"a configured logic system acting independently to alert operating personnel or shuts down the plant to safeguard against control system failure . . ."

Alarm and Safety Shutdown Interlock System: Balance Between Plant Production and Plant Protection

by

Remegio R. Lastrollo*

"ASSIS" is a configured logic system acting independently to alert operating personnel or shuts down the plant to safeguard against control system failure, process out-of-limit conditions, operator's error, and other situations that can result in human and/or economic catastrophe. The system must provide the necessary level of safety and the equally necessary assurance that nuisance interruptions of the process do not occur. Hence, maintaining the critical balance between continuous plant operation and dedicated on-going plant protection.

The "ASSIS" is the central collection point of a persistent surveillance system embracing sensing devices of many types and functions. Pressure and temperature switches, under and over voltage relays, gas analyzers, conductive relays and thousands of other unrelated devices actuate the logic system by means of their respective electrical contacts. Usually the system consists of 3-important sections – the annunciator, shutdown interlock and the power supply.

The Annunciator

The annunciator "announces" or alerts the operators, supervisory personnel or anybody in the vicinity that a significant change of condition has taken place.

*Process Control and Instrumentation Engineer, Resins, Inc.

That something, somewhere in the control system has gone out of predetermined limit. The announcement is usually in the form of visual and audible signs. Generally, the alert to an off-normal condition is sounding a horn, bell or buzzer – audible signal. The condition is further identified thru lighting of a lamp within which an engraved nameplate one can read the situation – visual signal. The visual signal usually are of varied forms too. Ranging from fast-intermittent flash, fast flash to steady on. The order of events or sequence, that is the action of the sensing device, signal contact, horn, lamp and the operator are of various forms also. Although generally the objectives are somewhat common.

1. It alerts the operator of an off-normal condition.
2. Identifies the nature of the condition.
3. Requires acknowledgement of the operator.
4. Informs operator when condition has returned to normal.

The signal contact which is the input to the system is normally a closed electrical contact that opens during an off-normal condition of a normally open electrical contact that closes during an off-normal condition. These mark or break the circuit with the electrical power coming from the alarms and safety shutdown interlock system. The audible and visual signal operates in accordance with the configured sequence. Push buttons generally are employed to serve Reset Test, Silence and Acknowledgment functions. (Ref. Figure 1)

The Shutdown Interlock

The shutdown interlock generally shares signal contact with the annunciator. It utilizes retransmitting relay or contact which is configured to deactivate, activate, start, shutdown, open, close or whatever action needed to carry out desired result. The mechanism may be entirely or selectively overriden by a by-pass switch as the case may be. By-pass switches are usually keylock operated. Resetting the acknowledge alarm condition can either be automatic or manual as configured in the system. Usually alarm situations automatically resets as soon as acknowledged and the process returns to normal. Shutdown conditions need manual reset; typical "mushroom" head push button are utilized to shutdown the system in case of emergency or failure of the signal contact to respond to off-normal shutdown condition.

The Power Supply

The power supply requirement for each of the different circuits is preconditioned by the power supply system. Both AC and DC voltage including the pulsing AC or DC for the flashing of lights for the back lighted windows emanates from this section.

Power supplies to electronic instruments are usually 24 V d. c., with the same voltage for the interlock circuits. Long-distance equipment-control power, from the control room to solenoids, motor starters, etc. in the plant, may be 24 or 110 a. c. in order to minimize the size of the carrier wiring.

To balance between production and protection is to have adequate control without sacrifices of flexibility and safety. Adequate control is not overcontrol, it is neither undercontrol. It means simple control, yet effective or responsive. The sensor which influences the "signal contact" should be located correctly. A poorly located sensor can create foe out of a friendly system. If possible locate sensor to measure directly the property you wish to know, not some other property from which it can be inferred. If an alarm or trip unit must be installed for pressure, overpressure as an example, don't install the pressure switch on the output line of a pressure transmitter, rather, obtain a reliable pressure switch and install it directly into the pressure tap provided in the vessel or pipeline (Figure 2b). In pipe lines where turbulent flow is expected, do not install pressure sensing devices on elbows and bends.

Stopping of fluid flow into a system by means of the safety shutdown interlock can be carried on in several ways.

1. For positive displacement pump – motor must be stopped and shutdown valve closed.

2. For centrifugal pump – motor must be stopped or shutdown valve closed.

3. For vapor application, snap acting valves installed along the vapor line closes simultaneously with shut-off of energy source for the vapor generator.

