SHUTDOWN SYSTEMS and

PLANT ALARMS

SECTION 11

SHUTDOWN SYSTEMS AND PLANT ALARMS

SECTION	CONTENT
11.1	Introduction
11.2	Components of a single loop shutdown system.
11.3	Multiple input and relay operated shutdown systems.
11.4	Latching and Manual reset.
11.5	Maintenance over rides
11.6	Emergency trip switches
11.7	Scheduled maintenance checks on shutdown systems
11.8	Process Alarms
11.9	Shutdown / Safeguarding checks
11.10	Protective systems

SHUTDOWN, SAFEGUARDING, PROTECTIVE AND ALARM SYSTEMS.

11.1 Introduction.

Shutdown, Safeguarding and alarm systems are designed to protect the plant, personnel and environment by tripping/ isolating/ closing down the plant, or part of it, in the event of an emergency or where critical process variables have gone into a potentially dangerous (*trip*) condition, and to provide warnings of such conditions via the use of both visual and audible process alarms.

The provision of a shutdown or safeguarding system is also a legal obligation under H.A.S.A.W.A section 2:-

'For an employer to provide, and maintain, a safe place, safe plant and safe systems of work'.

11.2 Components of a Single loop shutdown system.

A typical single shutdown loop consists of:

1. A ***measuring element***, which may for example be a Transmitter, Thermocouple or R.T.D.

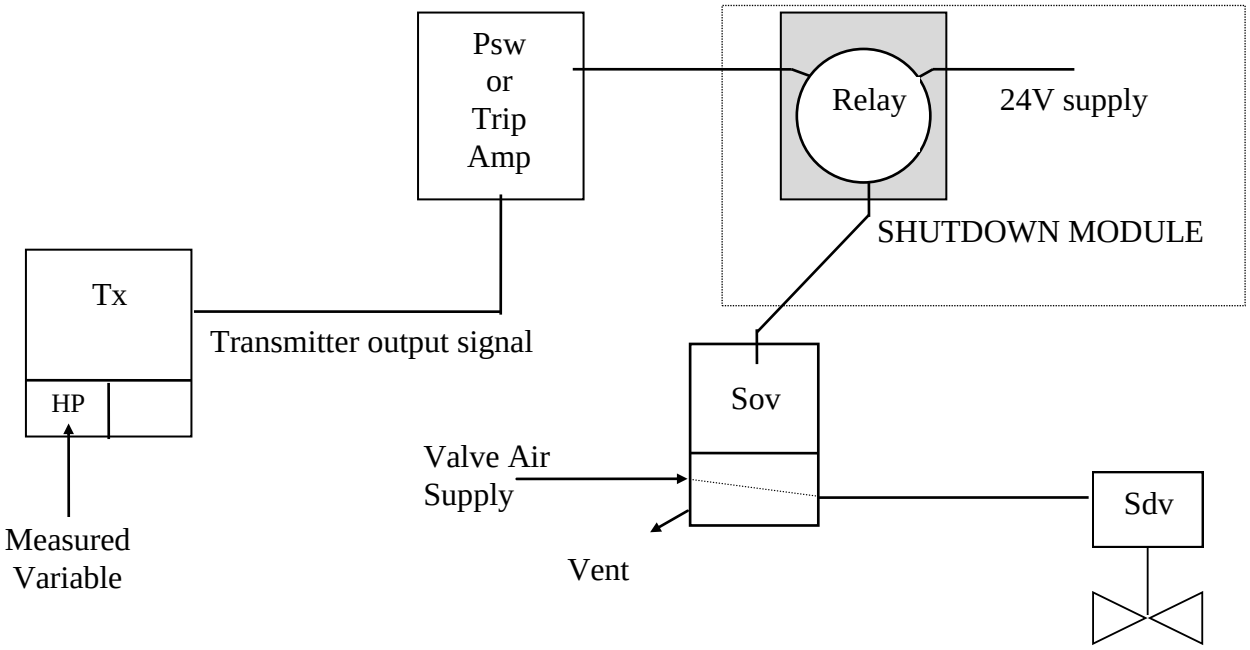
2. **Input devices**, such as A ***Pressure switch or Trip amplifier (Trip Amp)*** which receives the Tx signal, and once the desired setting or trip condition has been reached (either on a rising or falling input), the switch contacts will open switching off a 24v supply to a relay coil. Other input devices could include 'Alarm gauges', 'glass rods', 'Mobrey level switches', 'tuning fork level switches', 'position sensors' and 'proximity switches'. etc

