THE EMERGENCY STOP

the button of last resort

An overview of the Emergency Stop Button and methods for establishing and maintaining its reliability of it action throughout a control system

by

Robin J Carver

Dated
April 2002

THE EMERGENCY STOP

the button of last resort

An overview of the Emergency Stop Button and methods for establishing and maintaining its reliability of it action throughout a control system

by
Robin J Carver

Dated
April 2002

Robin J Carver
108 Carlton Road
Bilton
RUGBY
Warwickshire
UK
CV22 7PE
Tel: Int + 44 (0) 1788 33 66 81
Fax: Int + 44 (0) 1788 33 66 82
Email: robincarver@dial1.co.uk
Website: www.robin-carver.com

THE EMERGENCY STOP
the button of last resort

SAFE DESIGN

When considering the design of any machine it is important to eliminate as many hazards as possible and by doing so negating the need for any additional safety measures. However, most machines are not as simple as that and there will undoubtedly be hazards that cannot be eliminated. For hazards that cannot be reasonably removed or limited by design, protective guards (or similar safeguards) are required. These guards may be reinforced by interlocking devices, direct mechanical guard locking and/or control system linked, to affirm the guard's integrity. The design of the control system should be such that proximity to the hazard is restricted, typically by requiring two hand control or perimeter monitoring (light curtains etc.). Where the operational requirements of the machine leave hazards exposed or to reinforce other safeguards, then display notices in the form of text, words, signal, symbols, diagrams, etc., and, importantly, training and instructions. Poetically described as *"warn & inform"*.

Having refined the design to reduce the risks to a practical minimum and provided all the safety information possible, the machine is safe for all the foreseen safety incidents.

But what about the un-foreseen incidents?

This is what the Emergency Stop button is for!

EMERGENCY STOP ACTUATOR

When required the emergency stop must be accessible, recognisable and must work, reliably and safely.
It may not be a button. It could be a grab wire, rope, bar or handle and in some specific applications, a foot pedal without a protective cover or a combination of devises.
Whatever actuations are used they must be accessible to all who may have to operate them and their location should be obvious.

Location

They should be positioned for easy access by the operator or anyone who may need to use them, however, they should not be located where their use could endanger the user. Remember that the person using the emergency stop may not necessarily be the person in danger! It may, therefore, be prudent to position an emergency stop near an adjacent machine, or machine zone in the case of a complex system, giving the neighbouring operator the opportunity to stop the machine if the operator gets into trouble. Where this is done, the zone of effectiveness of the Emergency Stop must be clearly indicated to avoid confusion.

Presentation

The colour, and action of the emergency stop actuator is clearly defined in BS EN 418. It should be red and, as far as is practicable on a yellow background. An emergency stop button must be of a mushroom style.

Action

Emergency stop devices should meet the requirements defined by BS EN 418 and BS EN 60947-5-5. In common with all other actuators the emergency stop operation should result in it mechanically “latched in” and not “de-latching” until the device itself has been reset. Without exception operation of the emergency stop should result in the “de-energisation” of the emergency stop control circuit. This must be achieved through opening of the contacts

and “positive mode operation” where the contact separation must be as a direct result of the movement of the switch actuator. Emergency Stop buttons using detachable contact blocks should be configured such that the contact will open should the contact block become detached ensuring Fail Safe operation.

The resetting of the emergency stop device itself must not allow the machine to a restart.

THE EMERGENCY STOP SYSTEM

The design of the emergency stop system should take into account that, hopefully, it will be used very infrequently but it must be available and ready for operation at all times.

Operation in an emergency

The nature and operation of the machine must be considered.

- Is it safe to have the emergency stop system cut the power to the machine drives and actuators? This may result in the hazard "freefalling" leading to a more dangerous situation.
- Should the system actuate a brake or clamp?
- Would stopping the machine in position result in a worsening of an injury?
- Should the system allow the machine to continue on or reverse to a safe position?

BS EN 418 categorizes these considerations and BS EN 60204 further refines these as follows:-

Stop category 0:-

Uncontrolled stop -- stopping by immediate removal of power to the machine actuator(s), all brakes and/or mechanical stopping devices being applied.

