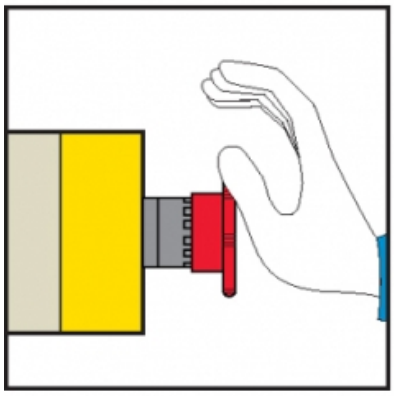
Safety Chain Solution – Safe Stop 0

PL d, SIL 2

Optimized implementation for increased protection



Function:

- Safety-related stop function initiated by the moveable guards designed to protect the access to a hazardous zone.
- The opening of each guard is detected by using two limit switches in combination mode (positive mode + negative mode), which are checked by the safety module allowing detection of the opening or the removal of the protective guard.
- Opening of any of these guards causes the deactivation of the safety module outputs (stop category 0 according to EN/IEC 60204-1), which results in a switch-off of the motor power supply to prevent possible hazardous movements or states by means of the contactors (K1 and K2).
- The main contactors are monitored by the safety module to detect e.g. contact welding, by means of their mirror contacts.

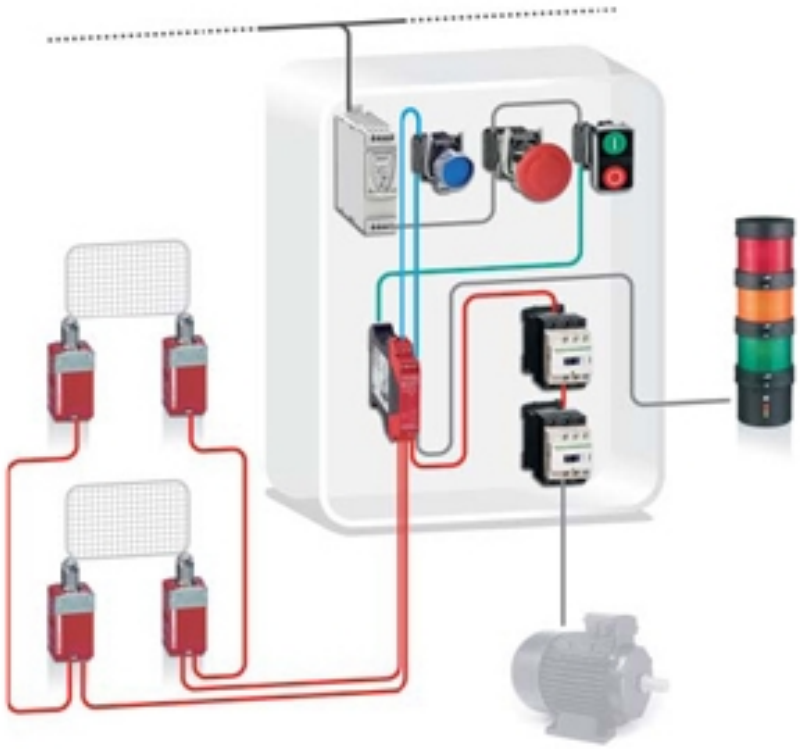
Typical applications:

- Assembling, textile, printing or similar machines where the access to the hazardous area is limited to maintenance interventions.

Safety Chain Solution – Safe Stop 0

Design:

