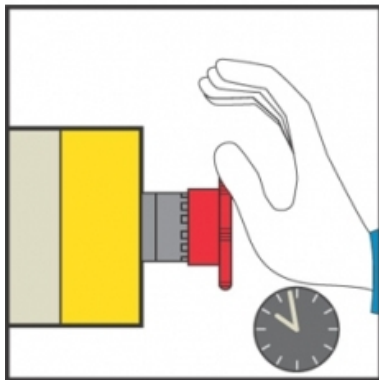


Safety Chain Solution – Safe stop 0 - High performance

PL e, SIL 3

Optimized implementation for increased protection



Function:

- Safety-related stop function initiated by a moveable guard designed to protect the access to a hazardous zone.
- The opening of this guard is detected by using a guard switch, which is checked by the safety module allowing detection of the opening or the removal of the protective guard according to EN1088.
- Opening of this guard 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:

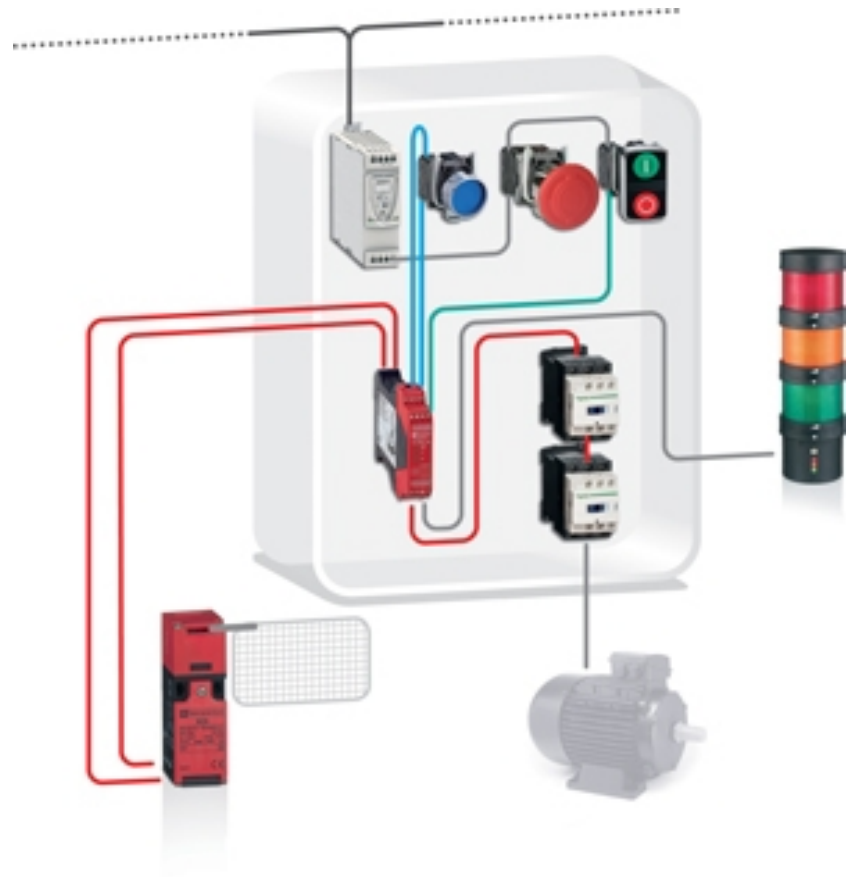
Assembling, machining centers or similar machines tools, where the access to the hazardous area is frequent or with long exposure time.



Safety Chain Solution – Safe stop 0 - High performance

Design:

- The safety function employs well-ried safety principles and is robust in the event of one component failure by means of two contactors (K1 and K2) and a guard switch (B1).
- The contact synchronization of the guard switch and failure of the contactors are detected by the safety module at the next demand upon the safety function by the restart interlock pushbutton.
- The start (S3) and restart interlock (S1) must be located outside the hazardous area and at a point from which the potential danger is visible.
- The guard switch (B1) has direct opening action in accordance with EN/IEC 60947-5-1 and is regarded as well-ried component.
- 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 guided 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-ried components.
- Protection against overcurrent must be provided in accordance with EN/IEC 60947-4-1. The design principles satisfies the machine tools requirements in accordance with EN 12417 for machining centers type C standard.