Stop category 1:-

Controlled stop -- with power available to the machine actuator(s) to achieve the stop and then removal of the power when the stop is achieved.

Stop category 2:-

Controlled stop -- with power left available to the machine actuator(s).

System integrity

The integrity of the system and its ability to resist faults requires consideration.

Positively Driven Contacts

The use of “positively driven” contacts in buttons, relays and contactors (also known as ”forced guidance”) is common and needs some clarification. These terms mean that all device contacts, in a set of contacts, must be mechanically linked in a manner that prevents abnormal operation; contacts must switch together or not at all. For example, if one set of contacts has welded (due to external circuit overload) it is impossible for the normally open and normally closed contacts in a set to be simultaneously conducting. Therefore, a safety system can employ simple logical tests, which rely on the relay's predictable performance.

Electronic or programmable electronic systems

With the exception of very sophisticated Programmable Electronic Safety Systems as defined in BS EN 61508, electronic, PLC or computer systems are not considered to be acceptable as safety systems. The safety system must be external and supervisory to any such systems and in accordance with BS EN 60204-1 section 9 must be hard-wired with final removal of power to actuators by means of electromechanical components.

BS EN954 Categories

With regard to determining the integrity of the Emergency Stop system overall; BS EN954 lists five categories of fault integrity determined by the following factors :-

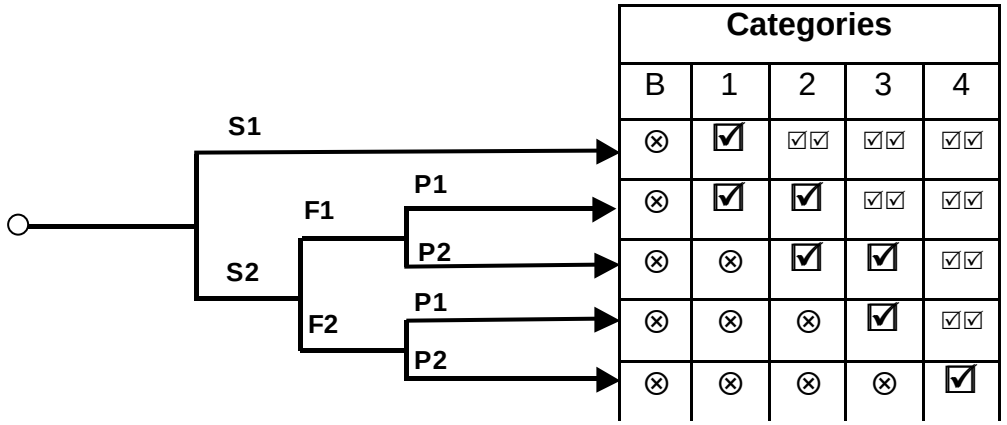
- the severity of any possible injury
- the frequency and exposure to the hazard

and

- the possibility of avoiding the hazard

The five categories range from the simplest category “B” through to category “1” up to category “4” this being the most stringent in acknowledgment of the higher risk anticipated.

British Standard publishes a category assessment chart in BS EN 954-1 based on the factors above.
The following assessment chart extracted from BS EN 954-1 determines the category.



Categories				
B	1	2	3	4
⊗	☑	☑☑	☑☑	☑☑
⊗	☑	☑	☑☑	☑☑
⊗	⊗	☑	☑	☑☑
⊗	⊗	⊗	☑	☑☑
⊗	⊗	⊗	⊗	☑

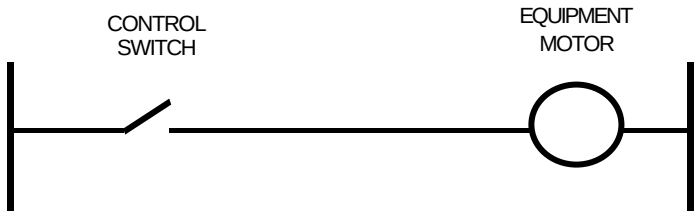
Key

S1	Severity of injury – Slight (i.e. cut or bruise)
S2	Severity of injury – Serious (i.e. hospital treatment to fatal)
F1	Frequency of exposure to hazard – seldom or often but short exposure
F2	Frequency of exposure to hazard – continuous or frequent with long exposure
P1	Possibility of avoiding hazard – possible or slow moving hazard
P2	Possibility of avoiding hazard – not possible or fast moving hazard
⊗	Possible category requiring further measures
☑	Preferred category
☑☑	Measures exceeding requirements for risk involved

Category B

The least demanding category, applicable in general to low risk “domestic” type equipment and hand tools. Here a single fault may lead to a loss of the safety function. Notwithstanding, the component parts of the control system must be suitable for the application and must be able to withstand the expected stresses and anticipated uses.