3. *A* ***Relay*** which contains a 24v coil and a series of normally open and normally closed contacts. Under 'healthy' conditions, 24v will be applied to the relay coil which will now be *energised*. As a consequence, the relay's normally open contacts will now be closed. With the output circuit now made, a separate 24v supply will now be applied to the coil a solenoid valve.

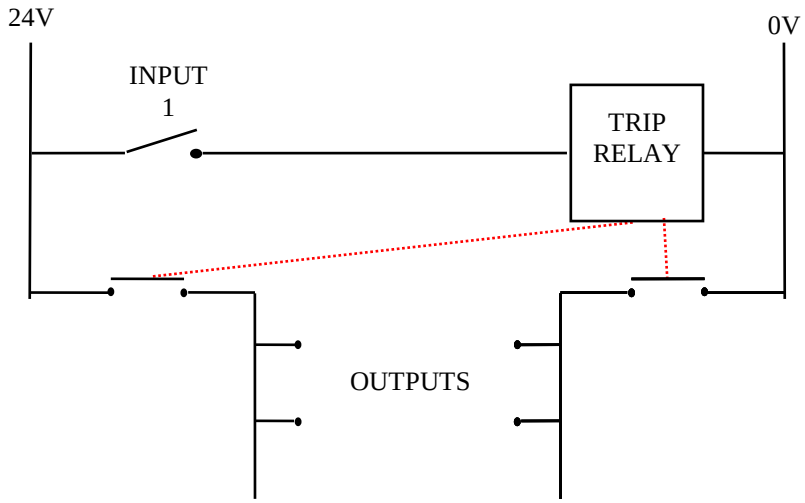
4. A ***Solenoid valve***, previously described as a electrically operated pneumatic switch. The coil of which is energised and de-energised by the switching of the relay. Under 'healthy' conditions, all circuit contacts will be closed and the solenoid energised. In this condition, the solenoid will allow an air supply to pass through it to the final trip element, usually a trip or shutdown valve.

5. ***The Trip valve*** - designed to open or close on air failure, depending on the nature of the process. Most types of valve can be adapted for this purpose (ie;- globe, butterfly, diaphragm or ball) the actuator may be a spring return or double piston type.

The following diagram shows a basic layout of how these components would be connected together:-

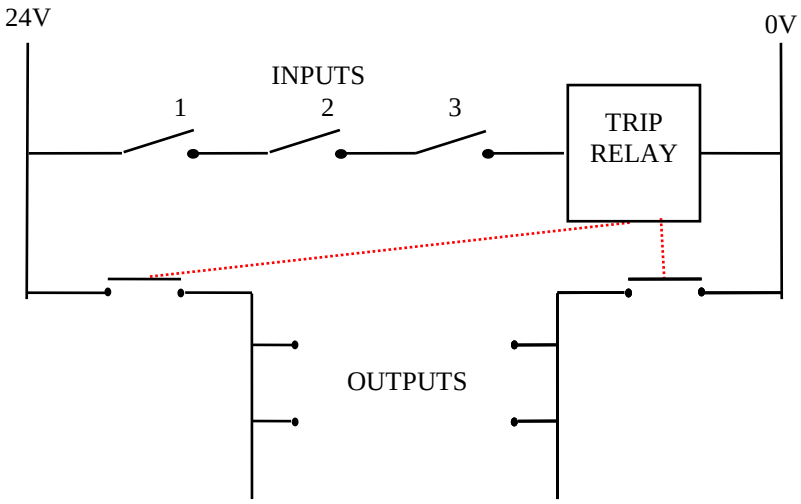


The above diagram represents a simple shutdown system using a relay to provide the logic function as to whether or not an output is required dependant upon the input state. The above system consists of a single input, and gives a single output. The diagram below displays this information as a simple ladder diagram. The pressure switch acts as input 1.

