Safety solutions using Preventa
Safety modules

Safety

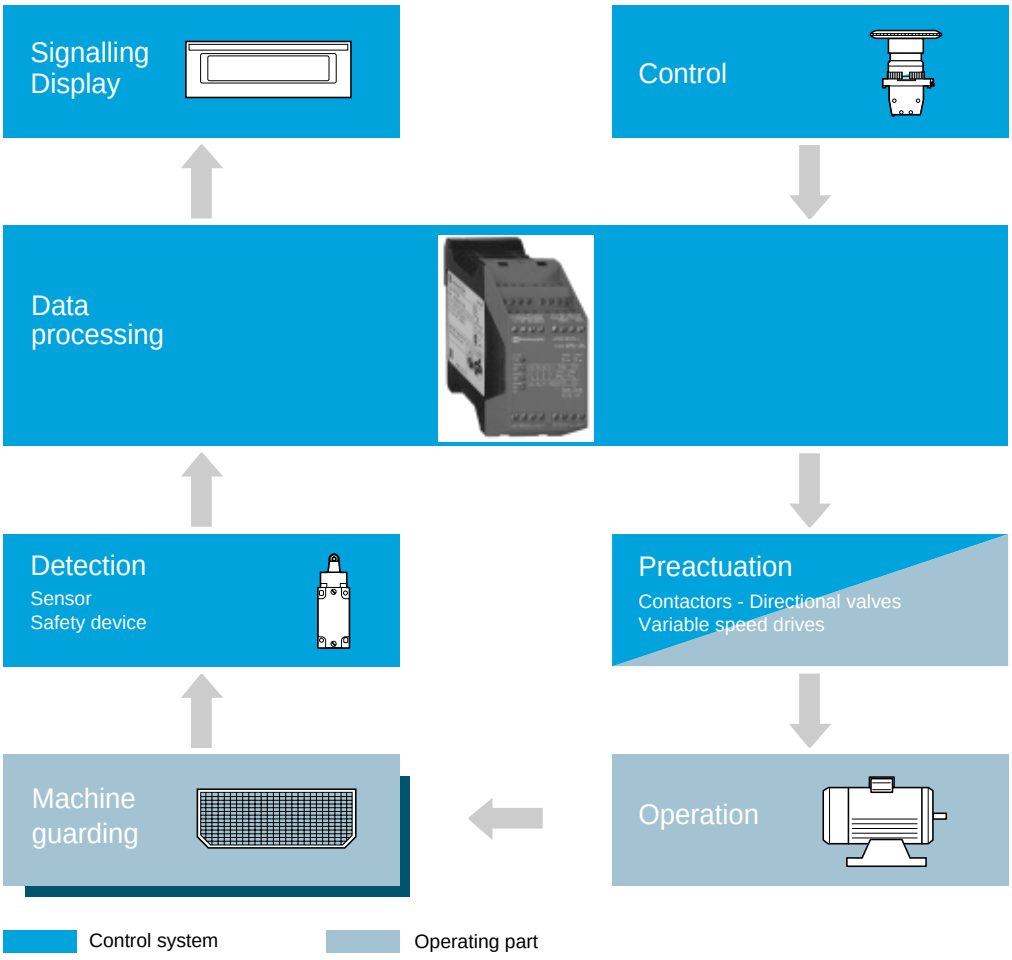
Manufacturing workshops and technical service installations in buildings are increasingly subject to more stringent safety requirements.
Good equipment is **safe** equipment, which combines:
- **safety**: of persons (risk limited to an acceptable level),
- **reliability of operation**: of the production tool (machine always able to perform its function)

Safety is achieved by:
- simultaneously optimising safety and reliability of operation,
- applying fundamental principles: redundancy, self-monitoring,
- making reliability a design consideration (failure causing the machine to react in a specified way, positive safety),
- ease of maintenance

Safety and automated systems

All dangerous areas must be identified and have restricted access, controlled in a secure manner, i.e. any breakdown or careless operation must result in the automation system failing to a non-dangerous position.
It should be noted that the use of safety products alone does not necessarily mean that the machine conforms to the machinery directive.
It is in fact correct operation, wiring, association with other devices and scheme used which make the entire machine safe.
It is more important to think in terms of safety solutions rather than safety products.

General structure of an automated machine



Safety solutions using Preventa
Safety modules

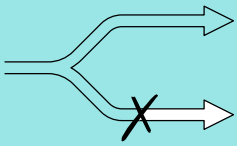
Objective

Detection of initial fault.
Ensure non-dangerous positioning (machine stops in safe state).
Ensure the safety of personnel operating industrial machines.