Example of a Category B circuit



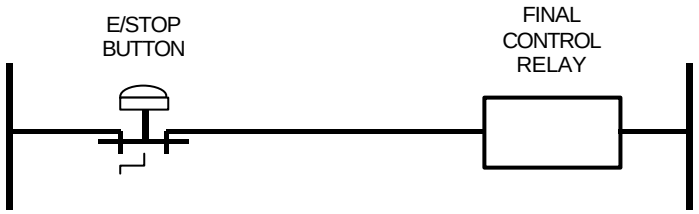
This simplified example illustrates a Category B Stop Circuit using a spring actuated control contact, de-energising the motor in an emergency. Any failure of the control switch spring or break-up of the switch could prevent the motor from stopping.

Generally, these would be “plugged in” powered devices and if they failed to switch off then the plug would be “pulled” by the user. The only practical way to detect faults is by inspection and test.

Category 1

As with Category B, a single fault may lead to a loss of the safety function but the design must employ well proven components and principles. Use of components that have been life tested, have positive mode operation and a known and appropriate failure characteristic would be expected.
Arguably, Category 1 would be the minimum level of system integrity used for industrial equipment.

Example of a Category 1 circuit

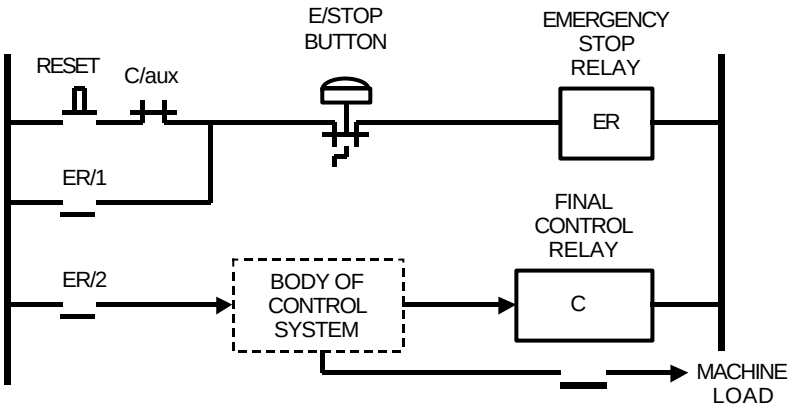


This simplified example illustrates a Category 1 Emergency Stop Circuit using a “positively driven” emergency stop contact, de-energising the Final Control relay in an emergency. By using an approved Emergency Stop button the device should be reliable, the Final Control Relay, however, may have been subjected to loading stresses and its contact could weld closed. A positively driven relay may be capable of breaking light welding, however, a spring driven type probably will not.
In common with Category B, these would be “plugged in” powered devices and if they failed to switch off then the plug would be “pulled” by the user.
Again the only practical way to detect faults is by inspection and test.

Category 2

As with Category 1, the design must employ well proven components and principles but in addition a functional check of the safety system must be performed as the machine commences operation and, if possible, periodically during operation.

