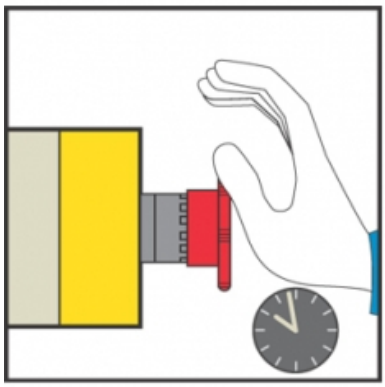
Safety Chain Solution – Safe Stop 1 – Servo Drive

PL e, SIL 3

Improved accuracy through safety integrated devices



Function:

- Safety-related stop function initiated by any of the moveable guards that help protect access to the hazardous area.
- Controlled stop with power available to the actuators (servo-drive) to achieve the stop (i.e. by controlled braking). Power is not interrupted until the stop is achieved (Safe Stop 1).
- After activating the function, the servo motor is braked in a controlled manner, maintaining the power on the actuators. The power is then cut after the machine has come to a halt.
- Opening of a guard is detected by a coded magnetic switch system that activates via the safety module the "Halt" function on the servo-drive; any active movement is decelerated via the adjusted ramp.
- After the delay time monitored by the safety module has elapsed, the safety delayed outputs (stop category 1 in accordance with EN/IEC 60204-1) are deactivated. The servo-drive power stage is then disabled, via the ‘safe torque off' (STO) safety function integrated within it, which prevents the servo-motor from restarting unintentionally.
- The switching of the two redundant STO inputs is monitored by the servo-drive. The power stage is disabled and an error message is generated if the time offset (< 1 sec) is exceeded. The servo-motor can no longer generate torque and coasts down without braking.
- The safety module also monitors the consistent actuation of the magnetic switch contacts to detect possible failure, before restart of the machine movement is permitted.

- Opening or removal of the protective guard is detected by means of the coded magnetic switch system, which are particularly usable for guards without accurate guidance and for use in difficult environments (dust, liquids, etc.).

Typical applications:

- Packaging, printing, or similar machines that use servo-drives in their movements due to high speed and precision needed, on which non-braking stopping would result in a impermissibly long run-down of the hazardous tool movements.

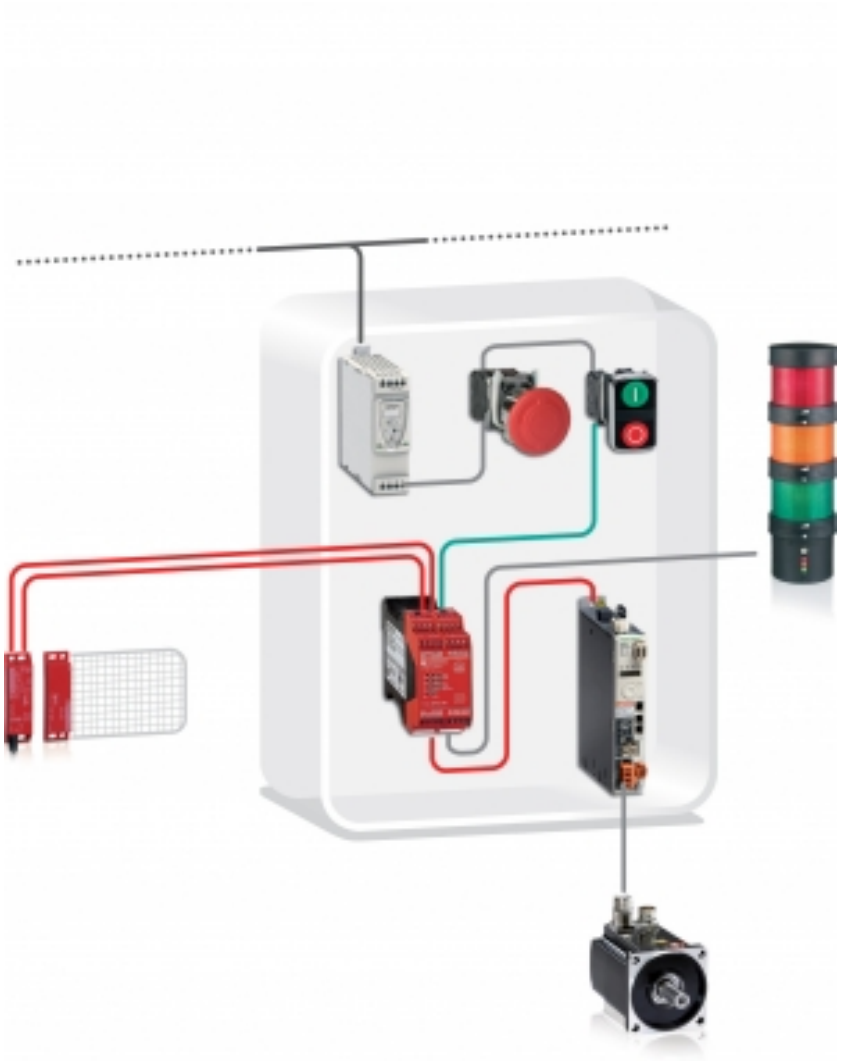
Safety Chain Solution – Safe Stop 1 – Servo Drive