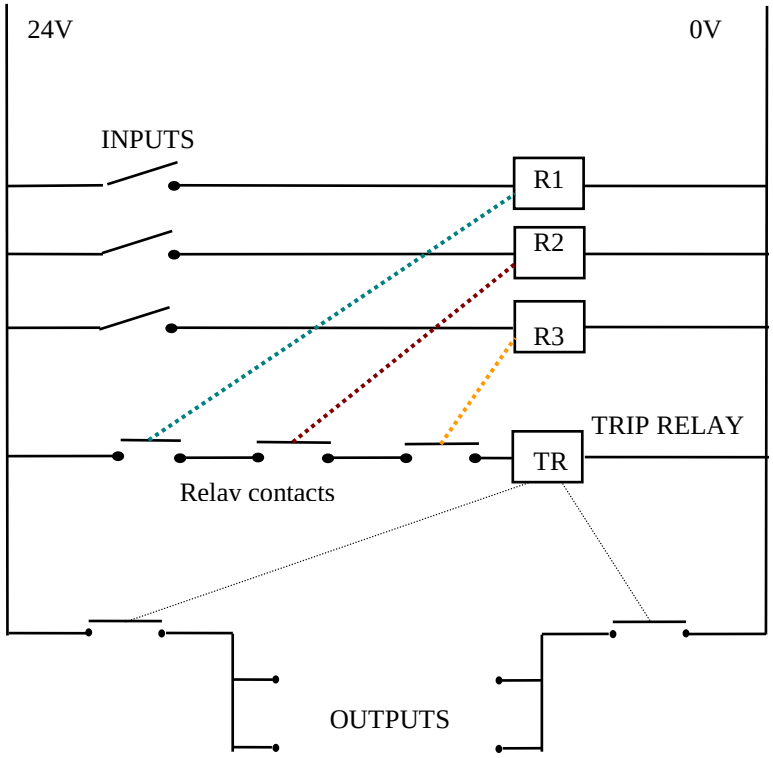


11.3 Multiple inputs and relay operated shutdown systems.

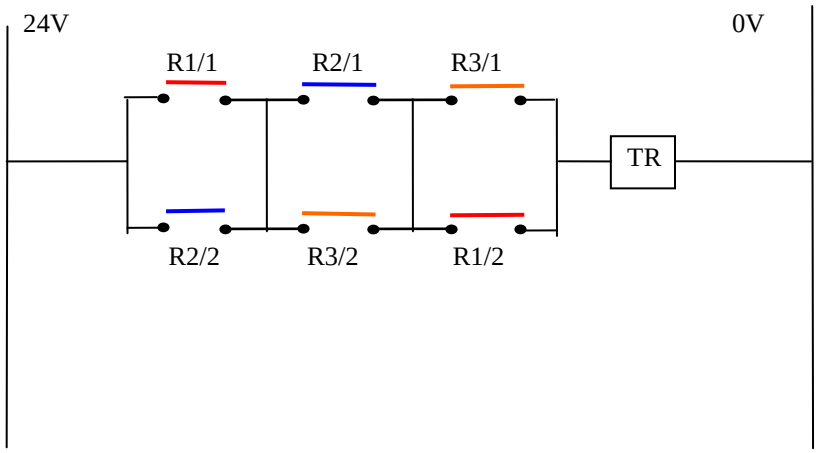
More complex functions involving multiple inputs are available by combining relays together as shown by the next series of ladder diagrams. The first diagram shows a 1 out of 3 input shutdown system, where the inputs are connected in series with each other, so that any 1 out of the 3 inputs that goes open circuit (trips) will trip the entire system:-



In reality 'it is the relay contacts that are wired in series not the actual inputs'. Each input is assigned its own relay, which contain 2 sets of normally open contacts. One set is used to operate / form the input switch for an alarm circuit, while the second set form the series chain to the final trip relay. As shown in the next diagram:-