Example of a Category 2 circuit

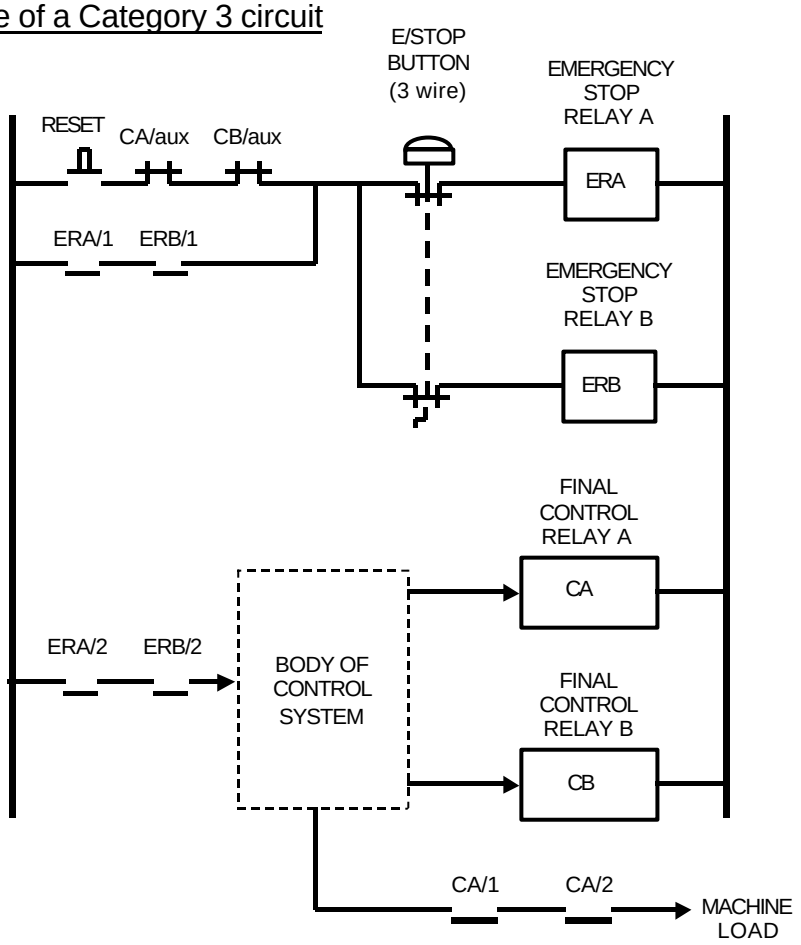


The simplified example above illustrates a Category 2 Emergency Stop system employs a functional check of the safety monitoring the action of the Final Control relay “C”. Both relays (ER & C) must be “positive driven” types ensuring that if the main load contacts “weld” the other contacts will be held in the matching position allowing the system to detect the failure. (Note: The auxiliary contact of relay “C” must be a directly operated contact of the relay, not an “add-on” auxiliary as they can be removed and may not correctly represent the action of the device.) On powering up the system the Emergency Stop button must be de-latched and the Emergency Stop Reset button must be pressed. If the Final Control relay has failed during the last operation C/aux will be open and the system will not be allowed to reset. With a Category 2 system, a routine of regular testing is essential and this should be included into the Instruction Manual and as a notice on the machine.

Category 3

All that applies to Category 2 applies to Category 3 plus the requirement that a single fault in the safety system shall not create any loss of safety. This means that not all faults need be detected and that an accumulation of faults could still cause a loss of safety.

Example of a Category 3 circuit



The simplified example above illustrates a Category 3 Emergency Stop system similar to Category 2 it employs “positive driven” relays and a functional check of the action of the Final Control relays. The requirement is that a single fault should not create a loss of safety. To this end some device redundant systems are employed. The Emergency Stop button has two independent sets of contacts each controlling two Emergency Stop relays (ERA & ERB). To allow the system to operate both relays must be energised. A failure of one of the Emergency Stop button contacts in the closed position, whilst not being detected, would not result in the Emergency Stop function

being inoperative. Similarly, the Final Control relays (CA & CB) are duplicated. In this instance, however, the action of both is monitored by the feedback contacts CA/aux & CB/aux. If either of these contact assemblies should fail (welded) in the closed position then the feedback contact would not close inhibiting the safety system from being reset following a power failure or the operation of the Emergency Stop button.
The integrity of a Category 3 system is much more demanding and, clearly, the use of some redundant devices is appropriate.

When emergency stop devices are connected via flexible cables, which are subject to constant flexing then care must be taken in the design of the system. With the type of configuration shown above (known as a 3-wire system) there is an increased risk of a short circuit between cables, which may not be detected and render the safety circuits ineffective. This is a very rare occurrence, but experience has shown that it can occur. When flexing of cables is considered a potential problem a 4-wire dual channel arrangement should be employed such as that illustrated for Category 4, below, were each channel can detect any short circuit between two conductors.