Basic principles

Redundancy

Consists of compensating for the failure of one component by the correct operation of another, based on the assumption that both will not fail simultaneously



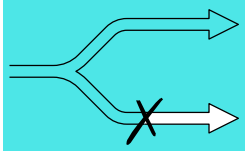
Reliable operation

If an initial fault is undetected, corrective action is not initiated and a second fault may occur thus compromising safety.

Redundancy + Self-monitoring

Redundancy

Consists of compensating for the failure of one component by the correct operation of another, based on the assumption that both will not fail simultaneously

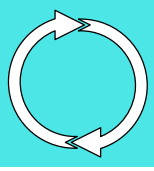


+

Self-monitoring

Consists of automatically checking, at each operating cycle, the operation of any component which changes state.

The next cycle can be inhibited or enabled.



Reliable operation + Safety

An initial fault in the safety circuits is detected before a second fault can occur (next cycle inhibited).

The use of a safety module with redundancy and self-monitoring functions allows a category 4 control system to be built in accordance with standard EN 954-1 (parts of control systems relating to safety).

Definitions

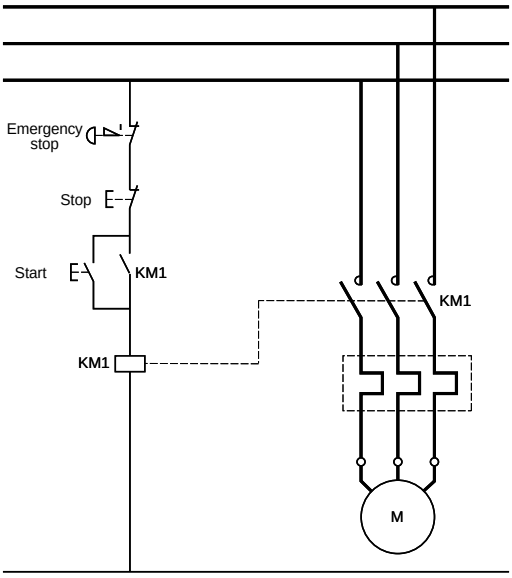
Redundancy function

This function is achieved by providing dual circuits at the design stage, together with a check function which will only permit a control action when at least two output signals are identical.

Self-monitoring function

Safety modules incorporate relays with mechanically linked N/O and N/C contacts.
This technique ensures that all N/O and N/C contacts within each relay remain synchronised.
The self-monitoring function is achieved by checking the correct operation of the linked contact relays which are energised during the current operating cycle.
The method for detecting the failure of a N/O contact in a mechanically linked contact relay consists of checking the correct operation of its N/C contacts which are thus incorporated in the self-monitoring circuit. This is only possible if mechanically linked relay contacts are used.

Operation of the control circuit without interposing relays



The control signal from the protection device (emergency stop in the circuit on the left) acts directly on the power contactor of the device.

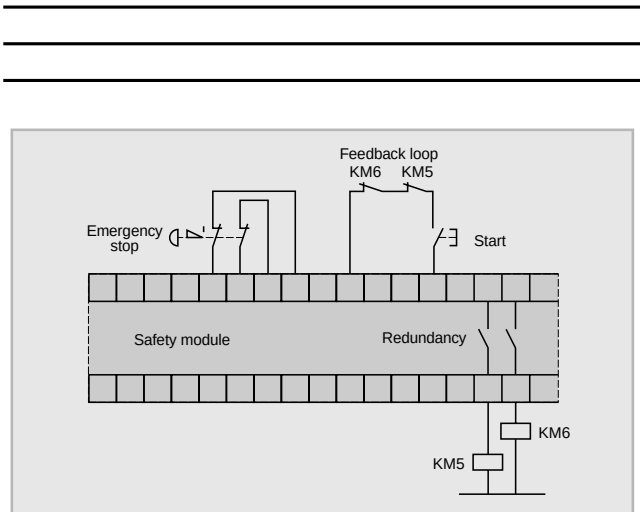
In this type of scheme, there is still a risk of simple faults:
- Emergency Stop button auxiliary contact being shorted out,
- KM1 contactor sticking in.

When the operator presses an Emergency Stop button, the instruction is not processed, and another sequence can begin following the emergency stop, despite the presence of the fault.