For a shutdown valve that will respond quickly, a snap-acting valve is best for this application. The use of solenoid valve couple to control valves to vent diaphragm air so valve will close is not fast enough for this application, so it may be used only on non-critical systems. Few control valve sets close tightly. Large solenoid valves if available, are equally effective as other tight setting snap acting on-off valves.

The Plant Operator

The operator's function in any safety interlock system must be limited only to the preparation of equipment required to clear a system for start-up, and to push button actions such as reset, start and stop. He must never be allowed discretionary powers to change alarm, interlock and response-time setpoints or sequences; all interlock systems must be made "operator proof". This entails both securing the physical installation or the systems and their components from unauthorized access and providing for the worst cases of operator dereliction or interference as defined by fault-free analysis. A review of these analyses, at this phase of engineering, must also consider the operator's physical relationship to the developed plant layout, his work routes and mandatory actions.

From these data, some plant design might be indicated – such as relocation of access routes, or relocation of components in order to direct his work routines through the best plant observation patterns.

Hardware – General Considerations

Electrical contacts should always be referred to and shown in their failed-or shelf-position and are to be designed to fail safe, that is always moving the initiating contacts into a safe condition on component failure.

Where intrinsically fail-safe conditions are essential, the switching devices must be electronic. The contacts of such devices fail to open for both high and low abnormal process conditions by deenergizing an internal relay. Where the employment of such fail-open contacts is mandatory, the contacts of the initiating device must be shown and the correct hardware provided to accomplish this failure mode.

Switch Actuation Consideration

A typical control "loop" may have three or more elements that can actuate a switch, namely, a transmitter, a controller-indicator-recorder and a valve-position indicator. Thus, a switch responding to a process variable that controls an interlock circuit can be initiated by several different methods.

When a switch is actuated by a process transmitter output, it usually takes its signal from the input to the receiver located in the process control panel, and thus such switches are most often located behind the panel. Tilting, mercury pressure switches are most commonly used if the transmitter is pneumatic. Electronic switches are used if the transmitter produces an electrical analog signal.

Where a critical "on-off" electrical signal is required, the interlock switch must be actuated by an independent and separate process-contacting device with its own transmitter and switch output. In other words, it must be totally independent backup to a process control when (not if) that loop fails.

It is permissible that an alarm switch be actuated by a signal or contact in the receiving instrument (indicator, recorder, or controller). For example, in certain electronic temperature circuits, the construction is such that the interlock switch is best located in the recorder or controller, but it must be pointed out that it is the least reliable switching method because any fault in the sensing element transmitting mechanism or receiving instrument can impose a false signal on the switch. This method should be used for advisory alarms only, and never for interlocks.

Valve-position indicators are useful in alarming, limiting the effect of overcontrol and determining current valve positions, but they do not measure the process. They are, therefore, secondary-effect mechanisms and should only be used as status devices.

Pushbuttons are provided in most critical interlock circuits to allow the operator to trip (shut down) a circuit if necessary, even though the process variables are within their safe limits. Pushbuttons are also used for reset and system start-up.

These services employ two basic types of pushbuttons, "momentary" (make or break) and "maintained" (make or break). A momentary-make push-button is spring-loaded so that the switch returns to its normal position when released. An electrical holding latch (actuated by the pushbutton switch) keeps the circuit energized after button release (a second, momentary-break, button required to deenergize the latch). Release of this button allows the first button to reactivate the holding latch at any time thereafter. "Maintained contact" push-button switches are mechanically interconnected pairs of buttons (e.g. start, stop). Pushing one (closing causes the other button's switch to open and vice versa. Once pressed, such a switch stays in the last position until the other button is pushed.

These pushbuttons are used where interlocking from alarms or other circuits are not required, such as in an emergency shutdown circuit. In these applications, they have the advantage (over momentary-contact pushbuttons) of eliminating the electrical holding latch, as well as by showing the circuit condition from the button positions. They are sometimes used in manual reset and interlock circuits to provide additional protection against the inadvertent reset of the circuit.

Rotary or selector switches have a wide range of applications, from relatively simple devices to complicated multicontact ones, with the position of the handle telling the operator which circuits are energized. Selector switches usually maintain their last position, but they can be equipped with mechanical or electrical actuators that will cause them to return to their first position in the event of a tripout. They are not used extensively in chemical process plants (except for the key-operated form described below) because most circuits are of the stop-start or the stop-reset interlock variety for which momentary pushbuttons are more suitable and safer.

Key-operated switches are similar to automobile ignition switches and although they can have multiple positions, are usually restricted to two. They are used for bypassing components of interlock circuits for maintenance – for instance, for the temporary isolation of a process analyzer for calibration.