Design:

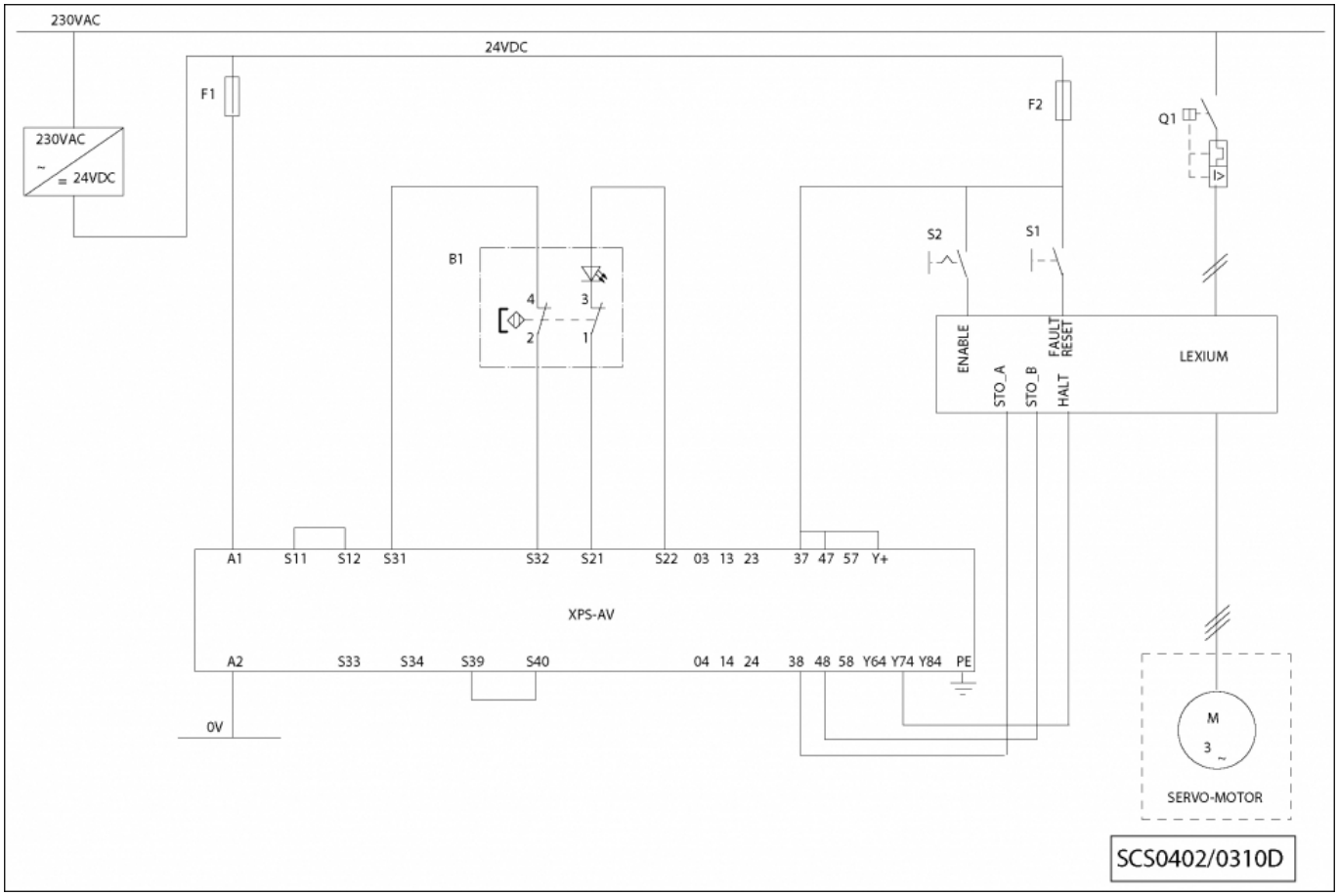
- The safety function employs well-tried safety principles and is robust in the event of a component failure by means of two redundant contacts on the magnetic switch device and two redundant internal circuits for the servo-drive safety function.
- A contact fault in the guard magnetic switches is detected by the safety module at the next demand upon the safety function. The resetting of the module is performed automatically by configuration of the selector buttons included on the device.
- The safety module satisfies the requirements for performance level up to PL e in accordance with EN ISO 13849-1 and SILCL 3 in accordance with EN/IEC 62061 for the safety delayed outputs.
- The delay time set from the safety module must correspond to the deceleration ramp time of the servo-drive and it is adjustable (0 to 300 sec.) by using selector buttons.
- Protection against overcurrent must be provided in accordance with EN/IEC 60947-4-1.
- The servo-drive can be installed directly as part of the safety chain of the safety-related control system as it features an integrated safety function (STO), which is designed to ensure the servo-motor stop and prevent accidental restarts.
- This STO function meets the requirements of category 3 and PL e of EN ISO 13849-1, SIL3 in accordance with EN/IEC 61508 and the standard dealing with the functional safety requirements of power drive systems, EN/IEC 61800-5-2.

