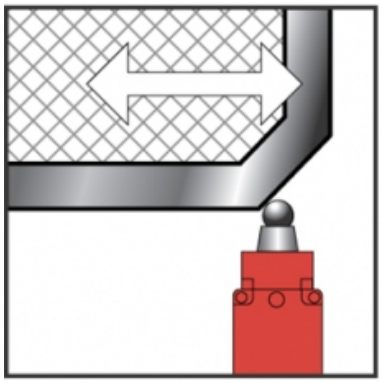
Safety Chain Solution – Multifunction - Safety guard

PL e, SIL 3

Complex machine applications using a centralized safety device



Function:

- Safety-related stop function initiated by a moveable guard that help protects access to a hazardous zone.
- The guard opening is detected by using a solenoid locked switch in combination with a limit switch in positive operating mode, which are checked by the safety module allowing detection of the opening or removal of the protective guard.
- Opening of the moveable guard causes the deactivation of the safety module outputs which results in switching-off the motor power supply by means of the contactors K1 and K2 to help prevent possible hazardous movements (stop category 0 according to EN/IEC 60204-1),
- The motor can be also de-energized when the emergency stop device (S1) is actuated.(*)
- The main contactors are monitored by the safety controller to detect for example contact welding, by means of the mirror contacts.
- The safety controller also monitors the consistent actuation of the limit switch contacts to detect failure, before restart of the machine movement is permitted.

(*) The function for stopping in an emergency is a protective measure which complements the safety functions for the safeguarding of hazardous zones according to EN ISO 12100-2

Typical applications:

- Plastic injection, eccentric press or similar complex machines with 4 or more safety functions included, where a centralized safety controller would be required.

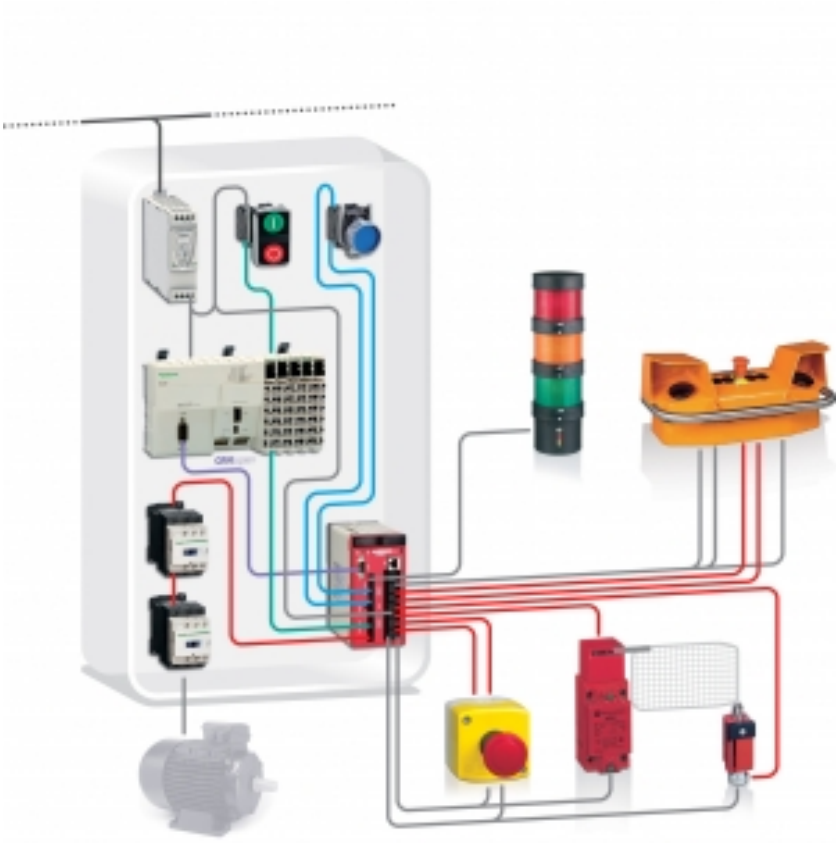
Safety Chain Solution – Multifunction - Safety guard

Design:

