The Motor Control Warehouse

Implementing Emergency Stop Systems - Safety Considerations & Regulations

A PRACTICAL GUIDE

V1.0.0

Implementing Emergency Stop Systems - Safety Considerations and The Regulations

Stopping Categories (Safest way the machine should stop when E-Stop button pressed)

Although emergency stops are required for all machines (the Machinery Directive allows two very specific exemptions) they are not considered to be a primary means of risk reduction. Instead they are referred to as a "complementary protective measure". They are provided as a backup for use in an emergency only. They need to be robust, dependable, and available at all positions where it might be necessary to operate them.

EN/IEC 60204-1 defines the following three categories of stop functions as follows: –

Stop category 0: stopping by immediate removal of power to the machine actuators/motors (uncontrolled stop).

Stop category 1: a controlled stop with power available to the machine actuators/motors to achieve the stop and then removal of power when the stop is achieved.

Stop category 2: a controlled stop with power left available to the machine actuators.

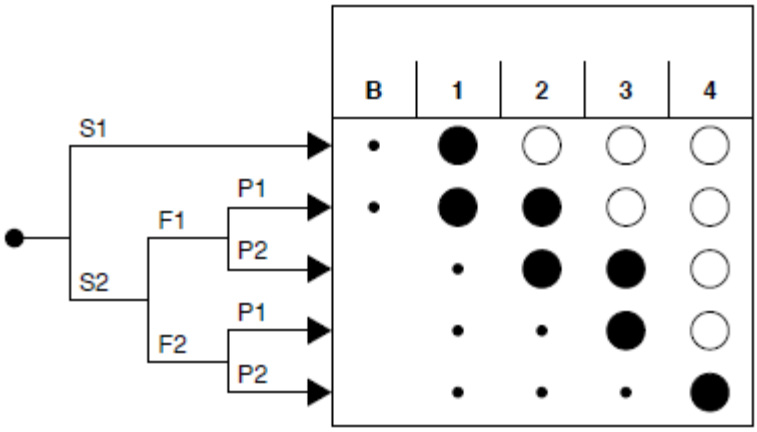
However stop category 2 is not usually considered suitable for emergency stops. Emergency stops on machinery must be "trigger action". This means that their design ensures that however slowly the button is pressed, or cable pulled, if the normally-closed contact opens the mechanism must latch. This prevents "teasing", which can cause dangerous situations. The converse must also be true, i.e. latching must not take place unless the NC contact opens. Emergency stop devices should comply with EN/IEC 60947-5-5.

Emergency Stop Integrity Levels - Standards:

Old Standard – "Integrity Levels" EN954-1:

Users of EN 954-1 will be familiar with the old "risk graph" which many used to design their safety related parts of electrical control circuits to the categories B, 1, 2, 3 or 4.

Please see overleaf -



The user was prompted to subjectively assess severity of injury, frequency of exposure and possibility of avoidance in terms of slight to serious, rare to frequent, and possible to virtually impossible, to arrive at a required category for each safety related part.

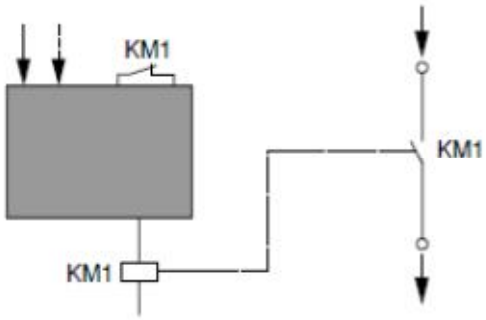
The thinking is that the more the risk reduction depends upon the safety machine control system (SRECS), the more it needs to be resistant to faults (such as short circuits, welded contacts etc).

The behaviour of the categories under fault conditions was defined as follows: -

Category B control circuits are basic and can lead to a loss of the safety function due to a fault.