Key-operated switches are used instead of maintained-contact pushbuttons or selector switches for such bypass services, because the need for a key limits unauthorized switch operation. In general practice, the lock is made so that the key cannot be removed unless the switch is in the "normal" position and panel lights are provided to emphasize the switch's condition.

Relays

The relays used in wired interlock systems are generally electro-mechanical devices consisting of an armature coil, an electromagnet plunger and one or more switching contacts. These contacts open or close discrete and separate circuits when the coil is energized and deenergized by a signal voltage. A relay is, essentially, a solenoid with switch contacts. Where possible, the type that allows visual checking is preferred because it permits relatively easy trouble-shooting.

Solid state relays (SCR's – silicon controlled rectifiers) which replace electro-mechanical relays in digital processors, act in the same manner as NO relay contacts, that is, in the conducting stage, they represent closed contacts and in the non-conducting stage, they represent closed contacts and in the non-conducting stage or failed condition, open contacts. Like mechanical relays, SCRs can be activated by either an outside voltage, current or contact closure. Where a. c. power switching is required, triac components may be used; however, they should be used with caution because they inherently fail closed.

Solenoid Valves

Where an interlock circuit is set up to rapidly stop or start the flow of some process fluid or utility, the means for doing this is almost always a solenoid valve. These devices combine an electromechanical coil and solenoid-plunger core with a valve, consisting of a disk or plug, which is positioned by the solenoid plunger to arrest or permit flow. Power to these valves is usually 24 or 110 a.c. The electrical enclosures can be either general-purpose or explosion-proof. The three basic types of solenoid valves are:

1. Two-way solenoid valves – These fail either normally open or closed, and are sometimes used to shut off or permit the flow or a utility stream. They

are limited in size and are seldom used directly in process streams because of their pressure, temperature and modulation-limitations. This type of valve can be furnished with an electrical or a manual reset, which must be actuated before the valve can return to its operating position. This feature is useful in the case of a furnace fuel shut-off, for example, because the operator can be required to go out to the furnace to reset the latch before permitting fuel to flow to the burner again. This requirement is a good safety practice to see that everything is satisfactory before reset so that the proper placement of such a device directs the operator's mandatory actions.

2. Three-way solenoid valves – These are used as intermediate devices between most interlock circuits that involve the stopping or starting of a process fluid. Here the solenoid valve acts as an air pilot to another valve, usually control valve. It has three pipe connections, an air supply and two pathways, one path being open while the other is closed. Such valves are available in three types: (a) normally open, (b) normally closed, (c) universal. The normally-open type is used to vent the control valve diaphragm when the solenoid is deenergized. Normally open or closed types are fixed-action – i.e., their construction does not permit repiping, and the internals cannot be reversed. The universal type can be arranged to operate either way, and may be needed when pressure is required at the vent port, but are not commonly used because of the possibility of error in assembly.

