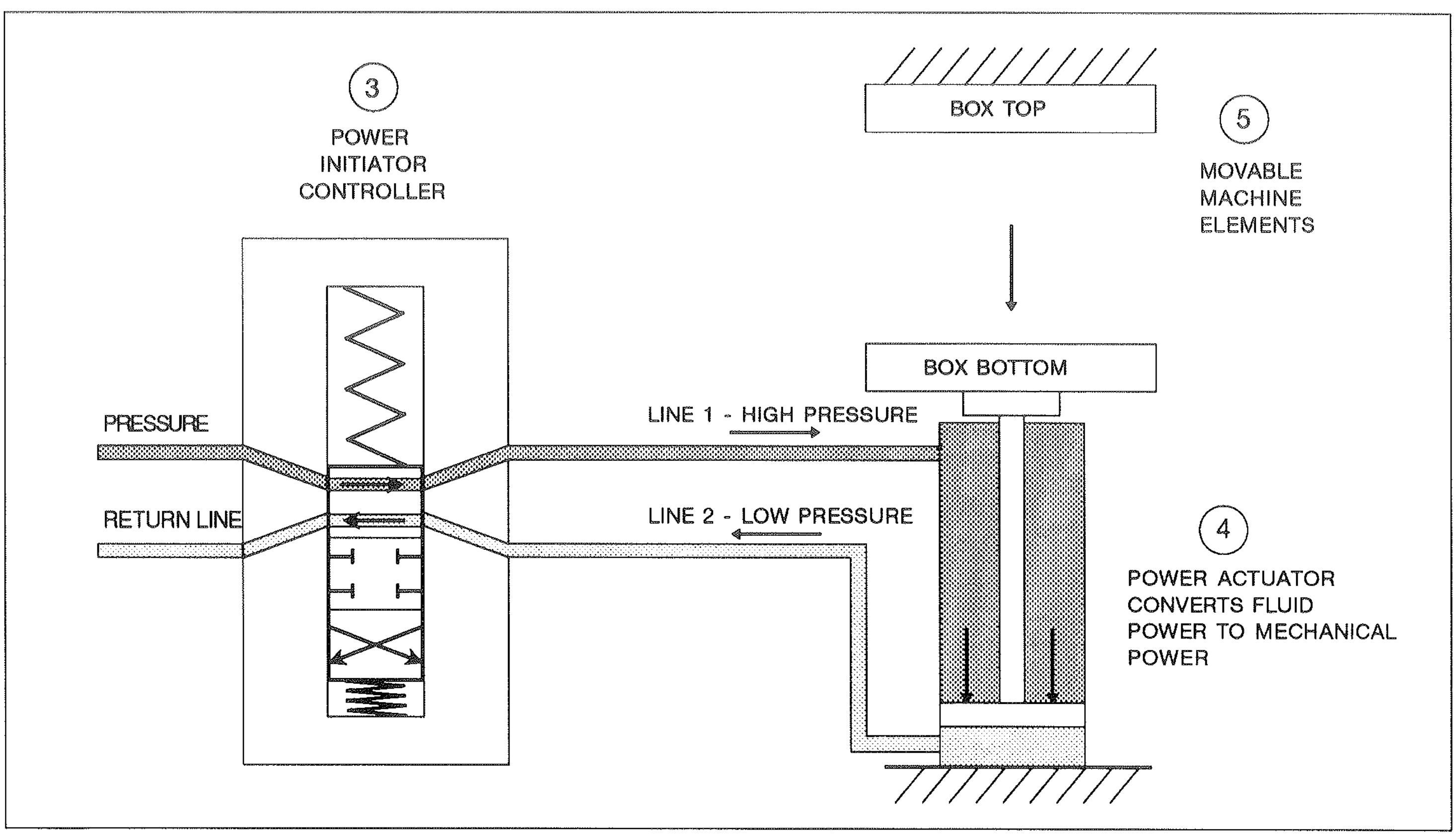


Figure A7 - Valve spool position directs oil under pressure to rod end of cylinder, retracting rod and lowering box bottom.

Whatever means was chosen, operating the spool from either an electric circuit or a small hydraulic circuit would be using secondary initiators (6). The valve itself is a power initiator (3) and it is shown controlling a power actuator (4) which in turn is causing a movable machine element (5) to stop (Figure A5) to move upward (Figure A6) or to move downward (Figure A7).

The principal idea to grasp is that the power is controlled through a large valve POWER INITIATOR (3) to a cylinder POWER ACTUATOR (4), operating a MOVABLE MACHINE ELEMENT (5). The POWER INITIATOR (3) is controlled (signalled what to do) by SECONDARY INITIATORS (6) such as a magnetic device or a smaller valve or even by a MANUAL (7) operator.

Remember, if you understand how energy gets to BOX 5, you will be able to judge how effective various alternative safety measures will be. Figure A helps analysis by grouping the complex machine and control functions into seven basic areas.

Figures B,C, D, E and F illustrate relationships that are possible among the elements of the Energy Control Chart shown in Figure A.

- Fig. B: Normal operation of machine
- Fig. C: Only primary power locked out, stored energy still present
- Fig. D: Primary protection
- Fig. E: Secondary protection defeated by malfunction
- Fig. F: Secondary protection defeated by manual override

HOW "PRIMARY/SECONDARY PROTECTION" RELATES TO INTERLOCKS

To the uninitiated, there is little difference between a "safety interlock" limit switch and a line voltage main disconnect switch to shut off power completely. When both a "safety interlock" and a main disconnect are present, it is easier to rely on the "safety interlock," and to ignore the disconnect switch. It is the purpose of this section to explain why the easier selection is the more dangerous.

There are two concepts that emphasize the two states of protection against unexpected and inadvertent movement of a machine - *secondary* protection and *primary* protection. An understanding of these concepts makes clear the limitations of interlocks (which are secondary protection). It also explains the conclusion: *When a choice is possible between the two, never choose secondary protection. Always choose primary protection.*

Sometimes personnel attempt to use secondary protection instead of primary protection because they are unaware of the risk involved. This is illustrated by Figure E. That is, instead of isolating the energy (Figure D), they incorrectly try to prevent movement by stopping the signals from some secondary initiators (6). A typical attempt is to padlock a STOP pushbutton in the depressed condition, believing that this will prevent the drive motor from being started.

This is only secondary protection and should never be relied on when primary protection is possible. For example, even with the stop pushbutton locked out, someone at the starter could manually close it with a screwdriver or other tool, and thus start the drive motor (See Figure F). For instance, look at Figure A2. To manually operate the motor starter, all you need to do is push the armature (I-bar) upward physically.

Secondary protection is an attempt to prevent machine movement by preventing *signals* (6) from reaching the *power initiator* (3), in the hope that machine movement will be prevented. This is not reliable because there are many accidental ways in which a power initiator can be actuated. In addition, most power initiators can be *manually overridden* (7) to an actuated state. That often happens inadvertently. See Figures E and F.

In almost all cases, pushbuttons, selector switches, limit switches and "safety interlocks" are only *secondary protection*. These devices are commonly called CONTROL DEVICES. Every safety program should teach personnel the difference between primary and secondary protection.

Of course, primary protection is not always feasible. For example, if an operator must repeatedly open a guard in order to have access to the workpiece during production, certainly primary protection (shutting the machine down) is not at all practical. Secondary protection then remains something to be considered.

HAZARDS OF CONCURRENT SERVICING

On larger machines, the possibility usually exists that more than one man may be working on different areas requiring service. One might be working on a mechanical unit or cleaning an area, while someone else might be troubleshooting the electrical controls. Sometimes neither is aware of the presence of the other. For instance, an electrician might check the operation of a motor starter either by actuating the armature *manually* (Figure F) with a screwdriver or other tool or electrically by jumpering directly from the control transformer to the starter coil (Figure E).

If primary protection is in effect (Figure D), the disconnect is locked in the open position - this will not matter. But if it is not, and one man is relying on an access door limit switch, even if there are ten levels of redundancy, the motor will start, for he has only secondary protection and his interlock protection has been by-passed or frustrated.