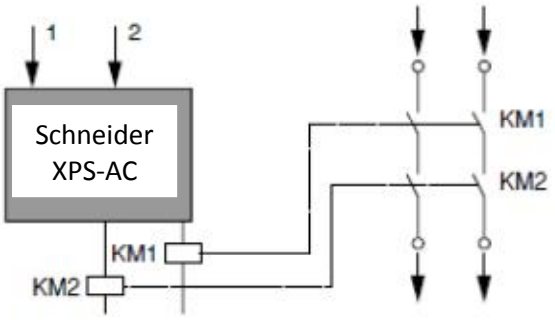
Category 1 can also lead to a loss of the safety function, but with less probability than category B.

Category 2 circuits detect faults by periodic testing at suitable intervals (the safety function can be lost between the periodic tests). Limited redundancy built in.



Typical Category 2 System

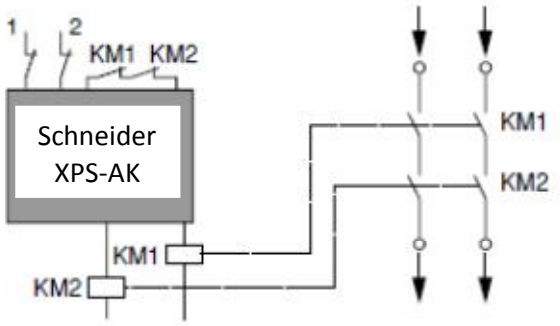
Category 3 circuits ensure the safety function in the presence of a single fault, for example by employing two channels (redundancy) but a loss of the safety function can occur in the case of an accumulation of faults. No feedback loop for monitoring safety relay outputs.



Typical Category 3 System

Example of Category 3 safety relay – Schneider XPS-AC

Category 4 circuits ensure that the safety function is always available even in the case of one or more faults, usually by employing both input and output redundancy, **together with a feedback loop for continuous monitoring of the outputs (KM1 &KM2 normally closed contacts).**



Typical Category 4 System

Example Category 4 safety relay – Schneider XPS-AK

The selection of the safety device (relay) is critical when differentiating between Category 3 and Category 4 emergency stop systems. Considerations are – the particular safety relay's ability to internally monitor itself and to monitor the emergency stop circuit's peripheral devices. (Also, depending which standard is applicable, the mean time to destructive failure and probability of dangerous failure per hour of the safety relay used).

New standards - Performance Levels (PL) and Safety Integrity Levels (SIL) ISO13849-1 & EN62061:

Unlike EN 954-1(Integrity Level) these new standards require consideration of the reliability of the selected components. The PL (Performance Level) PLa, PLb, PLc, PLd and PLe roughly equates to the old "integrity level" B, 1, 2, 3 and 4.

PL and SIL

Safety integrity measures the performance of a safety function. It helps quantify the likelihood of the safety function being achieved when requested. The required safety integrity for a function is determined during risk assessment and is represented by the achieved SIL or PL, depending on the standard used. SIL and PL use different evaluation techniques for a safety function, but their results are comparable and the terms and definitions are similar for both.

The performance of each safety function is specified as either a SIL (Safety Integrity Level) In the case of EN/IEC 62061 or PL (Performance Level) in the case of EN/ISO 13849-1.

Performance Level (PL) ISO 13849-1

Defines how to determine the required Performance Level (PL) and how to verify the achieved PL within a system. PL describes how well a safety system is able to perform a safety function under foreseeable conditions. Five possible PLs are available: a, b, c, d and e. PL 'e' has the highest safety reliability, PL 'a' the lowest.

