

VI - Safety techniques

In this chapter we discuss some of the more significant and common safety techniques and introduce some of the vocabulary used by safety equipment manufacturers like Honeywell to describe features and benefits of their products. The information provided is not intended to replace, and **must not** be used to replace, our detailed instructions for use or operation.

Definitions

Electrosensitive protective equipment (ESPE)

An assembly of devices and/or components working together for protective tripping or presence sensing purposes. As a minimum this comprises:

- a sensing function
- a control/monitoring function
- an output signal switching device (OSSD)

Output signal switching device (OSSD)

The component of the ESPE connected to the machine control system which, when the sensing function is actuated during normal operation, responds by going to the OFF state.

Machine primary control element (MPCE)

The electrically powered element that directly controls the normal operation of a machine in such a way that it is the last element (in time) to function when machine operation is initiated or arrested. This can be, for example, a main contactor, a magnetic clutch or an electrically operated hydraulic valve.

Machine secondary control element (MSCE)

A machine control element, independent of the primary control element(s), that is capable of removing the source of power from the prime mover of relevant hazardous parts. This can be, for

example, a main contactor, a magnetic clutch or an electrically operated hydraulic valve. When fitted, a MSCE is normally controlled by the Secondary Switching Device (SSD).

Final Switching Device (FSD)

The component which, when signaled by the OSSD going to the OFF state, responds by interrupting the circuit connecting the machine control system to the machine primary control system.

Secondary Switching Device (SSD)

A device which, in a lock-out situation, performs a back up function by going to the OFF state, and initiating an appropriate machine control action - e.g. de-energizing the machine secondary control element (MSCE).

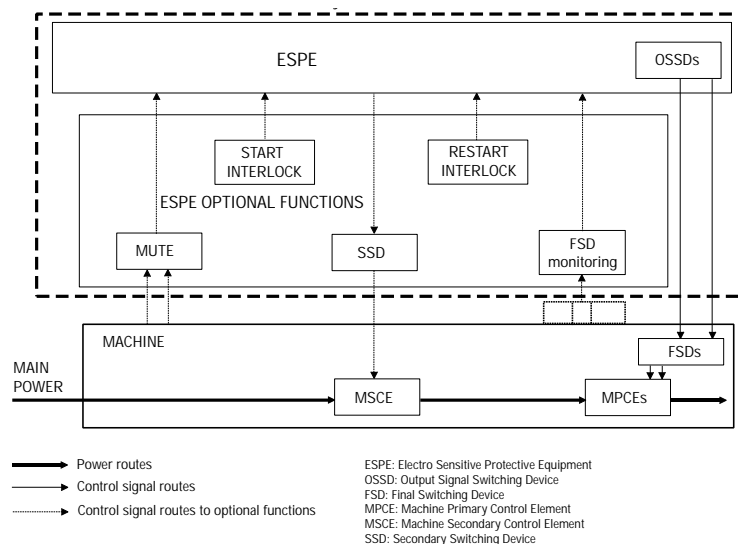
Normally Closed (NC) Contacts

Contacts which are closed in the “rest” (or un-energized) state. External actuation forces them open, breaking the circuit.

Normally Open (NO) Contacts

Contacts which are open in the “rest” (or un-energized) state. External actuation forces them together, initiating the circuit.


Diagram VI.1



Safety techniques (continued)

Common Safety techniques

1. Positive Opening

Positive opening safety switches use a contact rod directly linked to the actuator through a rigid mechanical link. In the case of a weld in the contacts, the action of the actuator will mechanically break the weld, opening the contact safely. Positive opening switches are represented with the symbol .

All of Honeywell’s electromechanical safety switches employ positive opening. Individually these products offer an efficient level of safety, and may be connected individually or in pairs to a variety of control circuits. They comply with all necessary safety standards.

2. Safety Mode

Sensing and Switching devices normally operate in one of 2 modes.

- **In negative mode** a signal is generated only on detection. Some internal fault could lead the safety contact not to open, bringing about a potential dangerous situation. (For example: A broken wire in an electric contact mat). In the absence of a signal, no distinction can be made between a fault in the sensor or no presence in the detection field.

- **In positive mode** a signal is permanently emitted and a detection causes an interruption. Furthermore, any internal fault - such as defective light source, cut wire, etc. - will cause the machine to stop.

Hence it can be seen that equipment installed in positive mode offers a greater assurance of safety than in the negative mode. This is illustrated in the diagram VI.2.