Everyone knows that a competent electrician would never check in this way unless he could be sure that no one is in the path of a machine movement. The real world unfortunately is not universally characterized by competency and the problem is aggravated by use of motor control centers, which otherwise have a number of advantages over the individual starter installations.

Motor control centers, despite all their other advantages, have some disadvantages. Usually they are not close enough to the machine to give personnel working there a good view of the controlled machine and other personnel who might be at risk at the machine.

FALSE RELIANCE INDUCED BY PRESENCE OF AN INTERLOCK

A very serious consideration is whether the presence of an interlock induces personnel to rely upon it rather than upon primary protection (locking open the primary power disconnect when appropriate). [17, 18]

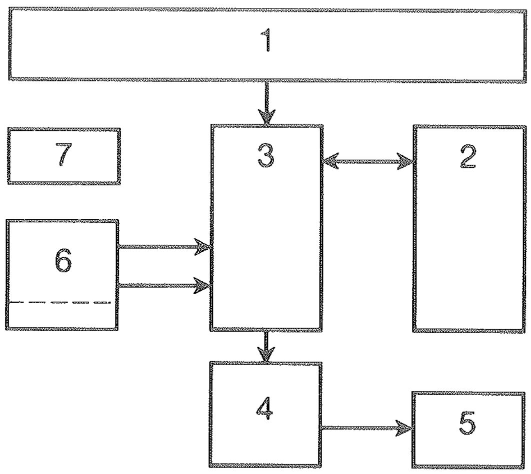


Figure B - The same as Figure A, with machine in operating mode.

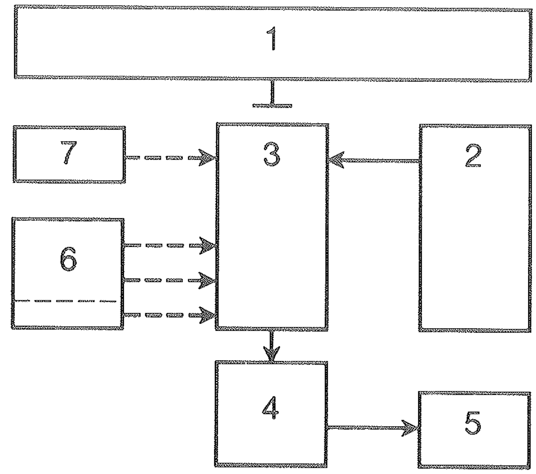


Figure C - Movement is possible when primary power is disconnected but stored energy is still present.

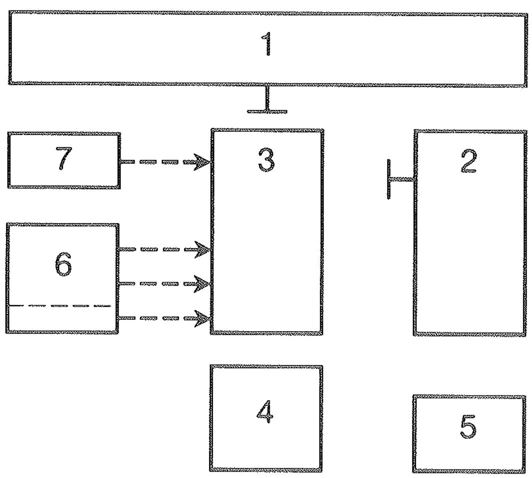


Figure D - PRIMARY PROTECTION. Minimum chance of movement. Energy source locked off. Stored energy reduced or restricted.

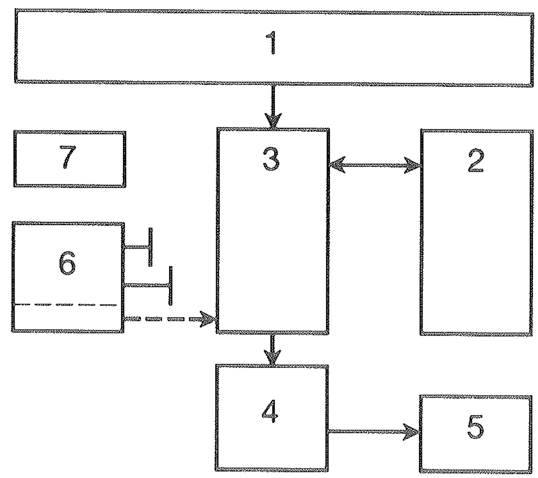


Figure E - SECONDARY PROTECTION. Attempt to protect by secondary means (interlocks). Malfunction causes movement.

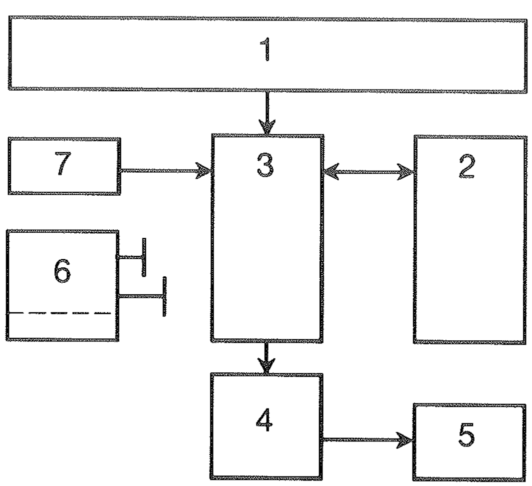


Figure F - SECONDARY PROTECTION. Defeated by MANUAL override of power initiators. Causes movement. Hazardous.

DEFINITIONS OF NUMBERS AS SHOWN IN FIGURE A:

1 - ENERGY SOURCES

2 - STORED ENERGY

3 - POWER INITIATORS

4 - POWER ACTUATORS

5 - MOVABLE MACHINE ELEMENTS

6 - SECONDARY INITIATORS

7 - MANUAL OPERATION OF POWER INITIATORS

Note: Refer to Energy Control Chart - Figure A

In the case *Myerson v. Niagara Machine & Tool Works*[4], neither the jury nor the trial court nor the Appellate Court found any significance in the injured man's having chosen to rely on *secondary protection* instead of upon the *primary protection* his actions demanded. The injured party had studied electrical engineering. The interlock device for the operator was a two-button control (a hostage control requiring one hand on each control for actuation).

It should be noted that it is the *presence* of a so-called "safety system" that the attorney and the court decided that Myerson was entitled to rely on. That is, they decided that because it was a "safety system," he was invited to rely on it and not to lockout the primary power. *As an electrical engineer, he should have known better!* Look at what the court said:

> "From the presence of a two-hand control button device... it would appear to the user completely safe to change dies while the power was on, in reliance on the ostensible safety of that system..."

Here is the further conclusion of the judge who obviously had no knowledge of the real world of industry and certainly none of primary and secondary protection:

> "... I think that a jury could reasonably find that a person such as the plaintiff, even because of his special knowledge, may be induced to rely on the apparent safety of the two-handed control mechanism, and therefore might place his hand in the machine..."[4]

The court knows the law, at least some of it, and some courts know less than others. Courts do not know the technology. Certainly, this court was not aware of the difference between secondary and primary protection. This decision shows a spectacular ignorance of the fundamental difference between a control circuit interlock (secondary protection) and a primary power disconnect switch.

That ignorance is not confined to the bench. Unfortunately, there is a similar, widespread ignorance among industrial workers of the difference between secondary and primary protection. [1, 6] This is why manufacturers refuse to put limit switches or interlocks to "backup" primary protection. The *presence* of the interlocks invites reliance on the interlock and *neglect of the primary power protection* (locking out the power disconnect switch).[20]

Many interlock suggestions at first seem quite novel, reasonable and worth using. Following is a simple example of an interlock with an appeal to safety. Consider an electric lawn-mower with the usual OFF-ON maintained-position switch on the handle. An operator might clean it without pulling the plug (disconnecting the lawnmower's electrical male plug from the electrical extension cord), and while he has the lawnmower with blades up, the switch might be inadvertently moved to ON with disastrous results.

A decision is made to backup the regular switch with a mercury tilt switch in series with it. That is, to mount a "tilt" mercury switch on the lawnmower, electrically connected in series with the OFF-ON switch so that if the lawnmower is turned upside down, the circuit will be broken.

