MACHINES PART III

CONTROL SYSTEMS

Control systems must be designed and constructed so that they are safe and reliable, in a way that will prevent a dangerous situation arising, above all they must be designed and constructed in such a way that: -

A. They can withstand the rigours of normal use and external factors

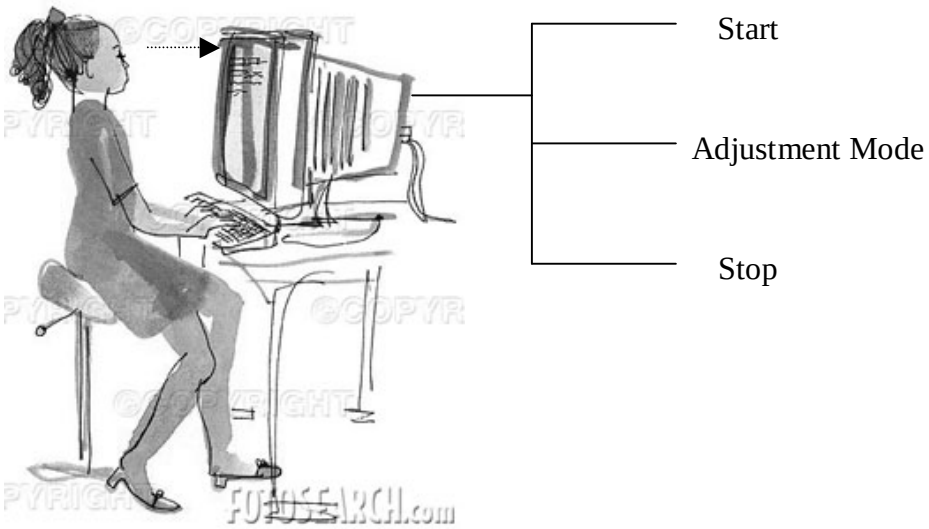
B. Errors in logic do not lead to dangerous situations

Similarly, the control devices must be: -

- Clearly visible and identifiable
- Appropriately marked
- Positioned for safe operation without hesitation or loss of time and without ambiguity
- Designed so that the movement of the control is consistent with it's effect
- Located outside of the danger zones
- Positioned so that their operation cannot cause additional risk
- Designed or protected so that desired effect, where a risk is involved, cannot occur without an intentional operation
- Made to withstand foreseeable strain

Emergency stop switches and robot training controls can be within the danger zone.

Where a control is designed and constructed to perform several different actions, i.e. where there is no one-to-one correspondence, e.g. keyboard and PC, the action to be performed must be clearly displayed and subject to confirmation.



Controls should be arranged that their layout, travel and resistance to operation are compatible with the action to be performed taking account of ergonomic principles. Constraints due to necessary or foreseeable use of personal protective equipment must be taken into account, e.g. if heavy gloves are worn, can the operator safely select the required action without causing a dangerous situation?

Machinery must be fitted with indicators and dials as required for safe operation, e.g. speeds, temperatures, loads etc.

The operator must be able to ensure that there is no exposed person within a danger zone before machinery is started. In some cases this is not possible due to the physical nature of the equipment and in such circumstances the control system must be designed and constructed so that an acoustic and/or visual warning signal is given whenever the machinery is about to start.

The exposed person must have time and the means to take rapid action to prevent the machinery starting up.

An example of this scenario is where an operator is carrying out adjustments to a portion of the machine, hidden from another operator about to start the machine.

There are three possible safety controls for this situation, namely: -

1. A safe system of work, i.e. a lock out/tag out procedure is in place. A draw back of this system if work is that it must be strictly supervised and requires a large administrative input by several people.

2. Audible and visual alarms are positioned with easily identifiable sounds/lights to warn of the impending start(e.g. 5 seconds). One draw back of this system is where several machines are located in close proximity to each other, each having numerous stopping and starting actions. Confusion can lead to a misinterpretation and evasive action not taken.

3. Emergency stop buttons or pull cords are located within the danger zone and within easy reach of the operator (EN 418)

The approach to be taken depends on the various specific problems or hazards presented by a machine. A risk assessment, carried out as per EN 1050 will provide the answer.

Later on in this part of the module, we will look in detail at a further risk assessment that must be carried out, namely under EN 954-1/1A.