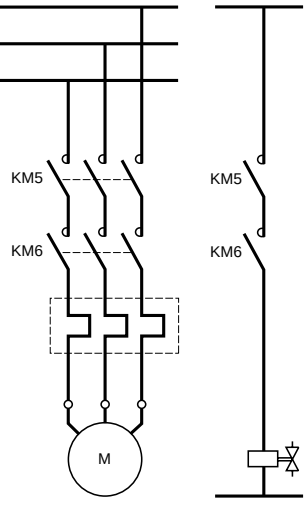
In this type of failure, the safety function (1) is no longer provided. Therefore, a reliable interposing relay system must be used.

(1) A safety function is a function whose non-execution or untimely execution results in immediate placing of the equipment in a non-hazardous condition.

Operation of the control circuit with interposing relays



KM5 and KM6 contactors with mechanically linked contacts



Independent safety circuits

Safety modules provide a reliable interposing relay function by overcoming a number of risks associated with:

- control circuit fault (inputs),
- power circuit fault (outputs),
- safety module internal component fault.

The safety function remains operative whenever any one of these faults occurs.

For the use of mechanically linked contact relays CA2-50 or CAD-32, LC1-D09 or D18 or D25, with contacts which can be used in the feedback loop, please consult your local representative or agent.

Selection criteria

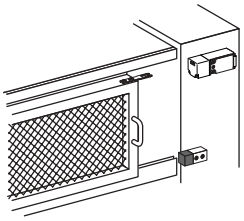
Low risk

Locking or interlocking device based on the principle of intrinsically safe design (tried and tested components and principles).

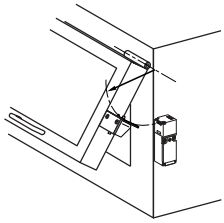
High risk

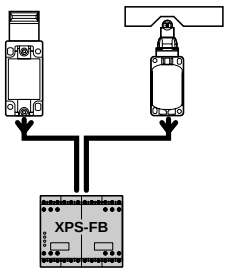
Locking or interlocking device based on the principle of redundancy and self-monitoring.
The safety modules perform both functions.

Machines with instant stopping. Locking
(stopping time < access time) (1)

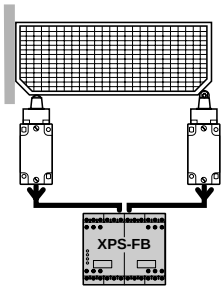


Locking by actuator key

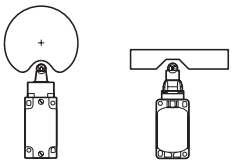




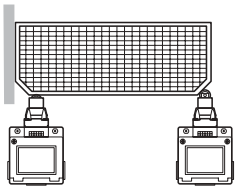
Locking by actuator key and activation in positive mode associated with a safety module



Activation in positive and negative (combined) mode associated with a safety module

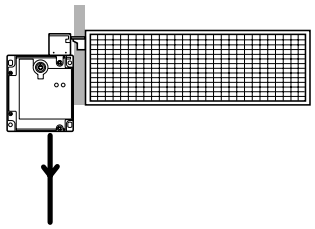


Activation in positive mode

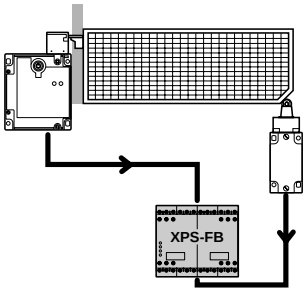


Activation in positive and negative (combined) mode

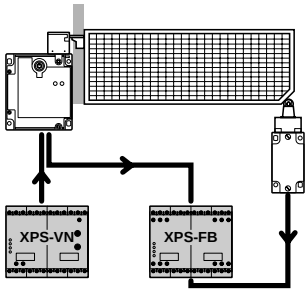
High inertia machines with long stopping times. Interlocking
(stopping time > access time) (1)



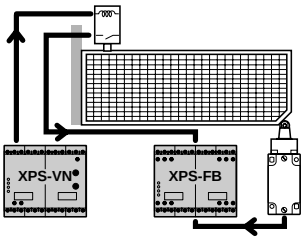
Interlocking device with actuator key captive in the guard



Interlocking device with operating key captive in the guard



Interlocking device with operating key captive in the guard and zero speed detection