Now when the OFF-ON switch has been turned off, turning the lawnmower over for cleaning will cause another "open" in the electrical circuit. Even if the user has failed to pull the plug, the danger of starting the mower by someone moving the OFF-ON switch to ON is minimized because the tilt switch is still open. Thus such a switch would be a valuable backup to the OFF-ON switch when the lawnmower is turned over to be cleaned - in theory.

This might seem to be a highly desirable feature on an electric lawnmower, but consider this example of how an interlock can be misused. How long would it take the average user to realize that to turn the motor off to clean the mower, all he has to do is simply turn the mower over by the handles? The tilt switch will automatically open the circuit and stop the motor. The user learns that he does not have to pull the plug or operate the OFF-ON switch to turn off the motor. He merely has to turn over the mower and begin to clean it.

The foreseeable accident occurs when he has done this and is cleaning the blade and discharge chute and forgets that he is now relying entirely on the tilt switch. When he finishes the cleaning, he grasps the mower with the discharge chute as a convenient handhold and rights it, and as he does so, the tilt switch closes again, the motor and blades start, and the scenario is complete as he loses three fingers. [17, 18]

The best solution is not the addition of a tilt switch, but training the user to PULL THE PLUG AND LET THE BLADE STOP. Even the OFF-ON switch is not adequate for protection when the user has his hands near the blades. He must rely on *primary protection* - he must PULL THE PLUG and completely disconnect the power source.

Let us anticipate some objections which might be raised by the technically skilled. Yes, the two-wire control could be replaced by a three-wire momentary relay circuit, and that supported by another level or two, but these "corrections" not only rapidly become impractical, but introduce other hazards. Each identification of a hazard gives rise to another suggestion of further interlocks, and resultant further hazards until the final solution falls under sheer complexity. [17, 18] Such a tilt switch would present a greater hazard than it prevents. It is the same story with many suggested uses of interlocks for "safety."

TYPES OF INTERLOCKS, BY FREQUENCY OF OPERATION

In considering whether or not to apply an interlock, the frequency of its application is an important consideration and can have a significant effect upon its reliability and hence upon its application. To distinguish among three broad classifications of interlock use, we identify interlocks as follows:

1. *QUIESCENT (PASSIVE) INTERLOCK:* One that may remain in the same state for long periods of time, possibly months or even years. Often involves disassembly or partial disassembly of interlocked unit to test the interlock. Example: Interlocked stationary guard.

Consider a stationary guard on a machine. Assume that the guard might remain in place for several years of machine operation. Here is an interlock that would get a *minimum* amount of "exercise." Over that period of time, any number of possibilities exist that might defeat the interlock. It could simply "freeze" from "old age" and fail to work when it should. It could be cannibalized "temporarily-permanently" by someone who realized that it would never be missed. If bypassed for this purpose, the condition might not be detected for years.

2. *MODICUM (ACTIVE) INTERLOCK:* One that is accessible for checking and actuation with minimum or no disassembly. Does not necessarily operate each machine cycle, but is designed to be actuated frequently.

Consider a guard that might be opened routinely during a shift to inspect the tooling. An interlock on such a guard would require regular inspection and presumably would be an item on the regular maintenance checklist. A guard of this kind designed for routine use would make the actuation of the interlock easy to check.

3. *CYCLING INTERLOCK:* One that changes state at least once during each regular operation of the machine cycle.

Finally there is the type of interlock, like the two-button hostage control with anti-tie-down features, in which the interlock is actuated at least once during each cycle. That is, the operator permits the machine to go through one cycle by pressing two pushbuttons simultaneously, thereby keeping his hands out of possible danger. But if he ties or wedges one button down, then the control will not start that cycle (anti-tie-down). The machine will not start until both pushbuttons are pressed again after both of them have been released.

It is possible with this kind of interlock to exercise it repeatedly and to check its operation automatically during the cycle. If it malfunctions, then it may be possible to have the circuit itself bring the automatic cycle to an end.

REGULAR VERIFICATION OF INTERLOCK INTEGRITY BASED ON TYPE

Consider the special problem of inspecting interlocks to be sure they are working correctly. The *cycling interlock* is certainly the one whose malfunction will be most quickly detected and most certainly repaired, because the machine cannot cycle if a cycling interlock malfunctions. Production stops until the interlock is fixed.

The *modicum (active) interlock* is one that might operate every day or every few days. Because it is ordinarily not difficult to check, good maintenance is facilitated. Not only is its actuation simple to test but usually there will not be a large number of such interlocks on a machine.

The situation is different with a *quiescent (passive) interlock.* As an example, consider a manufacturer whose machine has ten guards, well mounted and bolted to prevent unauthorized removal. The decision he faces is how to deal with ten quiescent (passive) interlocks.

When an interlock remains in place for long periods of time without operation - perhaps even for years - the probability increases that because of sheer lack of exercise it will stick in place. Its reliability diminishes. Condensation and/or breathing because of change of temperature and the aging and drying out of seals are some elements that will cause interlock failure. Quiescent or passive interlocks are extremely susceptible to this problem and to shorting contaminants.

To check the reliability of the interlock, it must be physically moved or operated as if the guard were being removed. This, of course, means that the guard must be removed. The better the installation of the guards, the more difficult the checking of the interlock becomes. The more guards, the more burdensome the task becomes.

If the guards are well mounted and bolted, checking the interlocks will entail a major mechanical task, that of removing each guard either wholly or partially, to verify the correct operation of the interlocks.

A conscientious employer who enforces a policy of keeping guards in place has already addressed the problem of protection. A less conscientious employer who does not, is not likely to enforce the necessary regular interlock inspection that requires so much work and time. So the conscientious employer really does not need the interlocks. The less conscientious employer who might otherwise benefit from them would probably not maintain them in working order.

Thus the use of a quiescent interlock is always either a redundant or useless procedure or a questionable one tending to high failure. Without regular verification of the correct functioning of an interlock, an interlock is dangerous in not providing the protection its presence seems to offer. *Quiescent (passive) interlocks are of dubious value and are always suspect.*

SOME DESIGN CONSIDERATIONS IN CHOOSING AN INTERLOCK

Below is a list of *some* of the factors that should be considered in selecting an interlock switch:

a. Frequency of operation: quiescent, modicum or cycling.
b. Risk involved: serious, grave, ultimate.
c. Capable of being tested without using radical measures.
d. The level of installation: poor, good, excellent - that can be reasonably expected from the usual installation.
e. Environment: conductive dust, liquids, adhesives, condensation; oil, dust, heat, cold; open flame; sparks; metallic particulates; presence of vibration, shock or impact.
f. Proximity switches, reed relay contacts, vibration, defeater devices; substitute (false) actuators; shielding; possibility of false signals.
g. Mechanical switches; positive mode actuation; negative mode actuation; teasing of contacts; snap action versus slow-make-slow-break mechanisms.
h. Use of redundancy; serial failure from single fault; welding effect of short circuit.
i. Length of relay coil wire runs and capacitance. Burden and effect of capacitance in defeating dropout; inductive nature of the interlocking circuit.

The foregoing abbreviated list merely hints at the design considerations that must be reviewed in the choice of electrical interlocks. Although the designer after many years of experience does not usually go through such an explicit review of considerations, his choices always reflect such review.

MECHANICS OF INTERLOCK DEFEAT (MOSTLY ELECTRICAL)

Some of the ways in which electrical interlocks can or may be defeated are the following:

1. Interlock shorted or grounded.
   a. In the switch itself
   b. In the wiring to the switch
   c. In the enclosure of the control cabinet
   d. By capacitance. Possible with long runs and light burden. Can be marginal and erratic.
2. Interlock falsely actuated.
   a. Mechanical actuator stuck, bent or broken
   b. Internal mechanism stuck, bent or broken
   c. Substituted magnet or metal mass
   d. Actuator tied, wedged or otherwise restrained
   e. Foreign field from magnetically held tool
   f. Shock, impact or vibration
   g. Stray magnetic fields on proximity device.
3. Active by-passing.
   a. Trapped interlock key released by duplicate key
   b. Trapped interlock key release by gimmick
   c. Electrical troubleshooting by-passing interlock
   d. Mechanical (manual) actuation of magnetic device (e.g., starter or relay operated manually or proximity switch by magnet or steel substitute)
   e. Manual overrides on pneumatic or hydraulic valves
   f. Starter (Contactor wedged closed - Abuse !) Drive started and stopped with disconnect switch.