Category 4

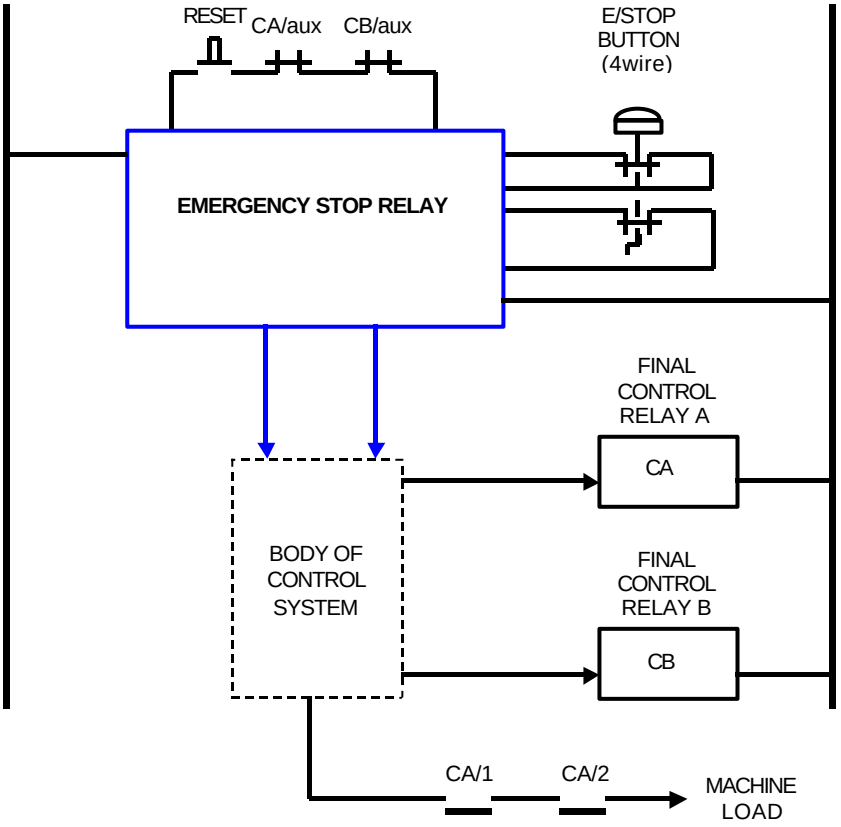
This is the most demanding category. All that applies to the lower categories applies to Category 4.

- The design must employ well-proven components and principles.
- A functional check of the safety system must be performed as the machine commences operation and, if possible, periodically during operation.

Plus

- Any fault must be detected before the safety system is called upon to function so that there is no loss of safety.
- If this is not possible an accumulation of faults in the safety system shall not create any loss of safety.

<u>Example of a Category 4 circuit</u>



Category 4 demands a very sophisticated safety system and the only practical and cost effective solution is to employ a dedicated Emergency Stop Relay. This is included in the illustration above.

Emergency Stop Relays are fail safe, maintaining the safety function in all circumstances. The circuit is redundant with built in self monitoring and the correct opening and closing of the safety function relay is automatically tested in each on/off cycle.

The unit employs a 4-wire duel channel circuit that monitors the Emergency Stop button contacts independently and can determine cross connections (i.e. due to cable damage etc.). The duplicated Final Control Relays are monitored inhibiting the safety system from being reset if a failure is detected.

The integrity of a Category 4 system is vital and, clearly, the use of redundant devices is essential.

ADDITIONAL PARTS OF THE EMERGENCY STOP SYSTEM

When designing the Emergency Stop safety system there is a tendency to think only in terms of the electrical controls. It is vital to take into account all the sources of power used on the machine, pneumatic, hydraulic, etc., and for the safety system to encompass them. It is important to remember that, unlike most standard ac electrical systems, pneumatic and hydraulic systems may retain significant amounts of energy even when the primary supply source has been isolated. From a safety perspective this retained energy may be a hazard or on the other hand the retained energy may be used to retard the hazard. These should be significant considerations in the safety design.