Safety Integrity Level (SIL) EN 62061

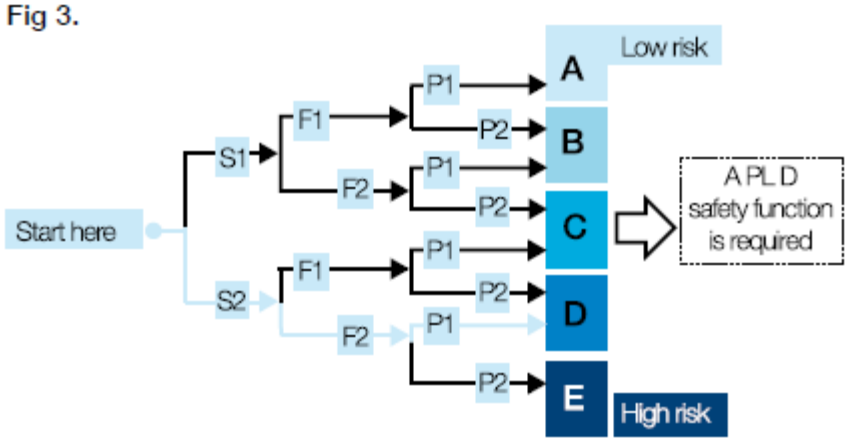
Defines how to determine the Safety Integrity Level (SIL). SIL represents the reliability and integrity of safety functions. Three SIL levels are used in machinery design: 1, 2, and 3. 'SIL 3' is the highest level of safety integrity and 'SIL 1' the lowest.

How to determine the required PL (ISO 13849-1)

To determine the required PL, select one of the alternatives from the following categories and create a 'path' to the required PL in the risk graph (Fig. 3), which lists the resulting performance level as a, b, c, d or e.

Determine the severity of injury/damage: – S1 Slight, usually reversible injury – S2 Severe, usually irreversible injury, including death.
Determine the frequency and duration of exposure to the hazard: – F1 Rare to often and/or short exposure – F2 Frequently to continuous and/or long exposure.
Determine the possibility of preventing the hazard or limiting the damage caused by the hazard: – P1 Possible under certain conditions – P2 Hardly possible. See fig 3

Fig 3.



How to determine the required SIL (EN 62061)

This process is as follows:

1. Determine the severity of the consequence of a hazardous event.
2. Determine the point value for the frequency and duration the person is exposed to harm.
3. Determine the point value for the probability of the hazardous event occurring .
4. Determine the point value for the possibility of preventing or limiting the scope of the harm.

Probability of occurence of harm

Fr Frequency, duration		Pr Probability of hazardous event		Av Avoidance	
<= hour	5	Very high	5		
> 1h <= day	5	Likely	4		
> day <= 2 wks	4	Possible	3	Impossible	5
> 2 wks <= 1 yr	3	Rarely	2	Possible	3
> 1 yr	2	Negligible	1	Likely	1
					Total: 5 + 3 + 3 = 11

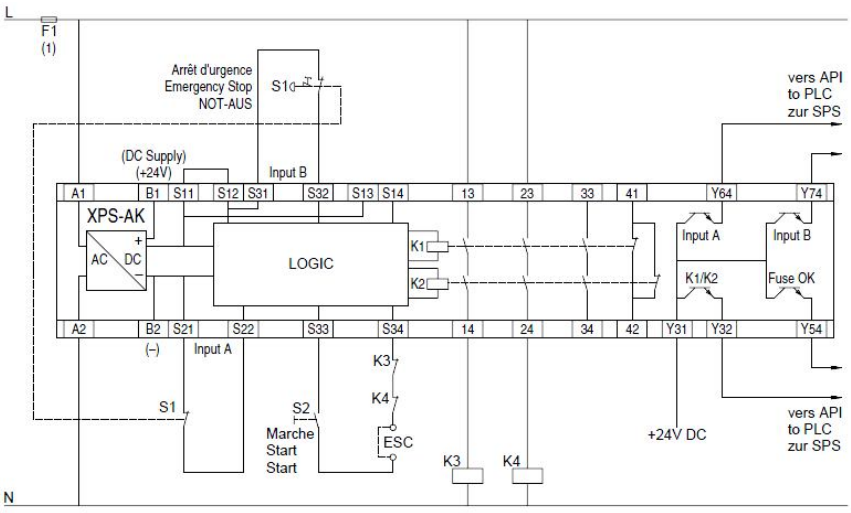
Severity of harm		SIL Class				
Se				Class Cl		
Consequences (severity)		3-4	5-7	8-10	11-13	14-15
Death, losing an eye or arm	4	SIL2	SIL2	SIL2	SIL3	SIL3
Permanent, losing fingers	3			SIL1 →	SIL2	SIL3
Reversible, medical attention	2				SIL1	SIL2
Reversible, first aid	1	Other measures				SIL1
						SIL2 safety function is required.