REASONS FOR DEFEAT OR FAILURE OF INTERLOCKS

1. Removal for repair, maintenance or inspection
2. Removal to check, test or replace
3. Removal of guard or interlocked member to allow increased production or convenience of access
4. Interlock device broken or requiring repair with no replacement units available. Becomes a "temporary-permanent" condition
5. Permanent removal or defeat of interlock to avoid trouble or expense of repairing it
6. Contamination of electrical interlock by environmental conductive dust
7. Contamination of electrical interlock by conductive liquids
8. Vibration teasing contacts - causing them to weld
9. Deterioration of interlock seals, causing sticking
10. Short circuiting caused by:
    a. Mechanical crushing of conduit, fittings
    b. Abrading of insulation on wires
    c. Deterioration of insulation by overload currents
    d. Deterioration of insulation from external heat

REDUNDANCY

The standard answer to objections based on the possibility of failure in an interlock is usually, "Then put in two of them and if one fails, the other will still work." This assumes that the causes of failure are independent and the probability of failure in the first place is very small for each.

If the first interlock fails in January, the system from then on has no redundancy and when the second interlock fails in June, the presence of the two interlocks invites reliance on them. But there is no protection!

"Then add a third interlock to back up the second one." That merely moves the system one more step. Suppose the second fails in June, leaving the system this time with a reduction in redundancy. Again when the third interlock fails, perhaps in December, there is no redundancy. The physical presence of three interlocks even more strongly invites reliance on them. But again there is no redundancy and protection.

"Shall we then add a fourth interlock to back up the third one?" And when should this process of adding redundant interlocks come to a halt? [17](First order...Second order...Third order... n^{th} order Safety System).

If we calculate the mean time to failure for each switch in an adverse environment, time for all of them begins to run from the same instant. It does not start for the second interlock from the demise of the first interlock. Rather, the failure of the first interlock is a signal that we may soon look for others to be on the verge of failing. From an adverse environment and particularly a quiescent application, a life expectancy to failure could easily be as little as a year, or even on rare occasions as soon as the first hour. Relying on redundancy to overcome that is simple minded.

Consider this analogy. In the population at large, life expectancy is perhaps fifty to sixty times as great as the correctly functioning life of an interlock. If you need someone to blow a bugle alarm one hundred and fifty years from now, it does not really matter whether you name one or fifty individuals to the task. The alarm signal will never be blown. It is the same with the ability of an interlock to alarm against a hazard; you cannot guarantee it by multiplying interlocks. Time, along with corrosion, deterioration, and human neglect alone will finally defeat your purpose.

Add to this another consideration. Redundant electrical interlocks are customarily wired in series so that if any one of them is actuated and opens, the circuit will be broken. Thus, if only one out of ten operates correctly, it will open the circuit. BUT there are two possibilities - neither of them uncommon - in which all of them can fail simultaneously!

The first possibility is that a short occurs, *by-passing the whole string of interlocks.* This often occurs when an electrician jumps out part of the circuit during electrical testing.

The second possibility is that a direct short or ground occurs and - even when a control circuit fuse blows - the *transient current welds the contacts on all of the interlocks*, leaving them firmly fixed in the closed position and showing nothing to suggest the damage to any operator other than a skilled electrician. In our analogy of selecting future buglers, this would be equivalent to a plague loosed on the population.

A combination of two interlocks of different nature is a slight improvement in redundancy. The combination of a mechanical interlock with an electrical interlock or with a fluid power interlock can be more effective than two electrical interlocks. It is not, however, an unmixed advantage, for both the mechanical and the fluid power interlocks have their own shortcomings which have to be considered.

INTERLOCK LIMIT SWITCH ACTUATION - POSITIVE AND NEGATIVE MODE

The *manner* in which the limit switch interlock is actuated poses another question that must be considered carefully. Assume we are considering the application of a limit switch interlock to a movable guard, allowing the operator routinely to clean or spray a pattern within the guarded area. Primary protection is not possible because of the frequency of entrance and thus it is only possible to provide secondary protection.

Under these assumptions, it is now appropriate to consider whatever measures might increase the protection afforded by the entry guard and its interlock switch.

The object, of course, is to be sure that the entry guard is closed while the machine is moving. This can be done in either of two ways of applying the interlock:

1. *Negative mode* (Figure G-1LS): We can sense that the guard is completely closed and use that information to PERMIT the machine to run or
2. *Positive mode* (Figure H-2LS): We can sense that the guard is NOT completely closed and use that information to PREVENT the machine from running.

Note that in Figure G, the interlock contacts of 1LS (1st Limit Switch) are shown as connected in series with a STOP pushbutton - so that the interlock contacts opening have the same effect as pressing the STOP pushbutton. Simlarly, if you were using the interlock contacts of 2LS (2nd Limit Switch), it would be connected in series with the STOP pushbutton contacts with the same effect.

In Figure H, *both* interlock contacts are connected in series with the STOP pushbutton so that there is not just a positive mode OR a negative mode interlock, but both.

What is involved is the manner in which the interlock is *actuated*? In the negative mode, the interlock (1LS) is actuated when the guard is completely closed. In the positive mode, the interlock (2LS) is actuated as soon as the guard is *not* completely closed. It remains actuated no matter how far the guard is opened.

These two modes are shown in Figures G and H. Figure G shows an access sliding door in the fully closed position. Note that interlock 1LS is being actuated and its contacts are closed because of the actuation against the internal spring. In Figure H, 1LS is no longer actuated, and the switch spring has opened the contacts. This is the *negative mode.*

In Figure G, note that the contacts of interlocks 2LS are closed because of the action of the internal spring. But as the sliding door begins to open, the cam action against the interlock wheel *forces* the wheel upward, opening the contacts and compressing the interlock spring. This is the *positive mode* of operation.

There are two general possibilities of failure involved with *actuation* of the interlock:

1. Failure of the interlock to *release* after being de-actuated, and
2. Failure of the interlock to *respond* to actuation.

The positive mode addresses primarily the first possibility. A difference in reliability is the crux of the matter. When you want to be sure some action will occur, you rely on *actuation* of a switch, not on *release* of the switch. Actuation of a device is more reliable than restoration of the device by gravity or springs when the actuation ceases.

In the *negative mode (interlock 1LS)*, reliance is placed on the interlock switch springs to open the interlock contact when the guard is opened. See Figure G, interlock 1LS. If the switch fails, then the machine can operate and the malfunction is critical because *there is no notification* that the interlock has failed.

In the *positive mode (interlock 2LS)*, an interlock switch is used that has the contacts directly linked to its arm. When the guard is opened, the movement of opening the guard directly *forces* the contacts open. See Figure H, interlock 2LS. Only when the guard is completely closed is the actuation removed. If when the guard is closed, the interlock contacts fail to close, then the machine will not run. The malfunction therefore causes what is called a fail-safe condition. Malfunction simulates the guard-open condition - i.e., hazardous.

There are, however, two general possibilities of failure involved with *actuation* of the interlock: failure of the interlock to release after being de-actuated, and failure of the interlock to respond to actuation.

Comparing *failure to release after de-actuation* in these two modes, it can be seen that malfunction of the *negative mode* interlock permits the machine to be started with the guard open - a dangerous condition.

Malfunction of a *positive mode* interlock prevents the machine from being started with the guard closed - a mere inconvenience to production that will quickly be remedied by maintenance.

Now that we have discussed the first general possibility of interlock failure - failure to return to its de-actuated state, we must consider the second general possibility of failure of the interlock - failure to respond to the attempted actuation. The actuating mechanism simply fails to actuate the interlock.