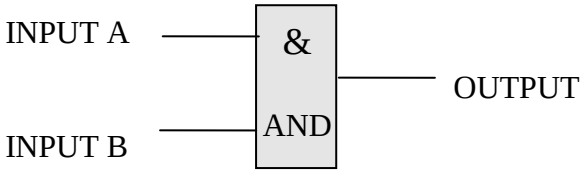
From the diagram previous, the relays used for R1, 2, 3 would be 8 pin, whilst the trip relay would be an 11 pin relay. A variation to the above could be the 2 out of 3 input shutdown module, this would be configured as shown in the next diagram:-



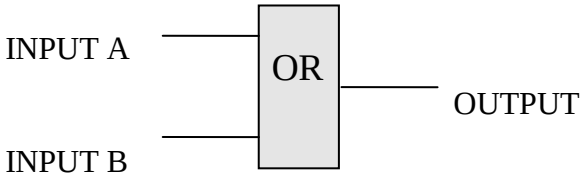
Not all circuits use relays for the logic functions, these may be performed using transistors. The added benefit of using transistor logic (as in the H.I.M.A system) means that more inputs may be monitored at any one time, whereas older systems (like the 'Trolex') although still in use are restricted because of their physical size.

Some modern shutdown systems still use relay logic however the size of relays has reduced so that more complex functions may be performed.

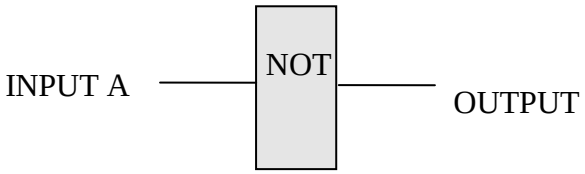
The following tables are the truth tables for a series of logic functions commonly used in shutdown systems:-



A	B	O/P
0	0	0
0	1	0
1	0	0
1	1	1



A	B	O/P
0	0	0
0	1	1
1	0	1
1	1	1



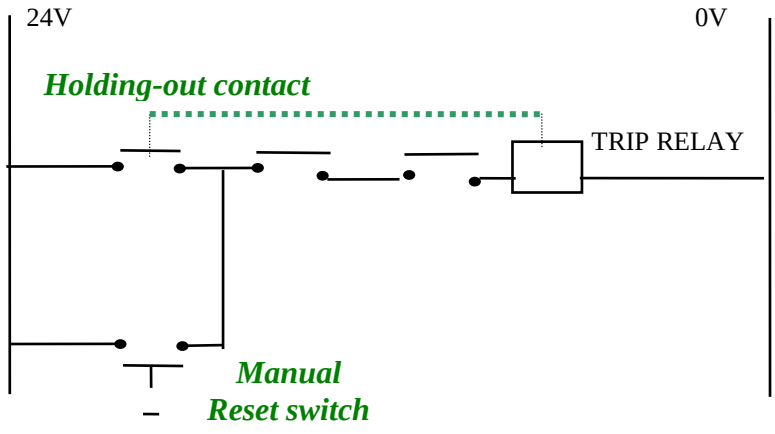
A	O/P
0	1
1	0

The logic 'NOT' function is often referred to as an inverter.

11.4 Latching and Manual reset.

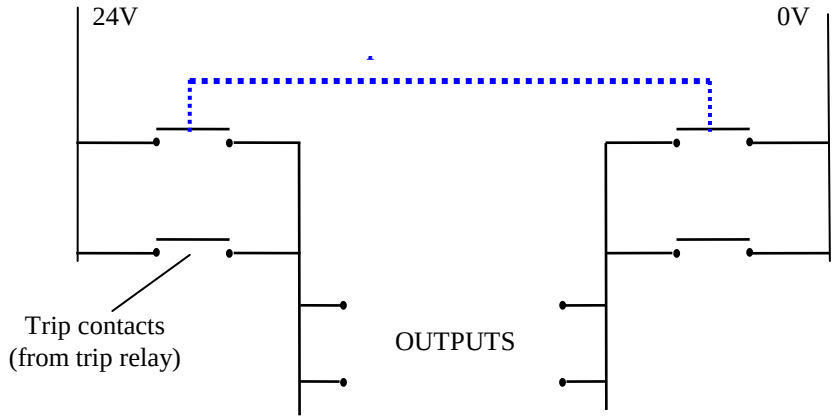
To ensure that a trip system cannot automatically re-set itself once a trip has been initiated, a ***latching* circuit** is used. This utilises one of the final trip relay's normally open contacts to prevent it's own coil from being automatically reset should the input go healthy.