Related products

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

Safety Chain Solution – Safe stop 0 - High

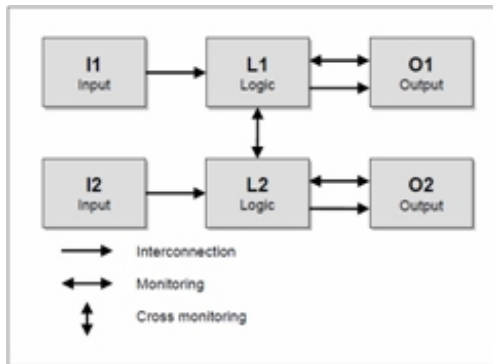
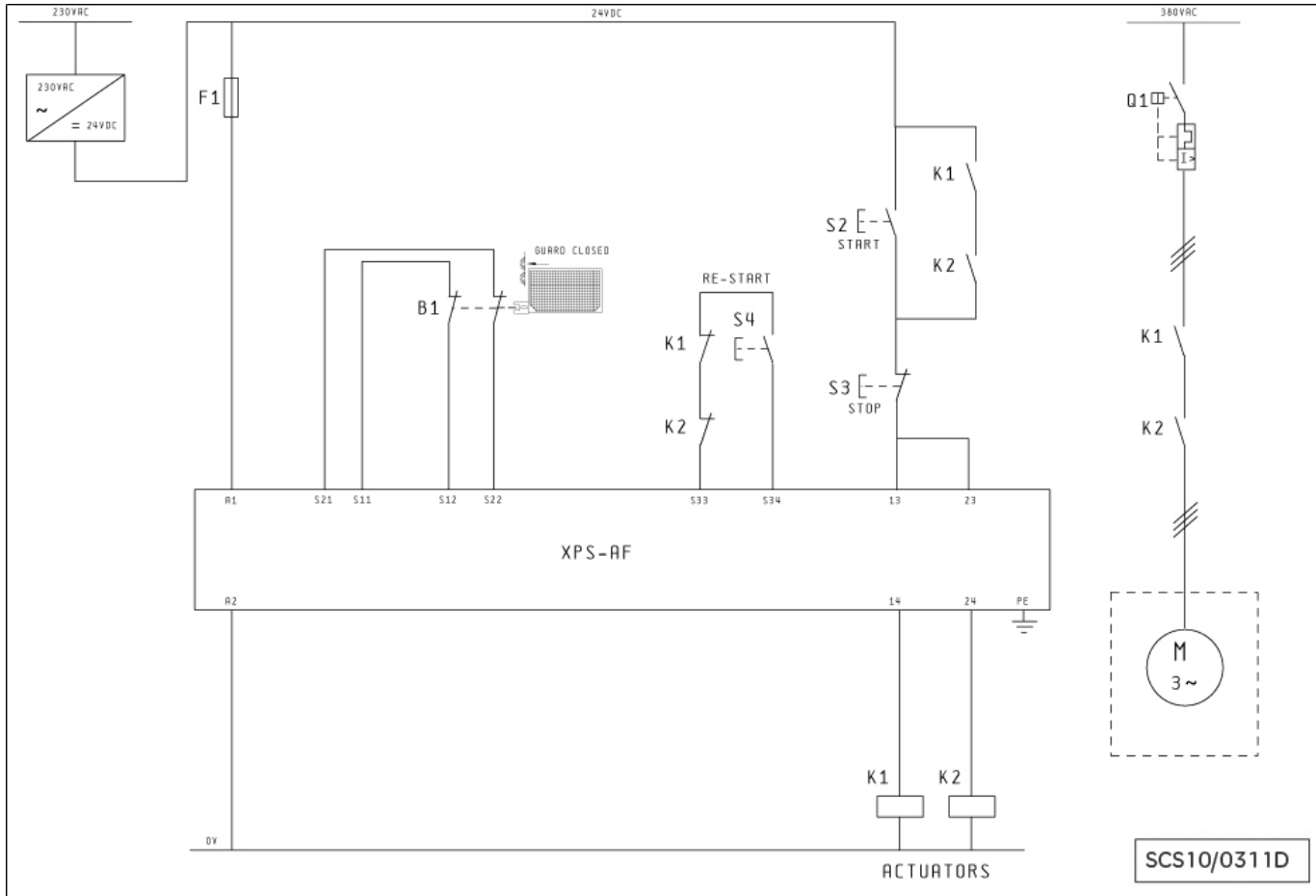