In this situation, the results from malfunction are exactly reversed. In the *negative mode*, the interlock (1LS) not being actuated is inconvenient to production because the machine fails to run. It will be fixed or by-passed by maintenance. In the *positive mode*, the interlock (2LS) *not* being actuated fails to prevent the machine from starting when the guard is open - a dangerous condition.

The actuation mechanism in positive mode is always more complicated or extended than that in negative mode. Greater design consideration and more frequent inspection are required to prevent wear and misalignment from frustrating the action intended. Briefly, negative mode actuation is simpler than positive mode actuation.

Here a special kind of redundancy is possible. Rather than merely using two interlocks of the same kind, it is preferable to use a combination of two interlocks - one in the negative mode and one in the positive mode. Figure H shows circuit 1 in series with circuit 2.

Whether this would be superior to the enforcement of a policy requiring that the interlock be functionally tested each day or at least each shift is arguable.

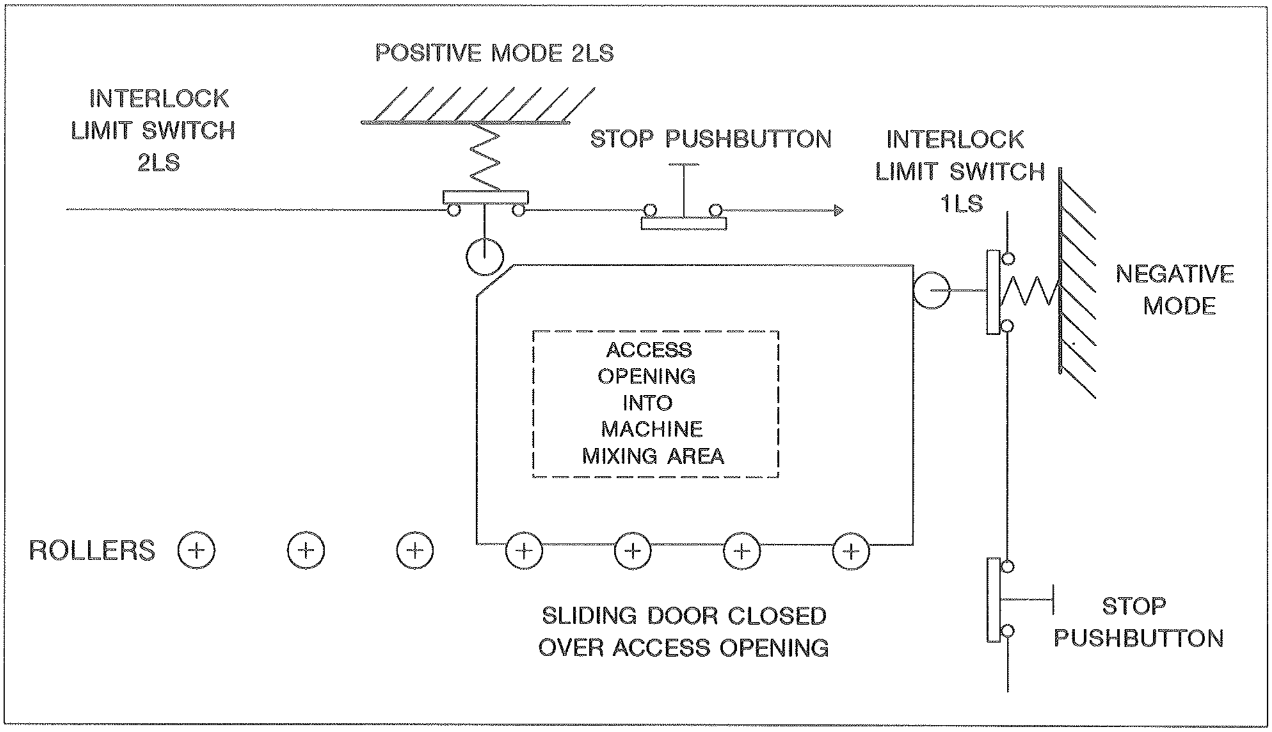


Figure G - Negative mode - interlock limit switch 1LS actuated. Access sliding door in fully closed position.[15]

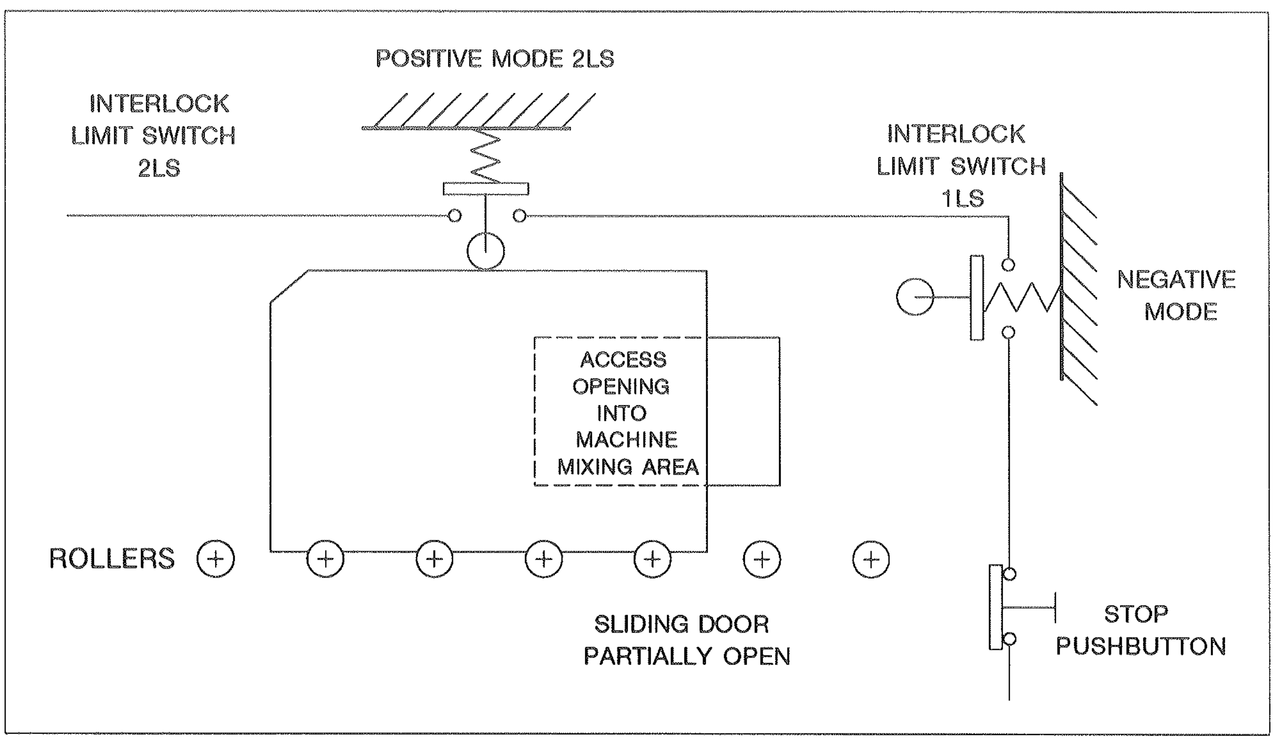


Figure H - Positive mode - interlock limit switch 2LS actuated. Access sliding door in partially open position (Interlock switches wired in series).[15]

As always, the redundancy could be reinforced by adding a pilot circuit that would cause a pilot light to light up if both limit switches had functioned correctly with the guard open. As always, the decision for reinforcement would depend on the individual case.

But suppose during maintenance, someone removed the access door completely. Since the door now cannot actuate the positive mode limit switch, it remains in a released position signalling that the door is closed. The motor can be started or run despite the fact that the access door is wide open. Furthermore, physical adjustment of this kind of interlock is critical and subject to wear and misadjustment.

Consider further the use of the so-called slow-make-slow-break switch. Unless the limit switch arm which is forced to operate by the door opening, really forces the contact to operate, most of the advantage of this type of switch disappears. It is not enough to force the switch arm to move, but the switch itself must perforce open the contacts.