Typical Safety Relay Characteristics

Schneider XPS-AK

- Safety level - Can reach **PL e/category 4** conforming to EN/ISO 13849-1
- Can reach **SILCL 3** conforming to EN/IEC 62061. (SIL CE, SIL Claim Limit)

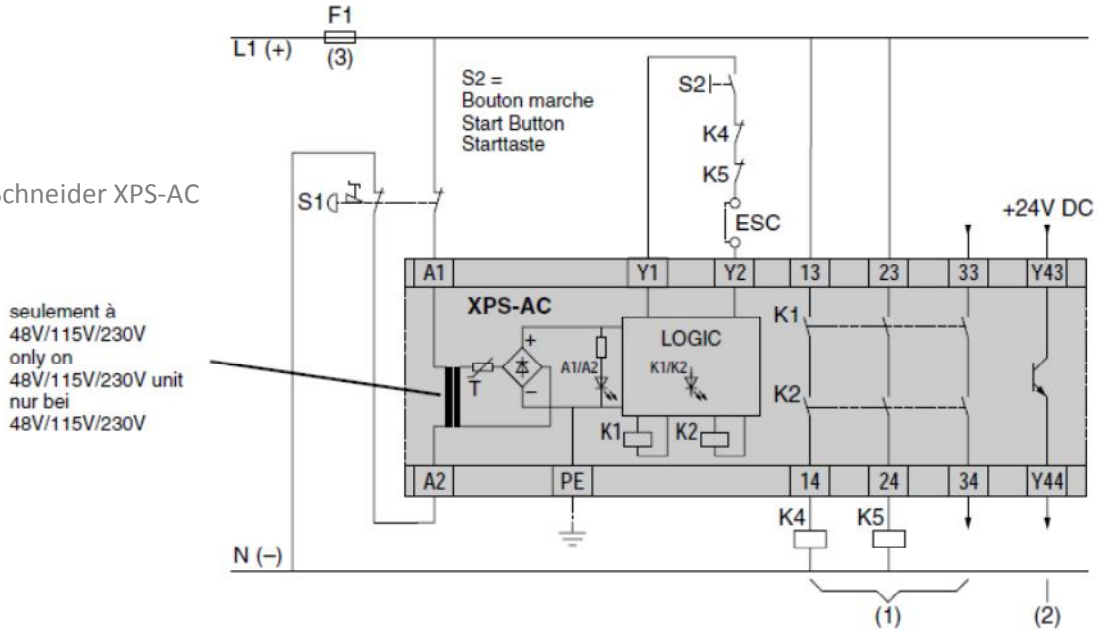
Schneider XPS-AK



Schneider XPS-AC

- Safety level - Can reach **PL e/category 3** conforming to EN/ISO 13849-1
- Can reach **SILCL 3** conforming to EN/IEC 62061 (SIL CE, SIL Claim Limit)

Schneider XPS-AC



Considerations when Designing and Implementing a High Integrity / High Performance Level, E-Stop Circuit

Emergency Stops Basics

1. Emergency stop devices shall be easy to reach and be accessible from all directions
2. Emergency stop devices shall end a dangerous state as quickly as possible without producing additional risks.
3. The emergency stop command shall have priority over all other functions and commands in all operating modes.
4. Resetting the emergency stop device shall not trigger a restart.
5. The principle of direct actuation with mechanical latching function shall be applied.
6. The emergency stop shall be made as per stop category 0 or 1 as described above in this document.

Emergency switching off

1. If there is a possibility of hazards or damage due to electrical power, emergency switching off should be provided. Here the supply of power is shut down using electromechanical switch gear, mains isolator.
2. It shall only be possible to switch on the supply of power after all emergency switching off commands have been reset - turned on.
3. As a result, emergency switching off gives stop category 0.

Re-setting an E-Stop Device

If a device for use in an emergency is actuated, devices triggered by this action shall remain in the off state until the device for use in an emergency has been reset. The reset of the emergency device shall be done manually at the specific location. The reset shall only prepare the machine to be put back in operation and not restart the machine.