Related products

Switches, pushbuttons, emergency stop - Harmony XB4
Switch mode Power supply - Phaseo ABL8
Coded magnetic system - Preventa XCSDM
Safety Module - Preventa XPSAV
Servo Drive - Lexium 32
Modular beacon and tower lights - Harmony XVB



Safety Chain Solution – Safe Stop 1 – Servo



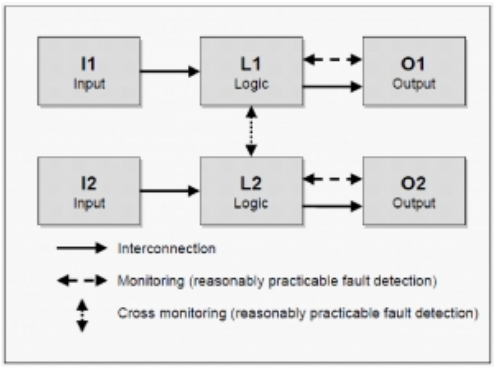


Figure 1

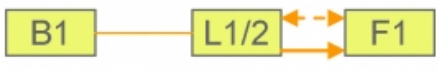


Figure 2

Chain structure:

- The circuit diagram SCS0402/0310D 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 3 system, two redundant channels are implemented.
- The circuit arrangement can be divided into three function blocks, input (I), logic (L) and output (O) per channel (see figure 1).
- The functional channel can be represented by the magnetic switch (B1) that corresponds to the input block (see figure 2).
- The safety module (XPSAV) corresponds to the logic block (L1/2), which maintains the internal redundancy of the safety circuits required for this category.
- The output block is represented by the servo drive (F1), which includes the STO safety function that is triggered via 2 redundant inputs. The circuits of the two inputs are separated (two channels) and are monitored, which is indicated by the broken lines.
- 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 1 – Servo Drive

Cycle time (s)	30
Number of hours' operation per day (h)	12
Number of days' operation per year	220
Number of operations per year (n_{op})	316800

		Values	
		Channel 1	Channel 2
Input (magnetic switch) XCS	$B10_d$ (operations)	50 000 000	50 000 000
	$T10_d$ (years)	158	158
	$MTTF_d$ (years)	1578.3	1578.3
	$MTTF_d$ resulting (years)	100	100
	PFH_d resulting (1/h)	2.47×10^{-8}	2.47×10^{-8}
	DC (%)	99	99
Logic (safety module) XPSAV	PFH_d (1/h)	7.95×10^{-9}	7.95×10^{-9}
Output (actuator) LXM32 servo-drive	$MTTF_d$ (years)	1400	1400
	DC (%)	90	90
	PFH_d (1/h)	1×10^{-9}	1×10^{-9}
Safety function	$MTTF_{dC}$	**30.1 (high)**	
	DC_{avg}	**96.3 (medium)**	
	PFH_d resulting (1/h)	**3.36×10^{-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.
- If the protective guard device is assumed to be actuated every half minute during 220 working days per year and 12 working hours, the number of operations (nop) would be 316 800.
- 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 structure or tests.
- A B10d value of 50 000 000 cycles is stated for the coded magnetic switch. In accordance with the assumed nop value, the MTTFd would be 1578,3 years for each channel. These values are therefore limited to 100 years ("high").
- A PFHd value of 7.95×10^{-9} is stated for the safety delayed outputs of the safety module (XPSAV). This value comes directly from the safety device data and is validated and certified by an accepted standards body.
- For the servo-drive a MTTFd value of 1400 years and a diagnostic coverage (DC) of 90% is stated. It results in a PFHd value of 1×10^{-9} for this device. This value comes directly from the device data and it is certified by an accepted standards body.
- Measures against common cause failures (Annex F of EN ISO 13849-1) must attain at least 65 points (i.e. separation (15), diversity (20), over voltage protection etc. (15) and environmental conditions (25+10)).
- The combination of channel 1 and channel 2 results in a DCavg 96,3% (medium) as the two redundant STO inputs are monitored by the servo-drive and the magnetic switch is monitored by the safety module.
- 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 3.36×10^{-8}.
- This corresponds to PL e and SIL 3.

SCS0402/0310 - 03-03-2010

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