Because it is slow-make-slow-break, its ability to open a current carrying circuit is limited or else it requires a large movement of the switch arm. The recommended solution is usually that two switches be used - one in negative mode and one in positive mode. In some instances, this may offset slightly the negative aspects of redundancy. This use has little advantage for a quiescent interlock.

In summary, *positive mode* actuation is mechanically much more difficult and subject to more problems of wear and holding alignment. It therefore requires more maintenance and inspection of the mechanical parts. Without detailing these objections, consider maintenance in which for some reason the *guard were to be completely removed*. Clearly the actuation is removed and the machine can be started. A very dangerous condition.

Again, there is no universally accepted solution to this decision to use positive or negative modes.

PROBABILITY OF FAILED INTERLOCK BEING REPAIRED OR REPLACED

In order to discuss the probability of a failed interlock being repaired, look at all the possible states of an interlock. Assume that it is a limit switch on an access door. Assume further that the interlock is intended to prevent the machine from running if the access door is open.

Our example will consider a machine with large mixing wheels, an access door, and a full enclosure. The entire enclosure not only functions as a dust enclosure but also as a complete guard over the moving parts.

An interlock is placed so that it will signal when the door is fully closed. Its electrical contacts are connected in the coil circuit of the motor starter (controller). The intent is that if the door is not fully closed, it will not be possible to start or run the machine.

Of course, once a man has climbed inside to clean the interior, he might for whatever reason close the door behind himself or the door might accidentally be closed by his light cord or something outside falling against the door. *This simple foreseeable event would defeat the intended protection completely*. But ignoring that contingency for the moment, the following four other possibilities exist. See Figure I.

If the interlock fails so that when the door is open (hazard) the interlock is still in the permissive mode; clearly it is dangerous because it does not give the protection its presence promises. See Case 2 of the Figure I.

It is convenient for discussion to designate this type of failure as a permissive malfunction. That is, it is dangerous because it has failed, although the interlock is still present, looks all right, but affords no protection to anyone relying on its presence (Case 2, Figure I).

If the interlock fails so that whether the door is closed (hazard guarded) or open (hazard present), the interlock is in the "hazard," "alarm," or "prevent" mode. A convenient reference is a preventive malfunction. See Case 4 of Figure I.

In deciding whether or not to use an interlock, one of the basic considerations is whether or not such an interlock when it has malfunctioned will be repaired or replaced. Clearly, if the probability is high that it will not be repaired or replaced, then common sense would dictate that it would not be used.

If an interlock has a permissive failure (Case 2), this gives no indication that it has failed, and the probability is very low that it will be replaced or repaired. If an interlock will not be fixed, it would be better never to install it in the first place. Thus the consideration of whether an interlock will be fixed if it malfunctions bears directly on the initial decision of whether there should be an interlock or not.

The probability of a failed interlock being repaired and restored to service depends largely upon the nature of the interlock - quiescent, modicum, or cycling - and the nature of the interlock failure.

Cycling interlock: If it is a cycling interlock with a checking characteristic, its repair is very probable, because unless it operates normally during the cycle, the cycle will not be completed. It is true that in some instances, a temporary expedient is to substitute a pushbutton for the operator's use in simulating the operation of the interlock. The added burden on production and on the operator usually becomes such a hardship that the maintenance department is soon pressured into repairing it.

Modicum interlock: Unless there is a self-checking feature to a modicum interlock, when it fails to danger, there is no inconvenience that occurs. There is simply an appearance of protection, which in fact does not exist. An interlock that fails-to-the-alarm mode (Case 4) will of course get immediate attention because the machine will not run until it is fixed, but the example here is a failed-to-danger interlock (Case 2).

Suppose that there is an interlocked gate which stops the machine if opened, and that the interlocked switch has a permissive malfunction (Case 2) so that opening the gate does not stop the machine. Depending upon the hazard protected against, probably a minimum requirement for testing this type of interlock would be once a day or every shift.

What is the "self-checking" feature referred to for a modicum interlock? This testing could be incorporated in the starting circuit by initiating a preliminary signal by opening the gate, followed by a completion signal to close it. Thus starting the machine would require first opening the gate followed by closing the gate. Without a self-checking

Figure I - Permissive and Preventive Malfunctions

Example: Machine with heavy driven wheels and paddles enclosed by a dusthood. An access door is provided in the dusthood. An interlock is provided which is intended to prevent machine startup unless the door is closed. Compare Figure G, Negative Mode Interlock 1LS. Shaded areas represent malfunction conditions.

	Condition of the Interlocked Door	State or Condition of the Interlock	Convenient Name for Interlock State
Case 1	Door CLOSED Hazard enclosed.	Interlock circuit permits machine to start or run.	PERMISSIVE
Case 2	Malfunction makes interlock act as if door were closed (safe), whether door is open or closed. Example: Interlock sticks and spring fails to open it.	MALFUNCTION of the interlock may cause it to remain in this "safe" state even when door is open allowing someone to enter.	PERMISSIVE MALFUNCTION (Failed in permissive state) Failure to danger.
Case 3	Door OPEN. Hazard to personnel exists if machine starts or runs.	Interlock circuit is intended to stop machine from starting or running. IT MIGHT NOT! At best it is only secondary protection.	PREVENTIVE Intended to prevent machine running or starting, BUT MIGHT NOT!
Case 4	THIS MALFUNCTION occurs when interlock fails to be actuated. Interlock fails in "door-open" position i.e. Fails to close when door is closed.	MALFUNCTION of the interlock may cause it to remain in this "door open" state even when door is closed ("safe" state). MALFUNCTION must be repaired before machine can run normally - but the danger exists that someone may simply bypass the interlock instead of repairing it.	PREVENTIVE MALFUNCTION (Failed in preventive state) Might prevent machine from running.

feature, a modicum interlock failed to danger does not really force maintenance to be done.

Quiescent interlock: Like a modicum interlock failed-to-the-alarm mode, this type of interlock will *not* be fixed - or it will be bypassed. Remember there is nothing that requires repair of a failed-to-danger interlock. If it fails in this position, it does not stop the machine and in fact provides no inconvenience. Unless maintenance is alert and discovers this failure, the malfunction will be ignored. And, if discovered, there is rarely any incentive to fix it. Thus, for this reason alone, logic would be against using quiescent interlocks. They invite reliance but actually provide no protection.

It is like an empty fire-extinguisher on the wall - it looks good but nobody really has to fill it if he is busy elsewhere. While appearing to give protection, it really provides none. It is probably better not to provide a fire extinguisher if it can reasonably be anticipated that it will not be serviced. Similar logic applies to an interlock.

Two steps in a failed interlock: First, the malfunction must be discovered. Second, the malfunction must be fixed. In the cycling interlock, certainly the malfunction will be discovered and it is probable that it will be fixed - otherwise the machine will not run.

In the modicum interlock with good maintenance, the failure-to-danger malfunction has a chance of being discovered. An awareness of the hazard guarded against will operate to have the malfunction fixed (Case 2). But ordinarily with a modicum interlock failed to danger, note that there is no compelling reason either to discover the malfunction or to fix it after it is discovered, as far as the operation of the machine is concerned - unless there is a checking feature.

It may even be the conservative design by a good engineer that is responsible for not fixing a malfunctioning interlock. For instance, the designer, in order to meet what he regards as an adverse condition, may have specified a switch of an ultra-heavy-duty kind. Availability of this special switch, however, may limit replacement.

Faced with the difficulty of procuring a replacement switch, the field maintenance man may defeat the interlock until he can get the replacement. This may become another "temporary-permanent" condition. Or he may substitute another, more available but inferior, interlock. The possibility therefore may be a dangerous interim in which the interlock remains defeated or in which a switch more susceptible to failure is substituted.

Thus the design engineer who has worked out a very conservative interlock system, may have built in a procurement problem that acts to defeat prompt repair or replacement of the malfunctioning interlock. The more unique his solution, the more probable this possibility. The closer he stays to standard, readily available, off-the-shelf items, the more he avoids this problem. [1]

CONCLUSIONS ABOUT INTERLOCKS

There is no way a manufacturer who builds machines with interlocks and guards can enforce either their use or their maintenance by the employer who buys and uses the machine. The manufacturer has sold a machine and although he can suggest and recommend, he has no way to control what happens to that machine.