The system can only be re-started by pressing a ***Manual reset*** button which momentarily by-passes the holding out contacts to energise the coil and close the contacts. The next diagram shows a ladder diagram with the addition of the manual reset and latch facility:-



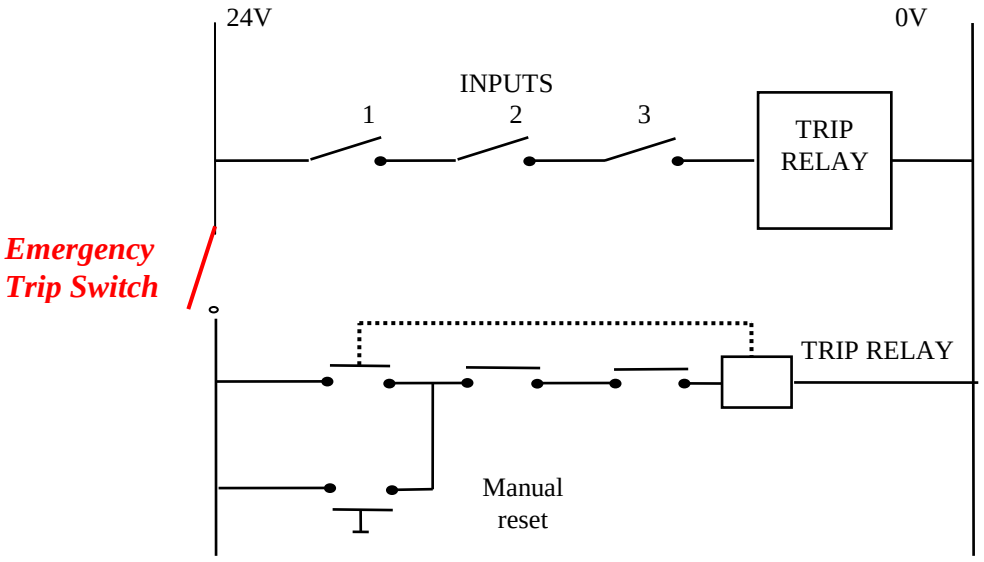
11.5 Maintenance over-rides.

Periodic maintenance and scheduled checks on shutdown systems need to be carried out without tripping the plant. To enable this, a ***trip isolation*** or maintenance over-ride facility is incorporated into the shutdown circuitry. This is normally an on/off switch which is key operated to prevent unauthorised use. The use of this function ensures that the output remains energised with 24V despite the position of any of the input switches. ***A real danger exists*** in this mode because if a dangerous condition occurred the shutdown system *would not* respond to it, so it is therefore vital to return the system to normal as soon as it is safe to do so. The next diagram shows the addition of this facility:-



11.6 Emergency trip switches.

In the event of an emergency (e.g. a plant fire etc.), the plant can be instantaneously shut down by means of ***manually operated emergency trip switches***. These are normally strategically placed around the plant and on the panel in the control room. The emergency trip switch(es) are connected in series with the trip circuit's 24v supply rail so that the supply is immediately lost once a switch is operated. The next diagram shows the introduction of the emergency trip switch:-



11.7 Scheduled maintenance checks on shutdown systems.

In accordance with the law, Shutdown systems *must* be checked at regular intervals, and ideally, should cover as much of the instrumentation as possible, without physically tripping the plant. The frequency of the checks is normally determined by the importance of the system and specific company requirements. Typically these are 1, 3 and 6 monthly intervals.

Checks are carried out to *set procedures* (sometimes referred to as shutdown checks) and typically are designed to check that all pressure switch, trip amp or other input settings are correct, that transmitters are zeroed and working correctly and that all other equipment, including alarm windows and inter-connections are fully functional.

To prevent the plant from tripping whilst checks are being carried out, a trip isolation or maintenance override must be switched on. The operation of solenoids can also be checked, provided that their linework is fitted with a bypass facility, in some cases the shutdown valve itself will be fitted with a bypass so it can be checked also.