STARTING DEVICES

It must be possible to start machinery only by voluntary activation of a control provided for that purpose.

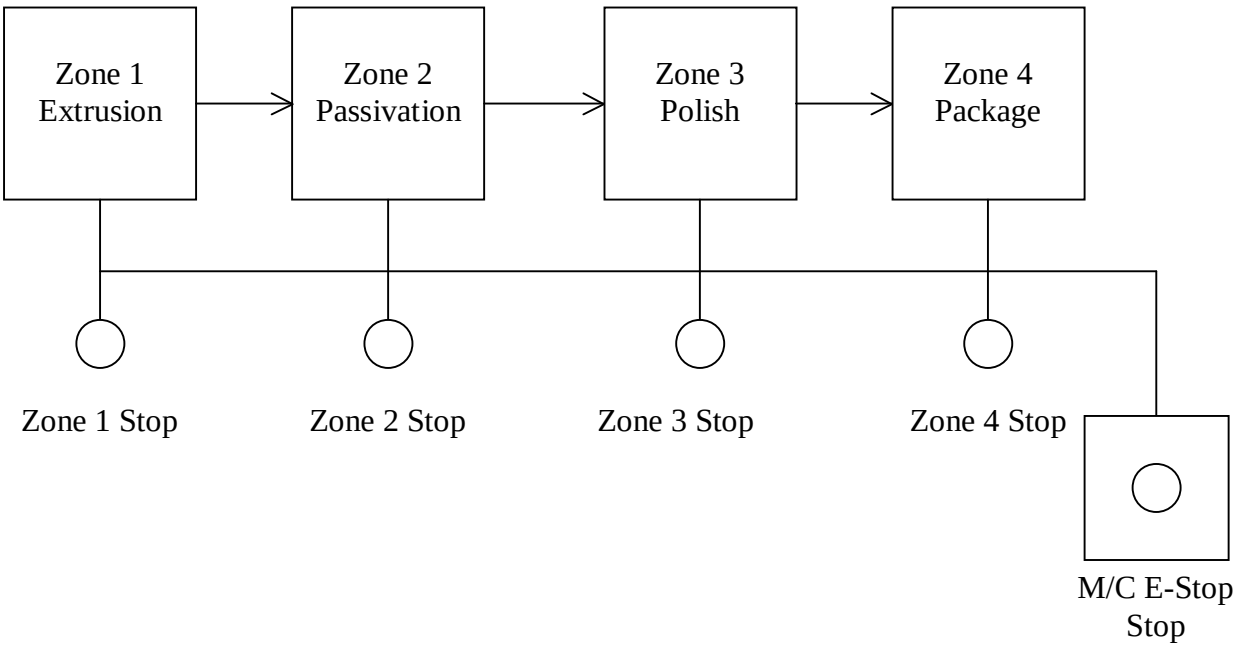
Where machinery has several starting controls and the operators can therefore put each other in danger, additional devices, e.g. enabling devices, selectors etc. allowing only one part of starting mechanism to be activated at any one time must be fitted.

STOPPING DEVICES

Each machine must be fitted with a normal stopping control whereby the machine can be safely brought to a safe stop.

Each workstation must be fitted with a control to stop some or all of the moving parts of the machinery.

The example of this can be seen in a process line, for the manufacture of medical devices, where each zone carries out a different task to the medical device.



The machinery stop controls must have priority over the start controls and one the machinery or its dangerous parts have stopped, the energy supply to the activators must be cut off.

In some cases it may create a more hazardous situation if the energy supply is removed from activators, e.g. where a pneumatic cylinder is holding a heavy roll of steel or fabric and the removal of that energy allows the lifting arm to slowly drop.