Most machine manufacturers are pessimistic as to ordinary maintenance on their equipment, even more pessimistic as to the maintenance of guards and interlocks in hostile environments. Through their field engineers and service personnel, they have been exposed to watching unwarranted reliance on interlocks instead of on primary protection. Many of them, in cases of guards, have consistently refused to provide interlocks, particularly in cases of ultimate or grave risk.

Their philosophy is very simple. Force personnel to rely only on primary protection by deliberately keeping secondary protection devices off their machines.

In the case, for instance, of a single motor drive machine, manufacturers have consistently insisted that locking out the primary power is the only reliable way of protecting personnel entering the machine - if the man entering the machine has the *only key in his possession.* They have now been supported by the OSHA Lockout/Tagout Directive which calls for this exact action. [3]

In such a case, the addition of an interlock to the machine would not only contribute to violations of this directive by offering an easier (but false) alternative, but would invite reliance instead on a device that does not offer the same scope of protection. That is, the addition of an interlock to the machine would tempt less informed personnel to rely on the interlock instead of using the less easy Zero Mechanical State (ZMS) procedure or the equivalent OSHA lockout/tagout procedure. Probably a conscientious, knowledgeable manufacturer would regard such a "backup" interlock as an increase of the hazard.

Lastly, to all who are not conversant with the various types of failure of interlocks and to all who might be tempted to add an interlock, thinking that certainly safety would be served, let us repeat this statement:

> *The choice of the kind of interlock to use in any particular case is a sophisticated engineering decision. Whether an interlock should be used at all, is an even more important decision. The choice is affected by whether or not the application permits use of primary protection. If so, the decisionmaker must consider whether the interlock by its presence significantly invites neglect of primary protection procedures.*

ABOUT THE AUTHOR

Frank B. Hall is an electrical engineer, attorney, author and engineering consultant, specializing in corporate product liability programs and in technical strategy for litigation relating to lockout/interlock issues involving heavy machinery. Mr. Hall's career spanned three decades, as an engineer, patent attorney and corporate counsel. In 1979, he received the American Foundrymen's Society Award for Scientific Merit for coauthorship of the Safety Concept of Zero Mechanical State.

Mr. Hall earned his Bachelor of Science degree in Electrical Engineering from the Illinois Institute of Technology and his Juris Doctor from DePaul University. He was admitted to the Illinois Bar in 1956 and admitted to practice in the U.S. Patent and Trademark Office in 1972. He taught in the Army Signal Corps Civilian Schools before military service and at the Industrial Training Institute after military service.

His engineering experience was primarily in the field of electrical/fluid controls for heavy automated machinery. He worked for Argonne National Laboratory in the Nuclear Reactor and the Particle Accelerator Divisions. His industrial and legal experience were largely with Beardsley Piper Division of the Pettibone Corporation, where he was involved in patent management and in product liability.

Mr. Hall is a senior member of the Institute for Electrical and Electronic Engineers, a member of the Chicago Bar Association, the Intellectual Property Law Association of Chicago, the National Society of Professional Engineers, the Sons of the American Revolution, and the Society of American Magicians. Mr. Hall has served on various committees, among them: Electrical Safety at the Zero Gradient Synchrontron and the AFS ANSI 10-D Committee on Foundry Safety Standard Z241.1. He was also a consulting editor of *Foundry Management and Technology*.

He is the author of *The Dictionary of Dismayed Defendants*, many professional papers and is listed in Who's Who in the Midwest.

REFERENCES

1. "American National Standard Safety Requirements for Sand Preparation, Molding and Coremaking in the Sand Foundry Industry," *ANSI Z241.1-1975*. Sponsored by the American Foundrymen's Society. Des Plaines, IL and approved by American National Standards Institute, New York, in 1975. Note: There are currently two additional ANSI standards, *ANSI Z241.2* (covering melting and pouring of metal) and *ANSI Z241.3* (covering cleaning and finishing of castings). The latest issue date for all three standards is 1989, and each of them incorporates the official definition of Zero Mechanical State (ZMS).

2. Appleton, Arthur L. and Robert J. Pastorel, "Mechanical Safety Interlock for Covers of Explosion-Proof Electrical Housing," *U.S. 3,743,800*, assigned to Appleton Electrical Company, Chicago, IL, patented July 3, 1973.

3. "The Control of Hazardous Energy Source (Lockout/Tagout); Final Rule," *29 CFR 1910.147*. Washington, D.C., U.S. Dept. of Labor, Occupational Safety and Health Administration, effective Oct. 31, 1989. *Federal Register* v. 54 #169 (Sept. 1, 1989): 36644-36696.

4. Frumer, Louis R. and Melvin I. Friedman, Eds. *Products Liability*. New York, Matthew Bender, 1960. Sec 8.05 (1)A. 186.10 (1).

5. Hall, Frank B. and Robert D. Mitchell, "Zero Mechanical State - A New Safety Concept beyond Power Off State," *Modern Castings* v. 63 #3 (March 1973): 48.

6. Hall, Frank B., "Zero Mechanical State - Historical Background of Concept," *National Safety Congress Transactions, Industrial Safety Session* v. 12 (1976): 55-61.

7. Hall, Frank B., "Health and Safety Management Section: Primary and Secondary Protection, Part 1: Working with Standards," *Modern Castings* v. 75 #5 (May 1985): 40.

8. Hall, Frank B., "Health and Safety Management Section: Primary and Secondary Protection, Part 2: Working with Secondary Protection," *Modern Castings* v. 75 #6 (June 1985): 64-5.

9. Hall, Frank B., "Primary and Secondary Protection (ZMS, ZES, Zero States, and Interlocking)," Paper presented at the *68th National Safety Congress and Expostion, Metals Section, Session 79* (Oct. 10, 1980): 28-page typescript.

10. Johnson, Earl A., "Zero Mechanical State Procedure Development," *National Safety Congress Transactions, Industrial Safety Session* v. 12 (1976): 70-74.

11. Mitchell, Robert D., "Application of ZMS and Other Safety Concepts," *National Safety Congress Transactions, Industrial Safety Session* v. 12 (1976): 62-69.

12. Pastorel, Robert J., "Defeater for Mechanical Safety Interlock for Covers of Explosion-Proof Electrical Housing," *U.S. 4,031,340*, assigned to Appleton Electrical Company, Chicago, IL, patented June 21, 1977.

13. Price, Charles, "ZES - Zero Energy State," *National Safety News* v. 12 #6 (1975): 56-57.

14. Price, Charles, "Commentary on Papers at National Safety Congress on ZMS," *National Safety Congress Transactions, Industrial Safety Session* v. 12 (1976): 75-76.

15. "Safety of Machinery. British Standard Code of Practice." BS5304: 1988. London, British Standards Institution, 1988, page 89.

TRIODYNE SAFETY BRIEFS RELEVANT TO INTERLOCKING

Since the 1980 presentation of this paper, Triodyne has issued some important and original papers that bear directly on the subject of interlocking, as it relates to system safeguarding. They are listed here because they reinforce and are reinforced by the discussion in this paper.

16. Barnett, Ralph L. and Peter Barroso, Jr., "On Classification of Safeguard Devices (Part I)," *Triodyne Safety Brief* v. 1 #1 (April 1981).

17. Barnett, Ralph L. and Peter Barroso, Jr., "On Classification of Safeguard Devices (Part II)," *Triodyne Safety Brief* v. 1 #2 (September 1981).

18. Barnett, Ralph L. and Beth A. Hamilton, "Philosophical Aspects of Dangerous Safety Systems," *Triodyne Safety Brief* v. 1 #4 (December 1982).

19. Barnett, Ralph L., "On Safety Codes and Standards," *Triodyne Safety Brief* v. 2 #1 (July 1983).

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

21. Barnett, Ralph L. Gene D. Litwin and Peter Barroso, Jr., "Dependency Hypothesis (Part II)," *Triodyne Safety Brief* v. 3 #1 (December 1984).