On completion of the checks, a Reset procedure must be followed before attempting to remove the trip-isolation:

1) With all inputs restored, individual trip loop alarm windows must first be accepted by pressing the *accept* and then *reset* buttons located on the alarm panel.

2) The 'Plant trip' alarm window however, must be *de-latched* and this is acheived by pressing the main manual *reset button* on the control panel.

3) Individual valves may also need to be reset on local reset buttons.

4) With ALL red trip windows now *extinguished*, the trip isolation can be removed.

N.B. Shutdown or emergency trip systems must never be used to stop the plant for anything other than an emergency. Where a *planned* shutdown is to be carried out (e.g. for maintenance work to be carried out) the plant must be shutdown in a *safe* and correct manner, following the shutdown procedure outlined in the *plant operations manual*.

11.8 Process alarms. (ALARM SYSTEMS)

Process alarms are designed to give the operator warnings. These may be in the form of a colour visual indication and also an audible alarm.

Alarm Panels:

The alarm panels are used to bring certain plant conditions to the attention of the operator. Each module in the alarm panel is operated by a switch. The use of these alarm panels in conjunction with shutdown systems is to identify:

- Which input has operated
- If the unit has tripped
- Is the unit 'trip isolated'?

As with trip loops, the process conditions are measured and monitored by measuring elements who's signals are transmitted to pressure switches or trip amps. These in turn, are used to switch a 24v supply to an alarm panel on either *rising* or *falling* inputs. This is achieved by utilising a N.O. contact on the appropriate shutdown system relay to switch the supply on or off to the alarm module.

Once a loop has gone into the trip condition, it's associated relay contacts open, causing the alarm module to operate.

In some companies, the alarm windows are colour coded to denote their importance:

Red = Plant trip
Blue = Trip Isolation 'on'
Yellow = Priority 1 alarm,
often referred to as a *pre-alarm*.
White = Priority 2 alarm.
(eg, condensate low flow)

Whenever a process alarm has activated, it must be acknowledged (and silenced) by first pressing the *accept* button on the alarm panel. The *reset* button must then be pressed to see if the alarm condition has cleared or cancelled. The system is so designed so that once initiated these alarms *will not self cancel,* therefore requiring process operator attention.

Where a series of alarms have sounded simultaneously, the operator needs to know which of these came up first. To facilitate this *first up* modules are used. Once the *accept* button is pressed, *all* alarm windows will *stop* flashing except the one which came up first, which will continue to flash.

Scheduled checks on Alarms:

Each alarm panel has it's own 'test', 'accept' and 'reset' buttons, the use of which has no effect on the plant conditions. The functions of these buttons are as follows:

Test: Will cause all the alarm windows to light up and flash. Also activates an audible alarm.

This facility is used to check the function and operation of all alarm windows and enables us to identify defective modules or light bulbs.

Accept: Used to acknowledge and silence alarms. Modules stay lit but stop flashing, except where 'first up' modules are installed.

('First up' modules are designed to show the operator which alarm came up first, when several alarms have sounded simultaneously. Once the 'accept' button has been pressed, all alarm windows, except the first to operate, will stop flashing.)

Reset: Will extinguish all alarm windows, provided that the alarm condition(s) have cleared. Not to be confused with latched circuits which can only be reset via the manual reset.

Periodical schedule checks are carried out on alarms as well as trip loops, again usually 1, 3 and 6 months frequency, depending on the company and importance of the alarm. During these checks, the correct operation of alarm windows are checked, along with the pressure switch or trip amp *settings*.

To begin the checks, a *lamp check* is carried out to ensure that all alarm windows are operational. This is acheived by pressing the *test* button, followed by the accept and reset buttons. At this stage, any defective bulbs or alarm modules should be replaced. When changing a defective alarm module it is important to note the module's *model number* and to change *like* for *like*.

Pressure switch / trip amp settings are then checked, and in each case, the correct operation of the *alarm window* should be observed.