Requirements and forms of implementation of E-Stop devices

The contacts on the emergency stop device shall be positive opening normally closed contacts. The emergency stop device shall be red, any background shall be yellow.

Examples:

1. Switches actuated with mushroom head pushbuttons
2. Switches actuated with wires, ropes or rails
3. Foot switches without covers (for emergency stop)

If wires and ropes are used as actuating elements for emergency devices, they shall be designed and fitted such that they are easy to actuate when pulled or the wire/rope is cut. Reset mechanisms should be arranged in the manner that the entire length of the wire or rope is visible from the location of the reset mechanism.

Implementation and Wiring of E-Stop Devices

1. Devices and wiring systems should be arranged to meet the requirements for survivability, protection against external influences and independence.
2. Independent systems or redundant channels should not share multicore cables with each other or power circuits, and may require diverse routes depending upon the safety integrity level to be achieved. (Category 3 and 4, SIL 3 and PLe).
3. Employ redundancy at every stage of the design, wherever possible. The more redundancy that can be integrated in to the design, the higher the integrity of the system.

Measures to protect against failures include:

1. Cable selection (screening etc.).
2. Protection of cables against fire, chemical attack, physical damage etc.
3. Physical separation or segregation of cables and cable routes.
4. Routing in benign environments.

Colour Codes for Push Buttons and Indication Lamps

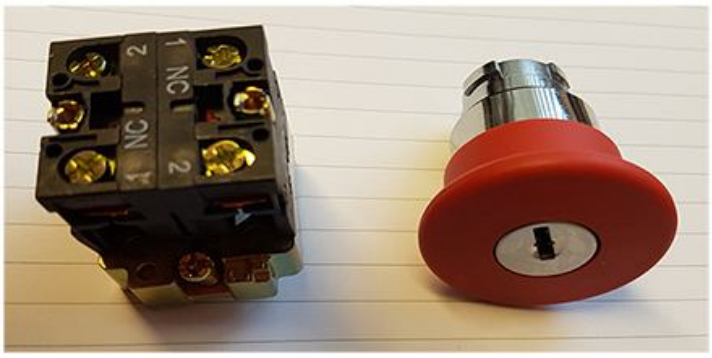
General meaning of the colors for controls

Color	Meaning	Explanation
White Grey Black	Unspecific	Initiation of functions
Green	Safe/Start/ON	Actuate during safe operation or to establish normal situation
Red	Emergency / Stop / OFF	Actuate in hazardous situation, emergency situations or stop/ off commands
Blue	Instruction	Actuate in situation that requires mandatory action
Yellow	Abnormal	Actuate in abnormal situation

General meaning of the colors for indicators

Color	Meaning	Explanation
White	Neutral	Use in case of doubt on the usage of green, red, blue or yellow
Green	Normal situation	
Red	Emergency	Dangerous state, react with immediate action
Blue	Mandatory	Indicate a situation that required mandatory action on the part of the operator
Yellow	Abnormal	Abnormal situation, Critical situation imminent

Typical Key Release E-Stop Actuator Button



Dual contact block terminals and actuator lock

E-Stop actuator and dual block housing

Contact Block

Glossary:

1. **PL e, Performance Level e (highest level).**
2. **SIL 3, Safety Integrity Level 3 (highest level).**
3. **SILCL 3, Safety Integrity Level - Claim Limit 3 (highest level).**
4. **$MTTF_d$** Mean Time To Destructive Failure.
5. **PFH_d** Dangerous Failures per Hour.

Sources of Information:

1. Safety and functional safety a general guide - ABB brochure 1SFC001008B0201**.**
2. Safety machinery handbook – Schneider Electric.
3. Safebook 4 – Rockwell Automation.
4. Machine Safety in the European Community – Defren / Kreutzkampf
5. Guidelines for safe machinery – Sick Inc.

Motor Control Warehouse

+44 (0)1686 688948

www.motorcontrolwarehouse.co.uk