Safety Shutoff Solenoids

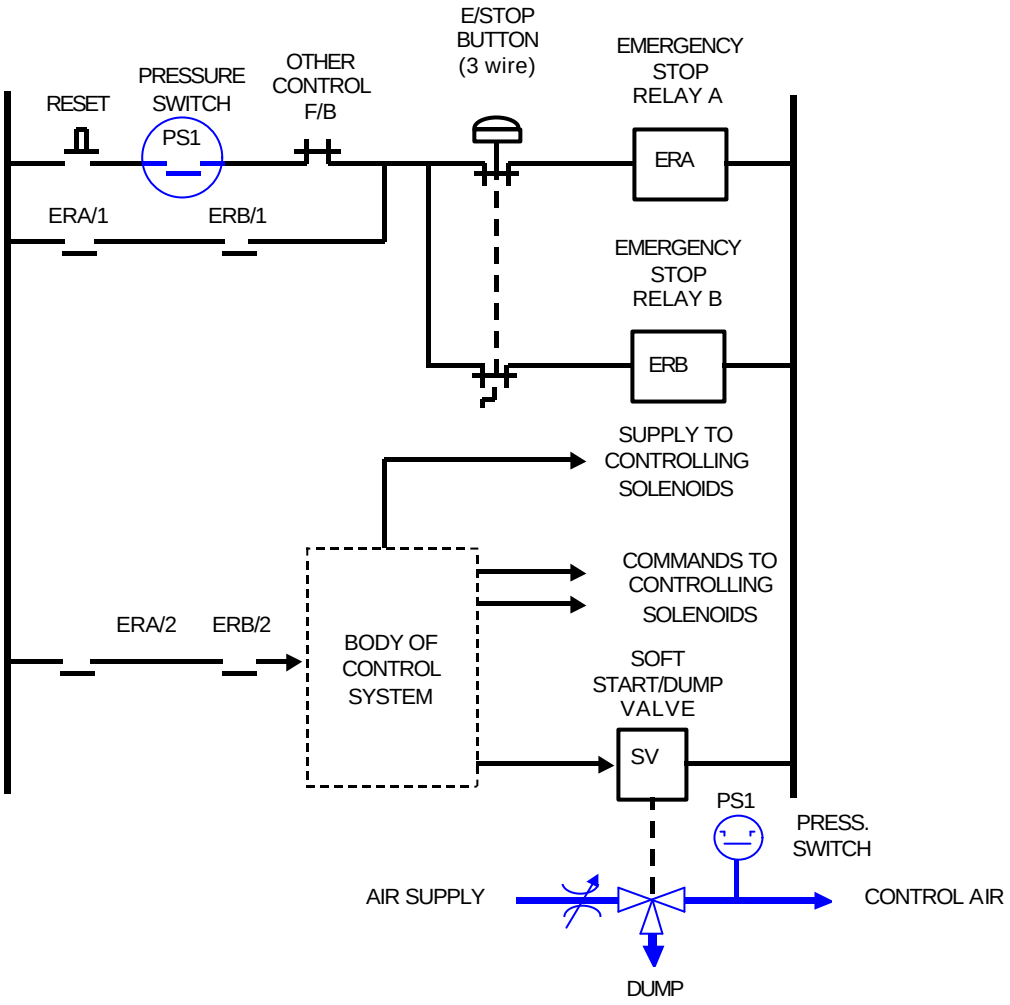
Special safety soft start/dump valves are available and should be used as appropriate, particularly in the primary supply. These valves, when first energised, allow for a slow build-up of pressure in the system, providing time for faults, such as leaking valves etc. to become apparent before the system has generated enough energy to be a significant hazard. Integrated into the Emergency Stop system the valve allows the supply to be shut off and the pressure retained in the system to be quickly “dumped” from the system.

Pressure Proving

In pressure-powered systems, consideration should be given to providing “proving” feedback to the safety system, via a pressure switch. As with the electrical systems, this would confirm that following a supply shutdown that the pressure in the system has been removed or lowered to a safe level. It is common practice to employ a valve plug proving contact, although this is only indicative of a safe pressure by virtue of the valve being closed.