TransAlarm Unit modes of alarm:

These may have several alarm modes:

a) Time delays – where the alarm condition has to exist for so many seconds before the alarm sounds.

b) First-up Alarm – as previously described.

c) Fleeting Contact Alarm – this triggers if the alarm condition only persists for a fraction of a second**.**

11.9 Shutdown/ Safeguarding checks :

As discussed earlier, shutdown or safeguarding systems must be regularly checked and results recorded to ensure, as much as is humanly possible, that the system and equipment are, at all times, well maintained and fully operational.

By checking and testing as much of the input / output systems, instrumentation and inter- connections as possible whilst maintaining the integrity of a running plant or

process, we can offer maximum guarantees that our shutdown system will operate should it be required to do so.

The procedures for carrying out scheduled maintenance checks will have been written down by the Engineers, and the Technician carrying out the testing will consequently have written procedures from which to work.

To begin the checks, a *lamp check* is carried out to ensure that all alarm windows are operational. This is acheived by pressing the *test* button, followed by the accept and reset buttons. At this stage, any defective bulbs or alarm modules should be replaced. When changing a defective alarm module it is important to note the module's *model number* and to change *like* for *like*.

Before carrying out the plant checks, the TRIP ISOLATION (or Maintenance Override) must be operated. This can usually be confirmed by the operation of the 'Trip Isolation' alarm window which is normally located on the panel in the control room.

Once the Trip Isolation has been activated, the outputs can only be de-energised via the Emergency Trip Switch, which as described earlier, removes the +24v to the final trip relay and the output solenoids.

It is also important to ensure that any control loops which form part of the trip system, are switched to MANUAL before testing can start.

'Shutdown checks are critical, and of utmost importance is that they are done right. It is important to read and follow the procedures. The work must not be rushed, and double check if you are unsure. ***A simple error, could have a costly consequence***.'

Testing Inputs:

The input devices commonly consist of:

a) The field transmitter or measuring element
b) The switching device, normally a pressure switch or Trip amp.

a) The transmitter:

Depending upon site requirements, the checks may include:

i) An on-line zero check of the Tx,
ii) Occasion range checks
iii) Functional checks to ensure that the transmitter and trip loop responds to simulated high or low trip conditions.

b) The Pressure Switch/ Trip Amp or other input device..

It is common practice to check all switch settings during shutdown checks, using the Instrument Data sheets to obtain the correct or desired settings.

Additionally, functional checks should also be carried out to ensure that:

i) The correct alarm / trip window has operated
ii) That the 'accept', 'reset' and manual reset facilities are fully operational.

It is also standard practice to record any faults or errors found during the checks and, where applicable, to correct and repair 'as you go along.'

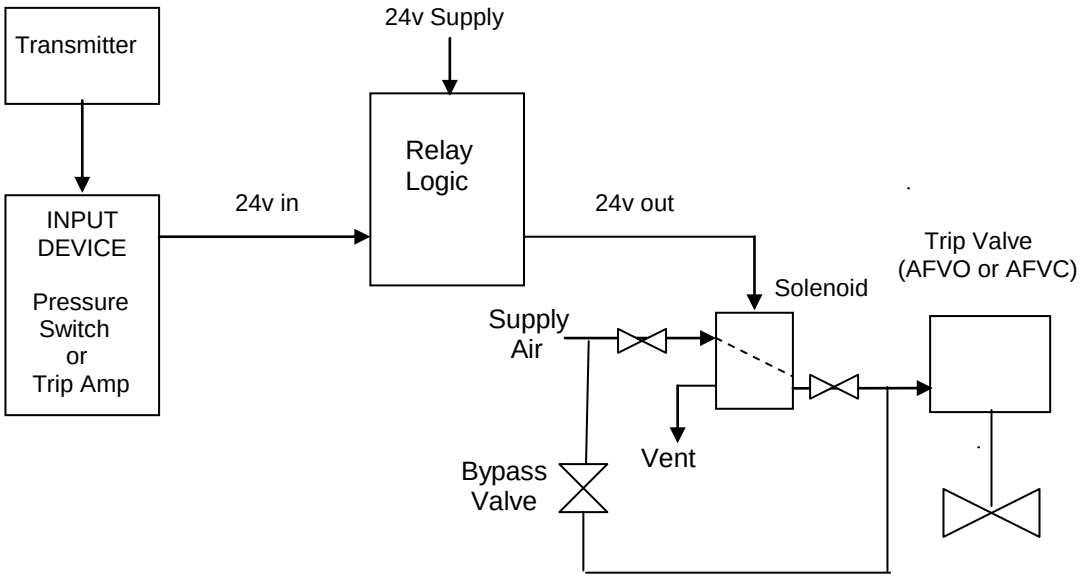
c) Testing Outputs:

We have seen that in the vast majority of cases, the loss of our 24v output will de-energise the trip solenoids, which in turn, operate the final trip valves.