22. Barnett, Ralph L. and Dennis Brickman, "Safety Hierarchy," *Triodyne Safety Brief* v. 3 #2 (June 1985).

TRIODYNE SAFETY PUBLICATIONS

The following publications are available. When ordering please send name of the requested material and where the materials should be sent. Direct your requests to:
Triodyne Safety Publications; 5950 West Touhy Avenue, Niles, IL 60714-4610. (708) 677-4730.

Triodyne Safety Briefs

Volume 1 No. 1
On Classification Of Safeguard Devices (Part I): Intrinsic Classification of Safeguarding Systems
by Ralph L. Barnett and Peter Barroso Jr.

Volume 1 No. 2
On Classification of Safeguard Devices (Part II): Functional Hierarchy of Safeguarding Systems
by Ralph L. Barnett and Peter Barroso Jr.

Volume 1 No. 3
Zero Obstruction Repair Overpass

Volume 1 No. 4
Philosophical Aspects of Dangerous Safety Systems
by Ralph L. Barnett and Beth A. Hamilton

Volume 2 No. 1
On Safety Codes and Standards
by Ralph L. Barnett

Volume 2 No. 2
Safety and Product Liability Considerations in Farm Machinery Equipment
Only Photocopies Available

Volume 2 No.3
The Dependency Hypothesis (Part I)
by Ralph L. Barnett, Gene Litwin and Peter Barroso Jr.

Volume 2 No. 4
On the Safety of Motorcycle Side Stands
by Dror Kopernik

Drill Press Guards
by William G. Switalski and Ralph L. Barnett

Volume 3 No. 1
The Dependency Hypothesis (Part II) - Expected Use
by Ralph L. Barnett, Gene D. Litwin and Peter Barroso Jr.

Volume 3 No. 2
Safety Hierarchy
by Ralph L. Barnett and Dennis Brickman

Volume 3 No. 3
Trailer Hitches & Towbars
by William G. Switalski and Ralph L. Barnett

Volume 3 No. 4
The Meat Grinder Safety Throat
by Ralph L. Barnett, Gene Litwin, and Gary M. Hutter

Volume 4 No. 1
Mechanical Power Press Safety Bibliography
by Beth A. Hamilton, Joyce E. Courtois and Cheryl Hansen

Volume 4 No. 2
On Rubber Augers - Failure Modes and Effects
by Dennis Brickman and Ralph L. Barnett

Volume 4 No. 2
On Rubber Augers - Failure Modes and Effects
by Dennis Brickman and Ralph L. Barnett

Volume 4 No. 3
Mandatory Seat-Belt Usage Laws: Exemptions to the Rule
by Gary M. Hutter and Cheryl A. Hansen

Volume 4 No. 4
A Proposed National Strategy for the Prevention of Severe Occupational Traumatic Injuries

Volume 5 No. 1
Principles of Human Safety
by Ralph L. Barnett and William G. Switalski

Volume 5 No. 2
Deadman Controls on Lawn Mowers and Snowblowers
by Ralph L. Barnett and Dennis Brickman

Volume 5 No. 3 Medical Series
Reliability and Safety of Medical Devices: Introduction
by James R. Wingfield

Volume 5 No. 4 Medical Series
Status of Standards of Practice in Pharmacy
by James T. O'Donnell

Volume 6 No. 1
The Changing World of Products Liability Law
by Kenneth W. Clarkson and Francisco O. Loriga

Volume 6 No. 2 Medical Series
Ergonomic Studies of Grip Strength - Literature Review
by Dennis B. Brickman

Volume 6 No. 3 Metallurgical Series
Part 1: Introduction to Fracture Mechanics
by E. J. Ripling

Volume 6 No. 4
Photographic Documentation and Analysis in Vehicle Accident Reconstruction
by Dror Kopernik and Crispin Hales

Volume 7 No. 1 Environmental Series
Airborne Contaminants in the Machine Tool Industry
by Gary M. Hutter

Volume 7 No. 2 Fire Series
Fire and Explosion Investigations - A Historical and Hysterical Perspective
by John A. Campbell and Kim R. Mniszewski

Volume 7 No. 3
Safety Interlocks - The Dark Side
by Frank B. Hall

Power Punch Press Safety Package $20.00
Power Press Brake Safety Package $10.00

This package contains a series of safety posters, each as large as 30" X 40", in a reduced 8-1/2" X 11" format. The posters depict classic safety devices for the power punch press, or press brake, the areas where each is applicable, and the circumstances where it is unsafe.

Safety Registry: 1000
(Includes updated $2.00 supplement) $7.00

Access to the Triodyne $3,000,000 safety literature data base, representing almost two decades of intensive effort by engineers, scientists, and information scientists. It is comprised of over a thousand advanced bibliographies containing codes, standards, regulations, trade, and technical literature on topics ranging from aerial baskets through woodworking machinery.

Commercial Vehicle Preventable Accident Manual: A Guide to Countermeasures $15.00
by S.C. Uzgiris, Michael A. Dilich, and Crispin Hales

Compiled for the U.S. Department of Transportation , Federal Highway Administration, Office of Motor Carriers, this manual is a key element in the FHWA Carrier Accident Prevention and Evaluation Program (CAPE). It is the result of a U.S. DOT investigation into the primary causes of commercial vehicle accidents and the development of countermeasures which could be used to prevent them.

A Table of Accident Situations and Countermeasures summarizes twenty-eight accident situations, with corresponding listings of potential causes and countermeasures. Accident Analysis Work Sheets are provided for all the twenty-eight accident situations, to help identify potential causes under specific circumstances. In another section of the Manual, each Countermeasure is assigned an Objective, a Description, Questions for Management, Maintenance Checks, Driving Tips and References, including applicable FMVSS Safety Regulations

Safety specialists and managers for commercial fleets, maintenance personnel, bus and truck drivers, and those involved in litigation relating to commercial vehicles will find this Manual a MUST tool for evaluating safety performance. The Manual focuses on improved safety management, preventive maintenance and defensive driving and provides safety tips for specific areas of responsibility. No other single sourcebook on commercial vehicles treats these subjects in such a concise and understandable way.

Carpal Tunnel and Other Compression Syndromes Bibliographic Database

PC and Macintosh Editions $60.00
by Merdith L. Hamilton

Departing for the first time from hardcopy format,Triodyne is offering a comprehensive bibliographic database and accompanying search software which allows users to search the database on a PC. Users can search by authors, keywords in article and journal titles, either displaying search results on the screen or by printing them out in text or database format or by merging them with other files. If printed out in hard-copy, the database is about 800 pages long. A Triodyne Support Disk is available by telephone to provide user support as needed.

Carpal tunnel and compression syndromes are reaching epidemic levels for occupational injuries. The world-wide body of literature on this subject is primarily in English or has English abstracts. All types of documents are included, from scholarly research reports to those written for the general public. The database includes over 6,000 citations, covering the scientific literature from the earliest 17th Century to reports indexed as of June 1, 1991. The primary disciplines represented are Medicine, Human Factors and Biomechanical Engineering.

The medical literature covers most compression-entrapment syndromes, such as DeQuervain's Disease, Colles fractures, trigger finger, Raynaud's Phenomenon (or white finger) and vibration syndrome. Literature on identification and control of CTS concerns diagnostic and evaluation techniques, exercise programs, drug therapies, nutrition, conservative management and surgical techniques.

The Human Factors studies show the impact on CTS of such work environmental features as work station and equipment design, manual and repetitive tasks, postural discomfort, hand positions and dominance, and work methods.

The Biomechanical Engineering lierature includes force analysis, grip measurement and loss, human strength, maximum weights and work loads in manual handling tasks, muscular strength, power grip, skin surface measurements, and prehensile movements.

A smaller portion of the citations is devoted to worker's compensation laws, pre-employment testing, and liability issues.

SAFETY BRIEF

Triodyne Inc.
Consulting Engineers and Scientists
5950 West Touhy Avenue   Niles, IL 60714-4610   (708) 677-4730
FAX: (708) 647-2047

Editor: Beth A. Hamilton
Illustrated and produced by Triodyne Graphics Group.