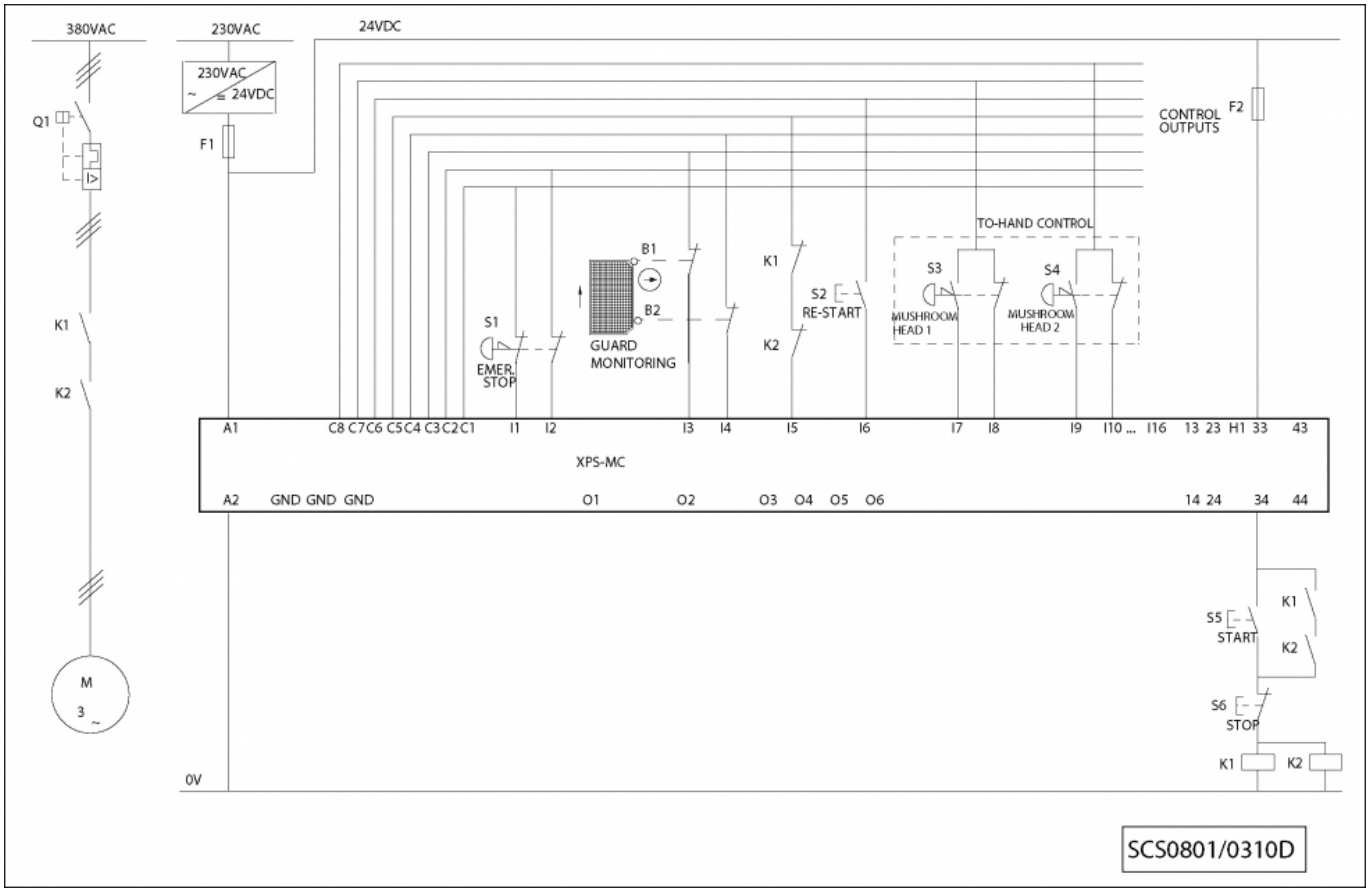
- The safety function employs well-tried safety principles and is robust in the event of a component failure by means of two redundant contacts on the guard switches and two redundant contactors (K1 and K2). The contact synchronization of the limit switches and failure of the contactors are detected by the safety controller at the next demand on the safety function.
- The emergency stop device is designed in accordance with EN ISO 13850 and it is considered a well-tried component with direct opening action in accordance with EN/IEC 60947-5-5.
- The start (S5) and the reset (S2) pushbuttons must be located outside the hazardous area and at a point from which the potential danger is visible.
- The limit switches (B1 and B2) have direct opening action in accordance with EN/IEC 60947-5-1 and are regarded as well-tried components.
- The safety controller satisfies the requirements for performance level PL e in accordance with EN ISO 13849-1 and SIL 3 in accordance with EN/IEC 61508.
- The contactors are considered as well-tried components.
- Protection against overcurrent must be provided in accordance with EN/IEC 60947-4-1.
- The contactors (K1 and K2) have mirror contacts in accordance with EN/IEC 60947-4-1, which are integrated into the input of the safety controller for fault detection.