For testing the outputs, we need to check that the solenoid has de-energised and, in a few cases, may even be able to allow the trip valve to operate, thereby competing a full functional check on the system.

In the majority of cases however, tripping the valve is not practicable. By equipping the final trip solenoid with a by-pass line however, we can safely check the solenoid's operation whilst maintaining an air supply to the trip valve.

The diagram below shows how these loop components connect together:



The solenoid is by-passed by opening the by-pass valve before closing valves A and B. This ensures that even when the solenoid de-energises, supply air to the trip valve is maintained via the by-pass facility.

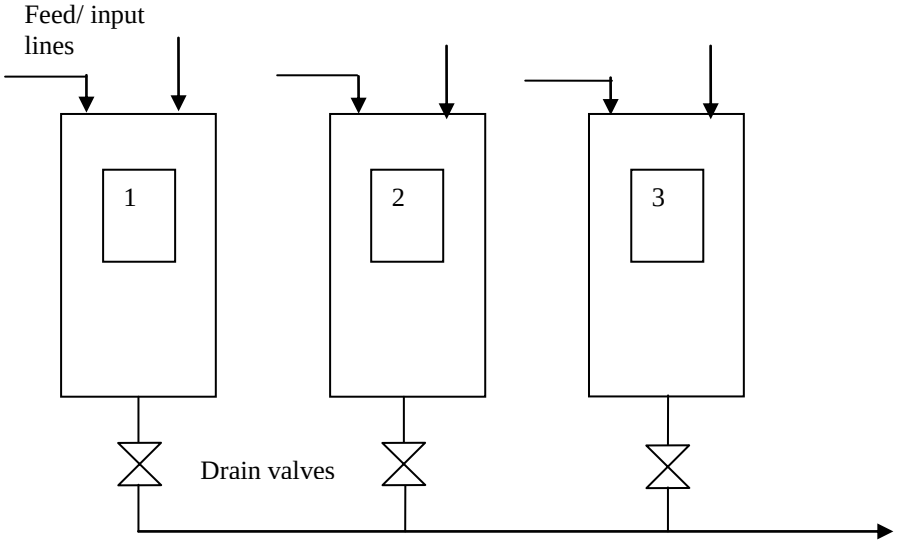
N.B. All three valves must be returned to their normal positions on completion of the checks.

It is also important to remember to follow the correct 'Accept' and 'Reset' procedure before attempting to remove the trip isolation on completion of the checks. This is confirmed when all Red Trip Alarm windows on the panel have extinguished.

11.10 Protective Systems

Protective Systems, or interlock systems are often used on plants or items of plant, to prevent predicted unwanted occurrences.

On one plant, a series of reactors have their outputs fed together, one of the input's to each vessel, is highly hazardous. So to prevent major incident, all other input's to the reactor, and the output valves must be shut. If this were not the case, in theory it would be possible for the hazardous product to go in one vessel and out to atmosphere via another. Equally, before moving the batched process onto the next stage of the process, all other drain valves must be closed, as it is possible to blast product under pressure into the other vessels. As in the diagram below.



An Interlock, or protective system is used to ensure possible dangerous conditions do not occur. (From the diagram above), pressurised materials from one vessel cannot enter into either of the other vessels. To facilitate this, this reactor pressure would be interlocked to the drain valves, or if one valve is open, the others must be closed. Position sensors, or proximity switches on each valve would feed back to a logic system, which would prevent the reactor dump valve from opening until all others were shut.

Like all, systems of this nature, regular checking is imperative to the safe operation of the plant.