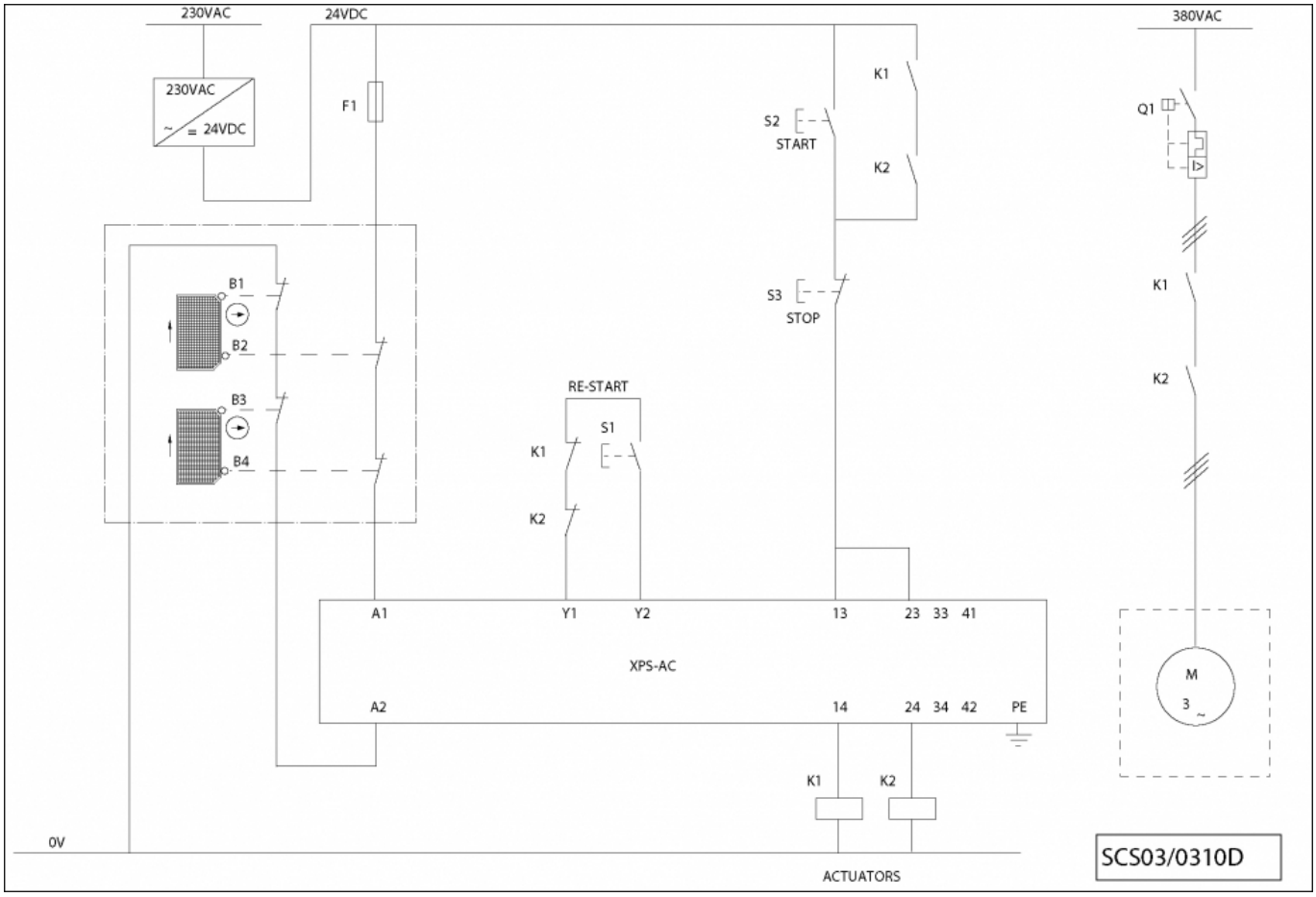
- The safety function employs well-tried safety principles and is robust in the event of one component failure by means of two contactors (K1 and K2) and two limit switches on each guard (B1, B2 and B3,B4).
- A contactor fault is detected by the safety module at the next demand upon the safety function by the restart interlock pushbutton.
- The start (S2) and restart interlock (S1) must be located outside the hazardous area and at a point from which the potential danger is visible.
- The limit switches (B1 and B3) have direct opening action in accordance with EN/IEC 60947-5-1 and are regarded as well-tried components.
- The safety module satisfies the requirements for performance level up to PL e according to EN ISO 13849-1 and SILCL 3 according to EN/IEC 62061.
- The contactors (K1 and K2) have mirror contacts in accordance with EN/IEC 60947-4-1, meaning that the normally closed auxiliary contacts cannot be in the closed state unless the main poles are open. They are also considered as well-tried components.
- Protection against overcurrent must be provided in accordance with EN/IEC 60947-4-1



Related products

- Switches, pushbuttons, emergency stop - Harmony XB4
- Switch mode Power supply - Phaseo ABL8
- Safety Module - Preventa XPSAC
- Safety switches - Preventa XCS
- Contactor - TeSys D
- Modular beacon and tower light - Harmony XVB

Safety Chain Solution – Safe Stop 0



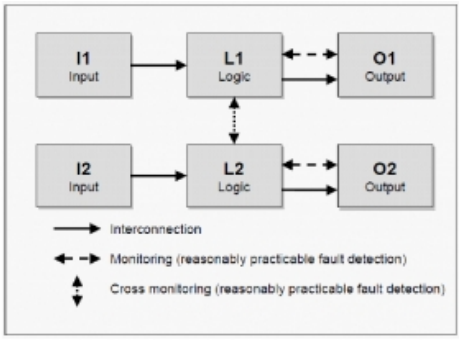


Figure 1

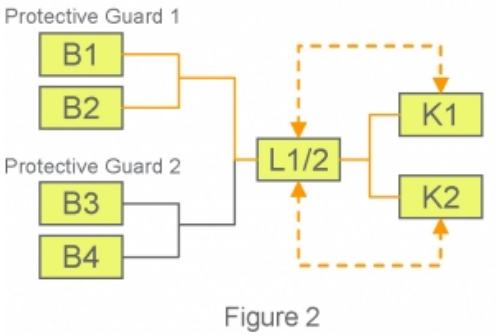


Figure 2

Chain structure:

- The circuit diagram SCS03/0310D is a conceptual schematic diagram and is limited to present the safety function with only the relevant safety components.
- For the designated architecture of category 3, two redundant channels are implemented.
- The circuit arrangement can be divided into three function blocks per channel with the input (I), logic (L) and output (O) blocks on each channel.
- The possibility of fault detection by monitoring the outputs is indicated by the broken lines (see figure 1).
- Since each protective guard forms part of a dedicated safety function, the calculation of the performance level considers only one of them.
- The functional channel can be represented by a single protective guard actuating two limit switches (i.e. B1 and B2) that would correspond to the input (see figure 2).
- The safety module (XPSAC) corresponds to the logic block (L1/L2), which maintains the internal redundancy of the safety circuits required for this architecture.
- The output block is represented by two redundant contactors (K1 and K2) that are monitored by the logic block (safety module) to detect any failure.
- The complete wiring must be in accordance to EN 60204-1 and the necessary means to avoid short circuits has to be provided (EN ISO 13849-2 Table D.4).

Safety Chain Solution – Safe Stop 0

Cycle time (s)	1800
Number of hours' operation per day (h)	12
Number of days' operation per year	220
Number of operations per year (n_{op})	5280

		Values	
		Channel 1	Channel 2
Input devices XCS	B10 (operations)	10 000 000	10 000 000
	% dangerous failure	20	20
	$B10_d$ (operations)	50 000 000	50 000 000
	$T10_d$ (years)	9470	9470
	$MTTF_d$ (years)	94696.9	94696.9
	$MTTF_d$ resulting (years)	100	100
	PFH_d resulting (1/h)	1.01×10^{-7}	1.01×10^{-7}
	DC (%)	60	60
Logic (safety module) XPSAC	PFH_d (1/h)	3.56×10^{-9}	3.56×10^{-9}
Output (actuator) LC1	B10 (operations)	1 000 000	1 000 000
	% dangerous failure	73	73
	$B10_d$ (operations)	1 369 863	1 369 863
	$T10_d$ (years)	259	259
	$MTTF_d$ (years)	2594.4	2594.4
	$MTTF_d$ resulting (years)	100	100
	PFH_d resulting (1/h)	2.47×10^{-8}	2.47×10^{-8}
	DC (%)	99	99
Safety function	$MTTF_{dC}$	**40.4 (high)**	
	DC_{avg} (%)	**83.4 (low)**	
	PFH_d resulting (1/h)	**1.5×10^{-7}**	
	PL attained	**d**	
	SIL attained	**2**	

Safety level calculation:

- A required performance level (PLr) must be specified for each intended safety function following a risk evaluation. The performance level (PL) attained by the control system must be validated by verifying if it is greater than or equal to the PLr.
- At 220 working days per year, 12 working hours per day and a cycle time of 30 minutes, the number of operations (nop) would be 5 280.
- Mean time to dangerous failure (MTTFd) values exceeding 100 years will be limited to this value in order for the component reliability not to be overstated in comparison with the other main influencing variables such as the architecture or tests.
- A B10d value of 50 000 000 cycles is stated for the mechanical aspects of of B1 and B2. In accordance with the assumed nop value, the MTTFd would be 94696,9 years for each component. These values are therefore limited to 100 years ("high").
- A PFHd value of 3.56×10^{-9} is stated for the safety module (XPSAC). This value comes directly from the safety device data and it is certified by an accepted standards body.
- For the redundant contactors K1 and K2, the B10 value corresponds under nominal load to an electrical lifetime of 1 000 000 switching cycles. If 73% of failures are assumed to be dangerous, the B10d value is 1 369 863 operations. With the assumed value for nop, it results in a MTTFd of 2594,4 years for each component. These values are therefore limited to 100 years ("high").
- The combination of channel 1 and channel 2 results in a DCavg of 83,4% (low) as no monitoring exists for the input states.
- Measures against common cause failures (Annex F of EN ISO 13849-1) must attain at least 65 points (i.e. separation (15), overvoltage protection etc. (15) and environmental conditions (25+10)).
- The safety-related control system corresponds to category 3 with high MTTFd. The complete functional safety chain results in average probability of dangerous failure (PFHd) of 1.5×10^{-7}.
- This corresponds to PL d and SIL 2.

SCS03/0310 - 03-03-2010

Schneider Electric Industries S.A.S
Head Office
35 rue Joseph Monier
CS 30323
92506 Rueil-Malmaison
www.schneider-electric.com