Figure 1

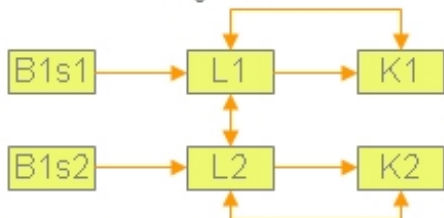


Figure 2

Chain structure:

- The circuit diagram SCS10/0311D 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 4, two redundant channels are implemented.
- The circuit arrangement can be divided into three function blocks, input (I), logic (L) and output (O) blocks, per channel.
- The unbroken lines for monitoring symbolize the higher DCavg assumed for this category (see figure 1).
- The functional channel is represented by the moveable guard switch device (B1) that correspond to the input part by means of two switches s1 and s2 (see figure 2).
- The safety module (XPSAF) 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 - High performance

Cycle time (s)	300
Number of hours' operation per day (h)	12
Number of days' operation per year	220
Number of operations per year (n_{op})	31680

		Values	
		Channel 1	Channel 2
Input (guard switch) XCS	B10 _s (operations)	5 000 000	5 000 000
	T10d (years)	157.8	157.8
	MTTF _s (years)	1578.3	1578.3
	MTTF _s resulting (years)	1578.3	1578.3
	PFH _s resulting (1/h)	1.44×10^{-9}	1.44×10^{-9}
	DC (%)	99	99
Logic (safety module) XPSAF	PFH _s (1/h)	4.62×10^{-9}	4.62×10^{-9}
Output (actuator) LC1	B10 (operations)	1 000 000	1 000 000
	% dangerous failure	73	73
	B10 _s (operations)	1 369 863	1 369 863
	T10 _s (years)	43	43
	MTTF _s (years)	432.4	432.4
	MTTF _s resulting (years)	432.4	432.4
	PFH _s resulting (1/h)	5.35×10^{-9}	5.35×10^{-9}
	DC (%)	99	99
	Safety function	MTTF _{sc}	100 (high)
DC _{avg}		99 (high)	
PFH _s resulting (1/h)		1.14×10^{-8}	
PL attained		e	
SIL attained		3	

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.
- Mean time to dangerous failure (MTTFd) values exceeding 100 years are 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.
- If the protective guard is assumed to be actuated every 5 minutes during 220 working days per year and 12 working hours, the number of operations (nop) would be 31 680.
- A B10d value of 5 000 000 cycles is stated for the guard switch. In accordance with the assumed above nop value, the MTTFd would be 1578.3 years for each channel. These values are not limited in this case as this is category 4 system and they are under the 2500 year limit used by the SISTEMA calculation tool.
- A PFHd value of 4.62×10^{-9} is stated for the safety module (XPSAF). This value comes directly from the safety device data and 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, this results in a MTTFd of 432.4 years for each component. These values are not limited in this case as this is category 4 system and they are under the 2500 year limit used by the SISTEMA calculation tool.
- Measures against common cause failures (Annex F of EN ISO 13849-1) must attain at least 65 points (i.e. separation of wiring (15), overvoltage protection etc. (15) and environmental conditions (25+10).
- Since this is the highest performance level, both the MTTFd of each channel and the DCavg must be high.
- The combination of channel 1 and channel 2 results in a DCavg > % (high) as we are monitoring the guard switch input contacts as well as the mirror contacts of the contactors.
- The safety-related control system corresponds to category 4 with high MTTFd (> 30). The complete functional safety chain results in average probability of dangerous failure (PFHd) of 1.14×10^{-8} .
- This corresponds to PL e and SIL 3.

SCS10/0311 - 17-03-2011

ATTENTION

The information provided in this documentation contains general descriptions and/or technical characteristics of the performance of the products contained herein. This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither Schneider Electric Industries SAS nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein.

Schneider Electric Industries S.A.S

Head Office
35 rue Joseph Monier
CS 30323
92506 Rueil-Malmaison
www.schneider-electric.com

As standards, specifications and designs change from time to time, please ask for confirmation of the information given in this publication.

Design : Schneider Electric
Photos : Schneider Electric