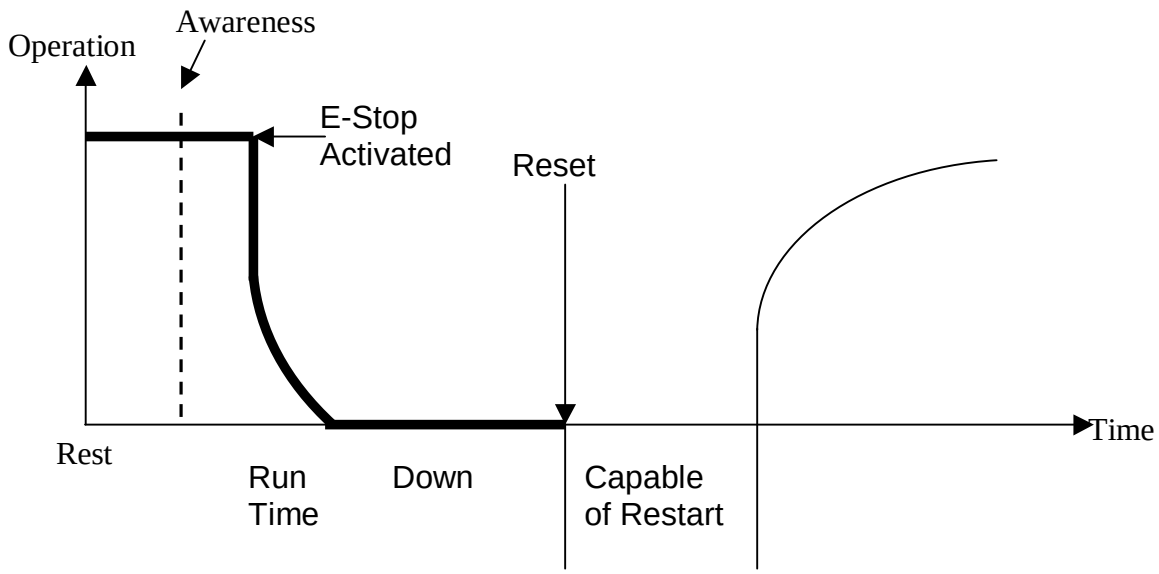
Each machine must be fitted with one or more emergency stopping devices [EN 418] to enable actual or impending danger to be averted.

Once the emergency stop had activated that stop command must be sustained by the engagement of the emergency stop device until that engagement is specifically overridden.

It must only be possible to disengage the device by a positive action, e.g. twisting and pulling the red button, or, holding a triggering switch whilst re-tensioning the cord.

Disengaging of the device must not restart the machinery but only permit restarting.

The functional aspects of an emergency stop control can be seen in the Figure below.



MODE SELECTION

The control mode selected must override all other control systems with the exception of the emergency stop.

An example of the control mode would include: -

- Jogging
- Operation
- Automatic
- Manual
- Maintenance

Each of these modes presents a different hazard and as such when any one of these is selected the selector switch must be capable of being locked into that position.

An example of this is that of an automatic robot, carrying out repetitive work such as removing products from a blow-moulding machine, turning them to facilitate the burning of excess material.

At some time or another, depending on the change of product designs, the robot will have to be 'trained' to pick and place at a specified position. This requires the technician to be in close proximity with the robot in order to carry out the necessary arm movements.

Under the normal automatic or operating mode, the gates to the enclosure, housing the robots are locked so that entry cannot be gained to the moving 'sightless' robot.

The technician can select the '**maintenance mode'**, which allows him to enter the enclosure and operate the robot from a pendant isolated beside same.

In order to carry out this mode change, the technician must remove a captive key from the mode switch, thus no third party can change the mode setting, and only the technician can reset the mode by inserting the key.

Whilst within the danger zone, the technician has four safety controls, namely: -

1. In the maintenance mode, the robot can only operate at a maximum of 10% of the normal operating speed.

2. An emergency stop(s) are within easy reach of the technician

3. The automatic control mode is disabled

4. A two handed sustained control is required. I.e. should the operator remove either of his hands from the pendant, the machine stops.

Other safety controls may have to be implemented, however, these can only be identified through risk assessment.

FAILURE OF THE POWER SUPPLY

The interruption and reestablishment in whatever manner of the power supply to the machinery must not lead to a dangerous situation, in particular: -

- The machinery must not start up unexpectedly (EN 1037)
- The machine must not be prevented from stopping if the command has already been given
- No moving part of the machinery or piece held by the machinery must fall or be ejected (robot or vacuum lift)
- Automatic or manual stopping of the moving parts must be impended
- The protection devices must remain fully effective (EN 60204)

FAILURE OF THE CONTROL CIRCUIT

Should there be a failure of the control circuit, the requirements for the machine are the same as that, had there been a failure of the power supply.