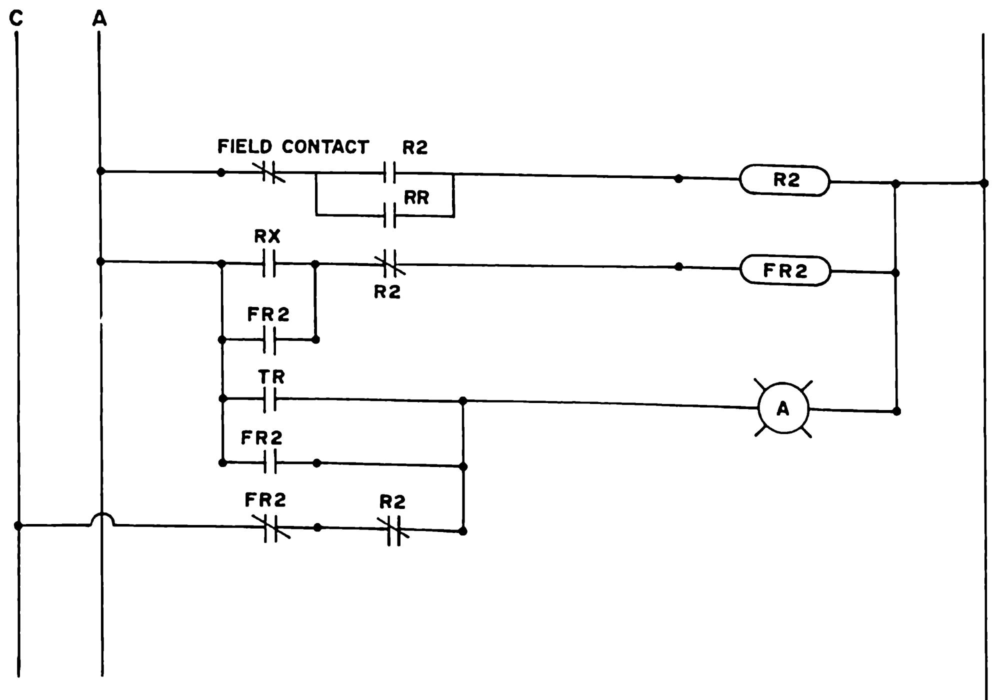

FIGURE 1

The three-way valve sizes used for diaphragm-motor actuation are usually 1/4 and 1/2-inch although sizes are available up to 2 inches. For very quick control-valve-venting actuation, an air-operated 3-way quick-exhaust valve, actuated in turn by a solenoid pilot, may be employed. This arrangement vents or pressurizes the diaphragm motor considerably faster than a common solenoid, and valve stroking times of 200 milli-seconds or less may be achieved even with large valves.