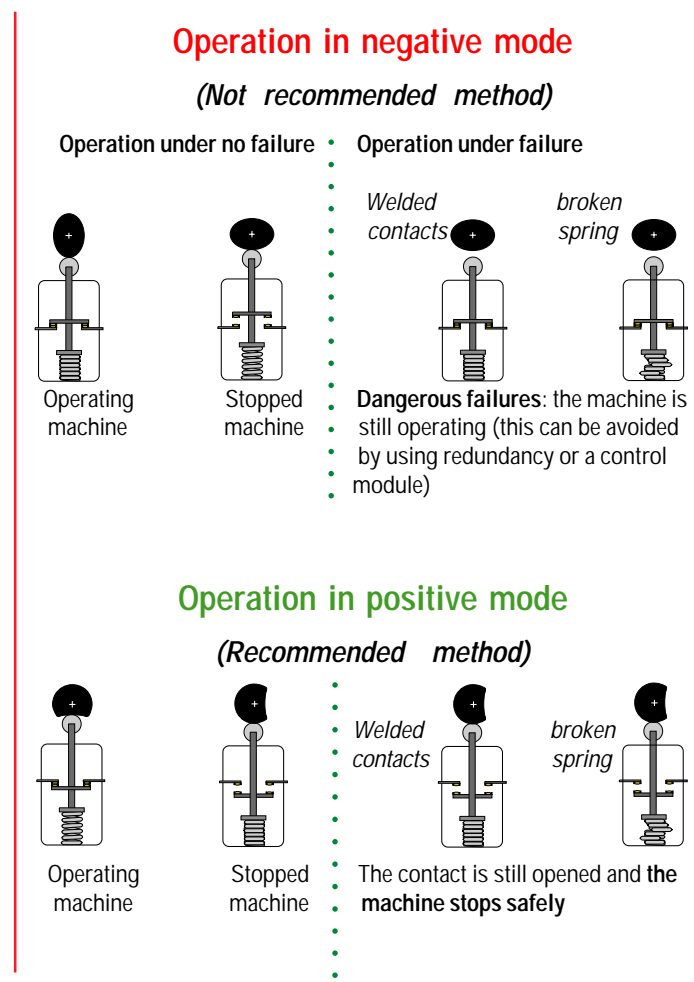


Diagram VI.2

3. Mechanically linked safety relay contacts

In Safety Relays, NO and NC contacts can be associated to increase safety. The mechanical link between the contacts makes any simultaneous closing of the NO and NC contacts impossible in the event of any welds, as the diagram VI.3 and VI.4 demonstrate. **All of Honeywell's relays employ this technique.**

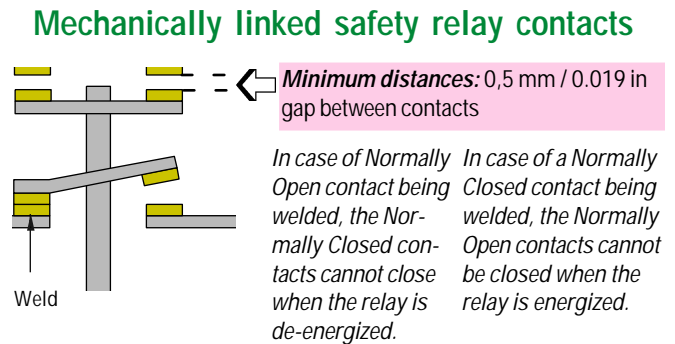


Diagram VI.3

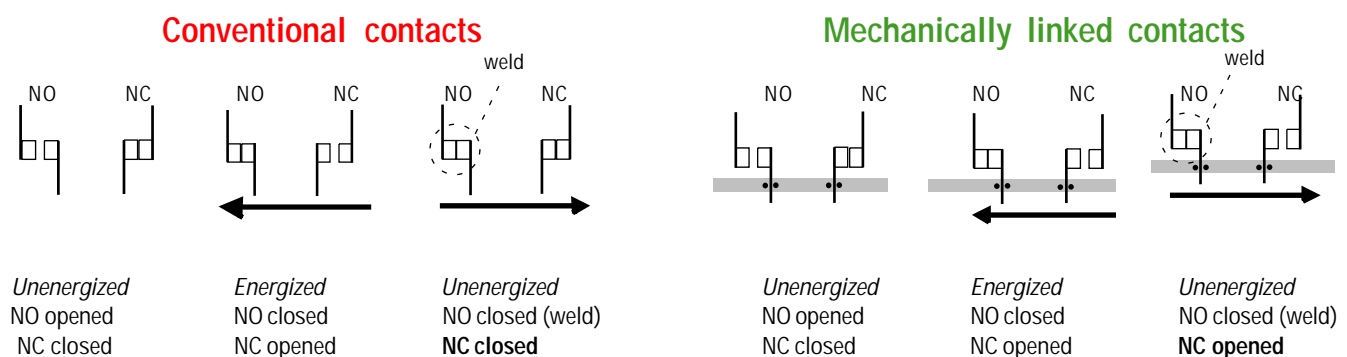


Diagram VI.4

4. Start/Restart Modes

Safety control systems have three possible restart modes:

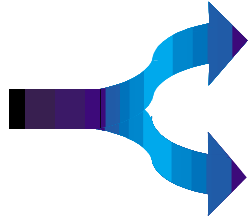
- Automatic mode - turning the equipment on and off after any interruption and release automatically resets it.
- Start and Restart Interlock - at start up and after any interruption and release, a manual reset must be done, normally with a push-button.