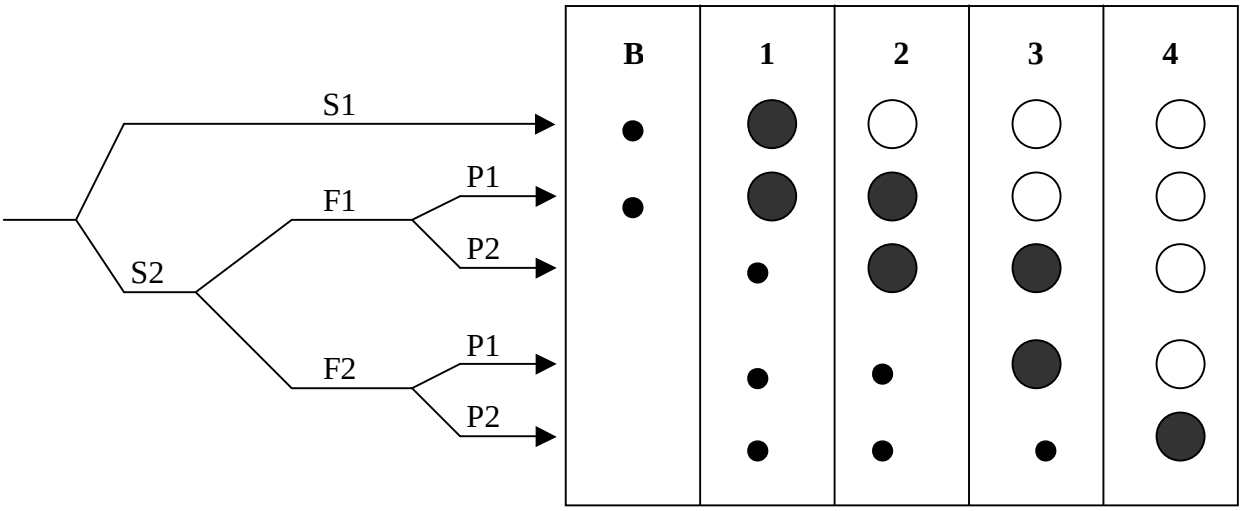
Where a control system fails it is imperative to understand the consequences, particularly, where the integrity of the safety components are concerned.

A guide to the safety related parts of control systems can be found in EN 954-1/1A and under this document it is essential the Category of safety determined.

There are essentially five Categories of safety, namely: -

Category B	(minor)
Category 1	
Category 2	
Category 3	
Category 4	(Major)

To determine into which category the machinery falls into, a risk assessment is required on behalf of the manufacturer or the person who places that machine into service.



Preferred Categories

Possible Categories, which can require additional measures

Over dimensioned measures relevant to the risk

S = Severity of Injury
S1 = Slight injury (normally reversible) cut or braise
S2 = Serious injury (normally irreversible) including death

F = Frequency and/or exposure time to the hazard
F1 = Seldom to quite often and/or the exposure time is short
F2 = Frequent to continuous and/or exposure time is long.

P = Possibility of Avoiding the Hazard
P1 = Possible under specific conditions
P2 = Scarcely possible

CATEGORY B

In this category a surge fault (interlock defective) can lead to a loss of the safety function.

Components selected should be well tried and tested for the tasks/environment placed upon them.

CATEGORY 1

The occurrence of a fault can lead to the loss of the safety function but the probability of occurrence is lower than for Category B.

The increased reliability of the devices can be checked against life testing results and positive mode operation.

CATEGORY 2

All the requirements of B and 1 above, in addition a safety function test must be carried out which should be performed as the machine starts up and if required periodically during operation.

The safety function check may be automatic or manual and will allow the system to function if no fault is detected.

If a fault is found, the safety check will generate a fault output, which will initiate a safe state whenever possible, most probably at the next start operation.

CATEGORY 3

All of the requirements of B, 1 and 2 apply, however here is that a single fault shall not cause the loss of the safety function.

Should a fault be detected it will not stop the machine but will prevent it from starting at the next cycle.

This does not mean that all faults will be detected, therefore an accumulation of faults could still cause the loss of the safety function, therefore to avoid this, the use of redundant devices is recommended, e.g. a guard monitoring relay.

CATEGORY 4

All the requirements of B, 1, 2 and 3 in addition to the fact that a single fault in any of the safety related parts of the system shall not cause the loss of the safety function.

The single fault must be detected at or before the next demand on the safety system.

Common faults must be eliminated by implementing special features that will identify them.