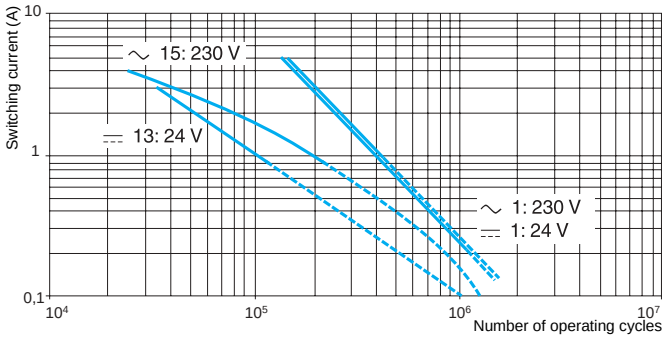
Interlocking device with electromagnetic lock

(1) Stopping time: time elapsed between actuation of the machine stop control and the moment the machine stops (risk eliminated).
Access time: time required for a person to gain access to the hazardous zone (calculated on the basis of an approach speed).

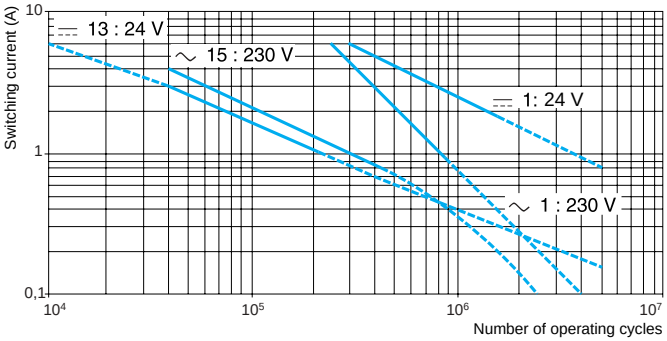
Other configurations Please consult your local representative or agent.

Curves showing electrical durability of safety contacts conforming to EN 60947-5-1, table C2

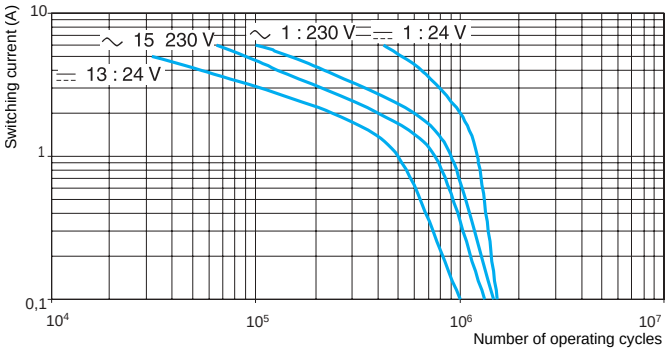
XPS-AL, **XPS-AC**, **XPS-AT** (time delay contacts), **XPS-AX**, **XPS-TSA, XPS-TSW, XPS-BA**, **XPS-BC**, **XPS-CM**, **XPS-DA, XPS-FB, XPS-NS, XPS-OT, XPS-PVK**, **XPS-PVT**, **XPS-VN**



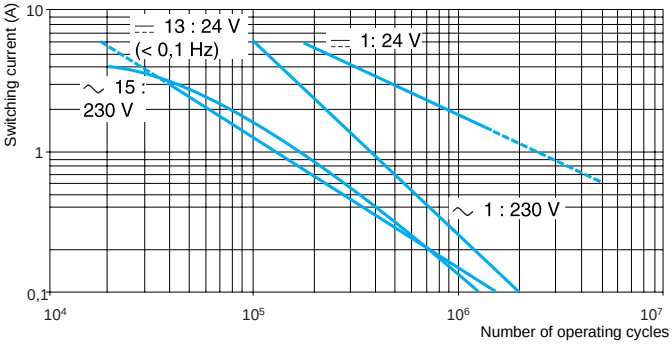
XPS-AT (instantaneous contacts), **XPS-ECM, XPS-ECP**