Related products

- Switches, pushbuttons - Harmony XB4
- Emergency stop control station - Harmony XALK
- Two-Hand control station - Preventa XY2 SB
- Switch mode Power supply - Phaseo ABL8
- Logic controller - Modicon M258
- Guard interlock switch and safety swiitches - Preventa XCS
- Safety Controller - Preventa XPS MC
- Contactor - TeSys D
  Modular beacon and tower light - Harmony XVB



Safety Chain Solution – Multifunction - Safety



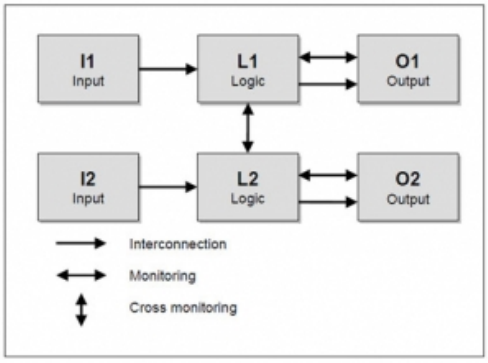


Figure 1

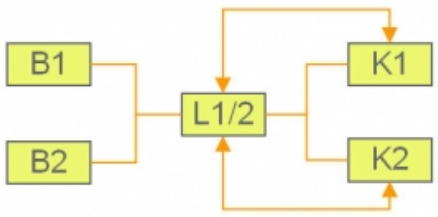


Figure 2

Chain structure:

- The circuit diagram SCS0801/0310D is a conceptual schematic diagram and is limited to present the safety function with only the relevant safety components.
- For the designated architecture of the Category 4 system, 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 with two switches (B1 and B2) that correspond to the input block (see figure 2).
- The safety controller (XPSMC) correspond to the logic block (L1/2), which maintains the internal redundancy of the safety circuits required for this Category.
- The output is represented by two redundant contactors (K1 and K2) that are monitored by the logic block (safety controller) to detect any possible 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 – Multifunction - Safety guard

Safety level calculation:

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	$B10_d$ (operations)	5 000 000	50 000 000
	T10d (years)	157.8	1578
	$MTTF_d$ (years)	1578.3	15782.8
	$MTTF_d$ resulting (years)	1578.3	2500
	PFH_d resulting (1/h)	1.09×10^{-9}	1.09×10^{-9}
	DC (%)	99	99
Logic (safety controller) XPSMC	PFH_d (1/h)	1.4×10^{-8}	1.4×10^{-8}
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)	43	43
	$MTTF_d$ (years)	432.4	432.4
	$MTTF_d$ resulting (years)	432.4	432.4
	PFH_d resulting (1/h)	5.35×10^{-9}	5.35×10^{-9}
	DC (%)	99	99
Safety function	$MTTF_{dC}$	**59.5 (high)**	
	DC_{avg}	**99 (high)**	
	PFH_d resulting (1/h)	**2.04×10^{-8}**	
	PL attained	**e**	
	SIL attained	**3**	

- 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.
- A fault exclusion is assumed for the emergency stop device in accordance with EN ISO 13849-2, since the maximum number of switching cycles during the mission time (20 years) of these devices is not exceeded.
- 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 channel 1. These values are not limited in this case as this is a category 4 system and they are under the 2500 year limit used by the SISTEMA calculation tool.
- A B10d value of 50 000 000 cycles is stated for the limit switch. In accordance with the assumed nop value, the MTTFd would be 15782.8 years for channel 2. This value is limited to 2500 years for this case as this is a category 4 system.
- A PFHd value of 1.4×10^{-8} per hour is stated for the safety controller (XPSMC). 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, 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 must attain at least 65 points (i.e. separation (15), diversity (20), over voltage 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 99% (high) as we are monitoring the combination of guard switch and limit switch contacts as well as the mirror contacts of the contactors.
- The safety-related control system corresponds to category 4 with high MTTFd. The complete functional safety chain results in an average probability of dangerous failure (PFHd) of 2.04×10^{-8}.
- This corresponds to PL e and SIL 3.

SCS0801/0310 - 03-03-2010

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