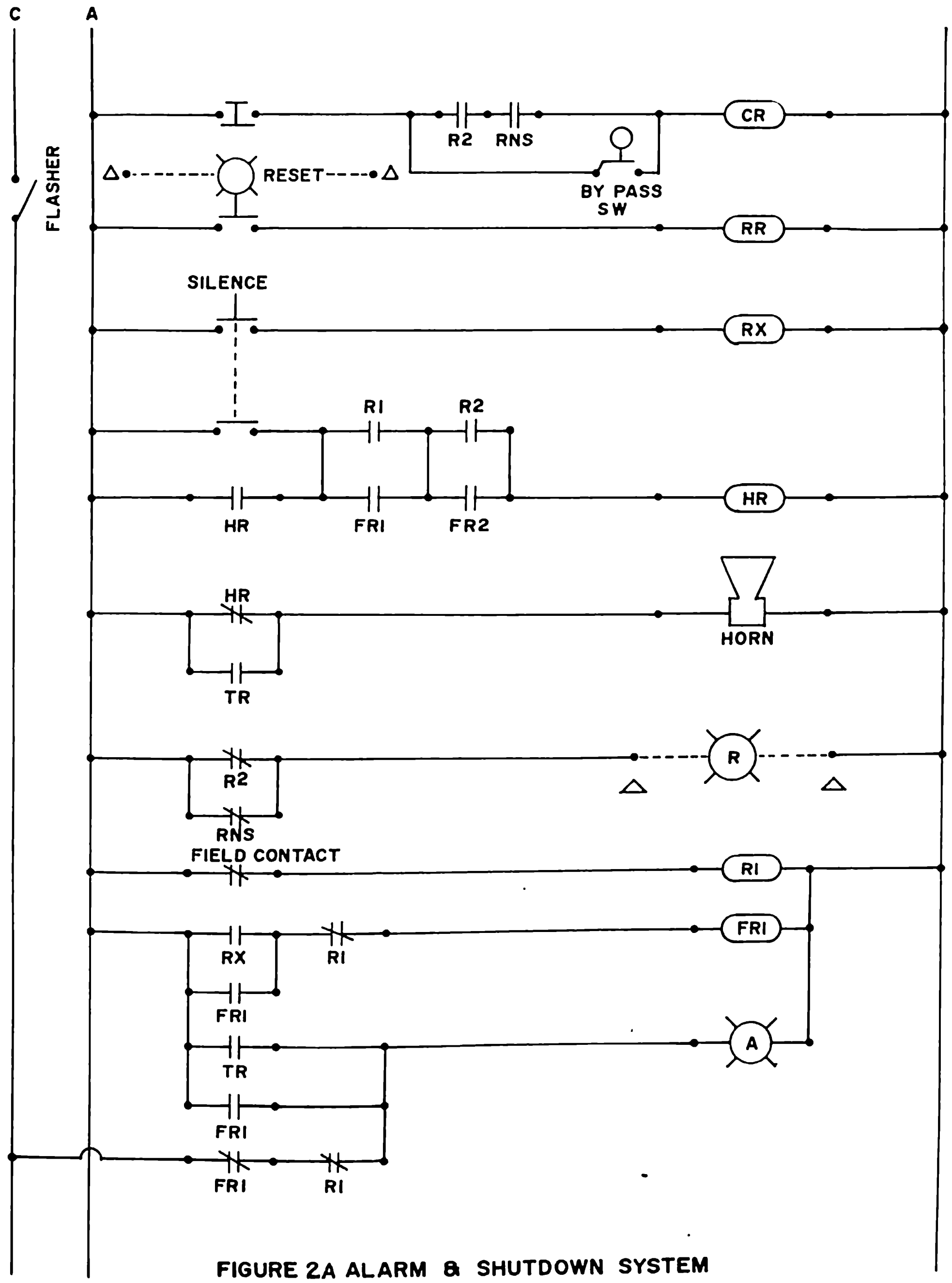

FIGURE 2A ALARM & SHUTDOWN SYSTEM

3. Four-way solenoid valves – These are generally used to operate double-acting piston operators on valves. They have four pipe connections: one supply connection, two cylinder connections and one exhaust. In the first valve position, pressure is applied to one end of an operator cylinder, while the other end exhausts. In the other valve position the pressure-end-exhaust-cylinder connections are reversed. Sizes are available from 1/4 to 1 inch. Double-acting cylinders, so actuated, are primarily used in process plant instrumentation for remotely-operated open or shut block valves that do not have fail-safe requirements.

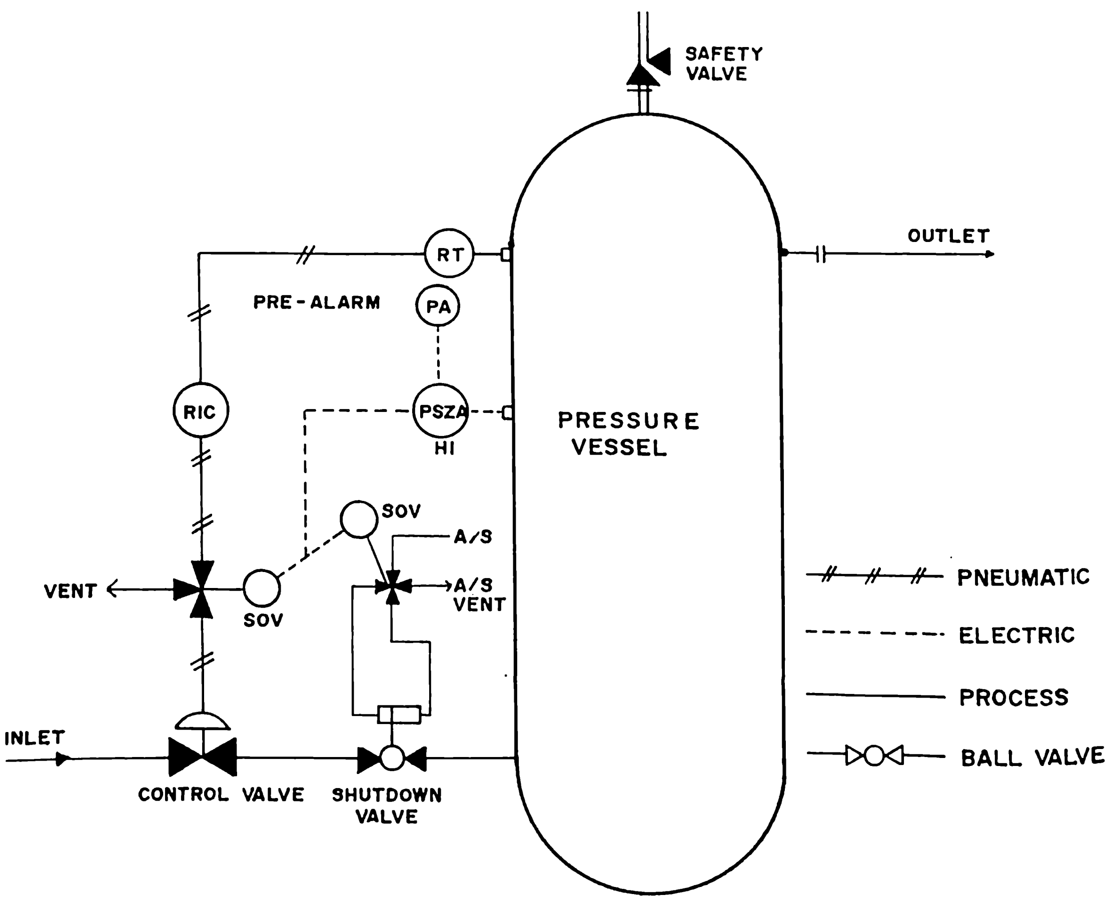

FIGURE 2B HIGHLY RELIABLE SYSTEM