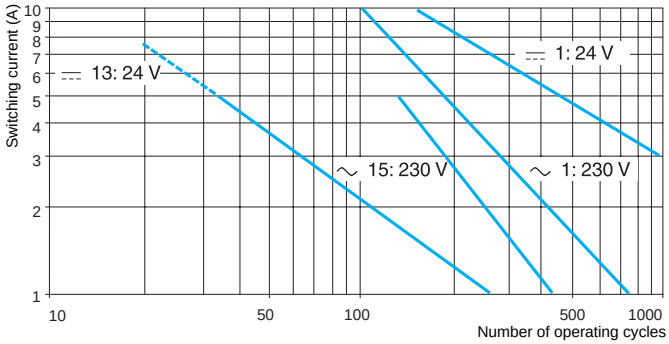
XPS-AF, XPS-AK, XPS-AFL



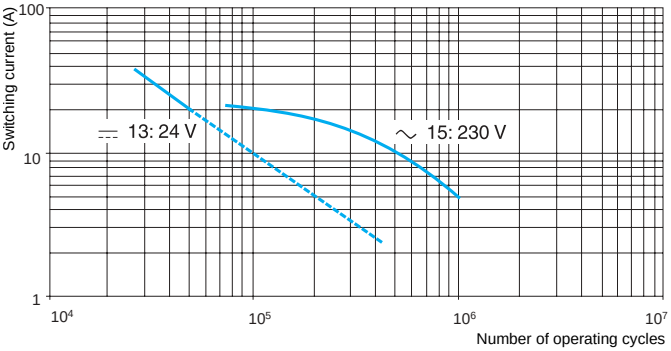
XPS-AV, **XPS-MP, XPS-VC**, **XPS-BF**



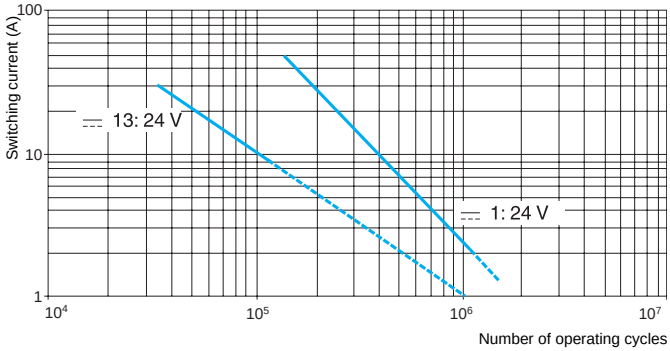
XPS-AR



XPS-DMB/DME



XPS-LMR/LMS



Definition of tests

Determining the electrical durability according to EN 60947-5-1 (table C2)

Type of current	Utilisation category	Start-up			Breaking		
		Current	Voltage	Cos φ	Current	Voltage	Cos φ
a.c. supply	AC-15	10 x Ie	Ue	0.7	Ie	Ue	0,4

Type of current	Utilisation category	Start-up			Breaking		
		Current	Voltage	$T_{0.95}$	Current	Voltage	$T_{0,95}$
d.c. supply	DC-13	Ie	Ue	50 ms	Ie	Ue	50 ms

Ie: Operational current measured.
Ue: Operational voltage measured.
Cos φ: Power factor.
T0,95: Time taken to reach 95 % of rated current.

The tests are carried out with a frequency of 6 switching operations per minute and with no additional protection of the components connected to the safety outputs.
The use of additional protection for the components connected to the safety outputs significantly increases the durability of the safety outputs.

Determining the breaking capacity according to EN 60947-5-1 (table 4)

Utilisation cat.	Start-up			Breaking			Total no. of switching ops.	Switching ops. per minute for 1…1000 switching ops.	Switching ops. per minute for 1001…6050 switching ops.	Minimum duration of switching operation
	Current	Voltage	Cos φ	Current	Voltage	Cos φ				
AC-15	10 x Ie	Ue	0.3	Ie	Ue	0.3	6050	60	6	50 ms

Utilisation cat.	Start-up			Breaking			Total no. of switching ops.	Switching ops. per minute for 1…1000 switching ops.	Switching ops. per minute for 1001…6050 switching ops.	Minimum duration of switching operation
	Current	Voltage	$T_{0.95}$	Current	Voltage	$T_{0.95}$				
DC-13	Ie	Ue	50 ms	Ie	Ue	50 ms	6050	60	6	50 ms

Ie: Operational current measured.
Ue: Operational voltage measured.
Cos φ: Power factor.
T0.95: Time taken to reach 95 % of rated current.

Comments :
The maximum values for the breaking capacity of the safety outputs in the various utilisation categories are not fixed and depend on the power factor and on the switching frequency. The test definition for the “breaking capacity” and “durability” tables in European standard EN 60947-5-1 uses different values for the power factor and the switching frequency.

The power factor (cos φ) in the “breaking capacity” table (0.3) is greater than that in the “durability” table (0.7)

In the "breaking capacity" table, the switching frequency of the safety outputs is higher for the first 1000 switching operations (60 per minute) than that for 1001 to 6050 switching operations (6 per minute).

Consequently, the maximum breaking capacity values determined using the “breaking capacity” table are lower than those in the “durability” table.