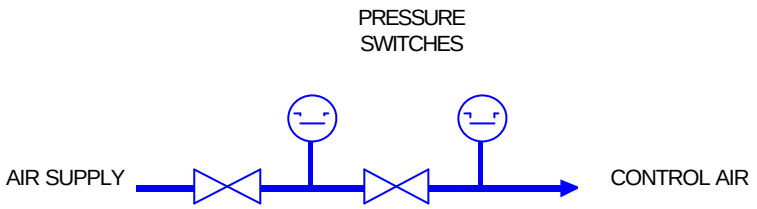
This configuration would be a requirement of most Category 3 or 4 systems and it desirability should be considered for Category 2. Device redundancy would be provided by safety isolation of the electrical control feeds to the individual control solenoids.

Example of a Category 3 circuit with Pressure Proving



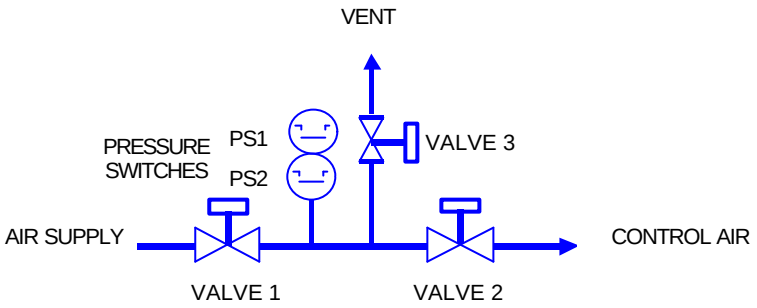
Valve Proving

Valve redundancy may be demanded and in its simplest configuration can be provided in the form of two shut off valves in series known as a “double block”. However, unlike electrical contactors with positively driven contacts, the successful operation of the valves (as a tight shut off) cannot be, absolutely, proven by limit switches. Pressure switches cannot be relied upon as trapped pressures between Valves may indicate a failure when none exists.



Basic Double Block Valve system

A system is required to test the valves is required. In practice, this can only be undertaken prior to starting the system.



Simple Valve Proving System

This operates as follows: -

Both valves 1 & 2 are closed.

VALVE 1 TEST

1. Valve 3 opens to vent the connecting pipe to atmosphere (or a vacuum is drawn).
2. Valve 3 closes.
3. After a preset time pressure switch PS2 (set at a low level) is checked to ensure that there has been no pressure build-up indicating that Valve 1 is leaking.

VALVE 2 TEST

4. Valve 1 opens to pressurise the connecting pipe.
5. Pressure switch PS1 (set at a high level) closes at this pressure.
6. Valve 1 closes.

7. After a preset time pressure switch PS1 remains closed proving that the pressure has not fallen indicating that Valve 2 (or Valve 3) is not leaking.

Should any valve fail the testing then the operation of the safety system will be inhibited.

THE LAST RESORT

The emergency stop is the control you hope never to use but if it is necessary to resort to using it, it must work, reliably and safely.

The design of the emergency stop system should take into account that, hopefully, it will be used very infrequently but it must be available and ready for operation at all times. During, possibly years of inactivity the circuitry may be subjected to neglect, wear, contamination etc. but if the time comes, and all the safety measures fail to prevent the risk becoming realised then the Emergency Stop system may be the last resort in preventing or reducing the consequences of an accident.

The emergency stop system should NEVER be an alternative to proper safeguarding nor as a substitute for proper automatic safety devices.

Robin J Carver is a Control & Safety Systems Engineer with considerable experience in design, engineering and management of a wide range of industrial process, production, energy management, and power control projects. Specialising in the specification, design and implementation of safety systems, Risk Assessment, CE Marking and PUWER 98.

Robin J Carver

108 Carlton Road
Bilton
RUGBY
Warwickshire
UK
CV22 7PE
Tel: Int + 44 (0) 1788 33 66 81
Fax: Int + 44 (0) 1788 33 66 82
Email: robincarver@dial1.co.uk
Website: www.robin-carver.com