Honeywell safety equipment can operate in either mode. An optional mode is offered on some of our products:

- Start Interlock - where the system is only operational at power-up after an external push-button has been activated. It starts again automatically after each interruption and release.

5. Redundancy

Redundancy is often used in safety control circuits. Since it is highly unlikely that two components will fail at the same time, it is safer to double some devices or functional chains. This may be active or passive.



- **Active** means that all redundant means are simultaneously active. This offers a greater guarantee of safety.
- **Passive** means that only a portion of the means is operating, the remainder being called in only in the event of failure.

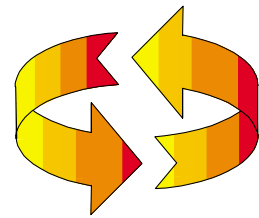
Note: Passive redundancy has benefits in terms of machine uptime but only active redundancy offers a real improvement in safety.

Active redundancy is essential for designing Category 3 or 4 controls per EN 954-1.

To avoid external factors causing both channels to fail at the same time (e.g. vibration, corrosion, radio frequency interference), diverse redundancy can be used. Here a different technology or component is used on each channel. For example, door monitors may use a pair of switches, one in positive mode, one in negative mode, to avoid both failing simultaneously. This prevents for example a broken cam to fail triggering both switches.

6. Self-checking

A self-checking function permits automatic verification of the proper operation of each safety component.



Devices which change condition with each cycle are checked to detect any failure or malfunction. If a failure is detected during self-check, the machine stops, preventing the next cycle. **Cyclical** self-checking is used to guarantee a Category 2 control per EN 954-1. **Permanent** self-checking can be used to reach Categories 3 and 4 per EN 954-1.

7. Redundancy and self-checking

The association of these two techniques permits the detection of faults through self-checking, and also an assurance that safety is maintained after a first failure, through redundancy. Together, they make a Category 4 safety system per EN 954-1.

Redundancy should include the final switching devices, aligning the safety category of the control system with that of the safety component. If there is a fault in one of the channels of a dual channel safety system, it is detected through self-checking.

Safety techniques (continued)

8. FSD (Final Switching Device) loop

An FSD loop allows for the control of external contactors controlled by the safety device. The control unit may offer a self-diagnostic output that gives information on the condition of the internal relays and the condition of the controlled contactors.

9. Electrical interfaces

Machine controls have to be designed to match the same safety level as the electrosensitive protective equipment. This assures the hazardous motion is stopped if the detection function is activated.

Four standards apply to the design of circuits to support this:

- EN 954-1: Safety related parts of control systems
- EN 60204-1: Electrical equipment of machines - general requirements
- EN 60947-5-1: Low-voltage switchgear and controlgear. Part 5: Control circuit devices and switching elements - Section 1: Electromechanical control circuit devices
- EN 61496-1: Electrosensitive protective equipment - general requirements

In addition any Type C standards if they exist for your machine and ANSI B11.20 in the USA.

10. Test input

In order to increase the reliability of detection on some devices, a **cyclical test initiated by the machine and managed by the control unit** is often used to increase safety. This verifies the operation of the emitting and receiving modules as well as the control circuits of the machine. A test input is compulsory on Type 2 products which are tested cyclically. On Type 3 or Type 4 products, the test input is not needed to test the product itself, but together with the

FSD loop, the test controls the **proper operation of the external relays or of the external contactors.**

11. Hard guards

Electrosensitive protective equipment or pressure sensitive devices are sometimes insufficient and the operators may find themselves in a dangerous zone. This can be avoided **by forcing them to be in the detection area.** The simplest way to do this is to install additional forms of protection to the safety systems for channelling people into the detection area. **The goal is to have no access to the dangerous zone except through the detection area.**

Normally, hard guards are used as per EN 294 and EN 811. These are either fixed or automatically controlled in position. In the latter case the operator should not be able to defeat the sensors or switches associated with the screens. Normally they are interlocking devices as defined under EN 953 and EN 1088.



In the picture we see the example of a safety system installed on a robotic line in the automobile industry. It is possible to see the additional forms of protection fixed on the side of the assembly line, which prevents the operator passing outside the protected zone (addition of red plastic pieces on the sides of the automated line).

Minimum authorized spaces on the sides are laid out by standards EN 294 and EN 811.