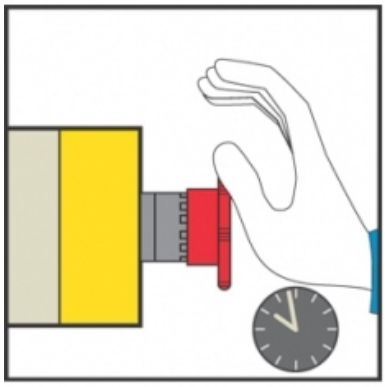
Safety Chain Solution – Safe Stop 2 – Servo enhanced safety

PL e, SIL 3

Improved accuracy through safety integrated devices



Function:

- Safety-related stop function realized by a moveable guard that help protects access to the hazardous area.
- The hazardous movement is interrupted either if the stop button (S2) or the emergency stop device (S3) is actuated, which initiates the functional stopping of the servo-drive, i.e. by a deceleration ramp.
- The Safe Stop 2 safety function is used to achieve a category 2 safe stop in accordance with EN/IEC 61800-5-2, where the servo motor is braked in a controlled manner, maintaining the power on the actuators.
- The safety function SS2 (Safe Stop 2), integrated in the enhanced safety module (eSM) card, monitors the deceleration and the standstill position.
- When the SS2 function is triggered, a deceleration of movement is monitored with the specified monitoring ramp up to standstill. The motor is then immobilized by the ‘safe operating stop‘ (SOS) function, which is used to monitor any deviation from the standstill position.
- If the monitored deceleration ramp is violated or the monitored standstill position is not maintained, the drive is halted by the ‘safe torque off‘ (STO) function, which prevents the motor from restarting unintentionally.
- The eSM card also monitors the consistent actuation of the redundant switch contacts from the magnetic switch to detect possible failure, before restart of the machine movement is permitted.

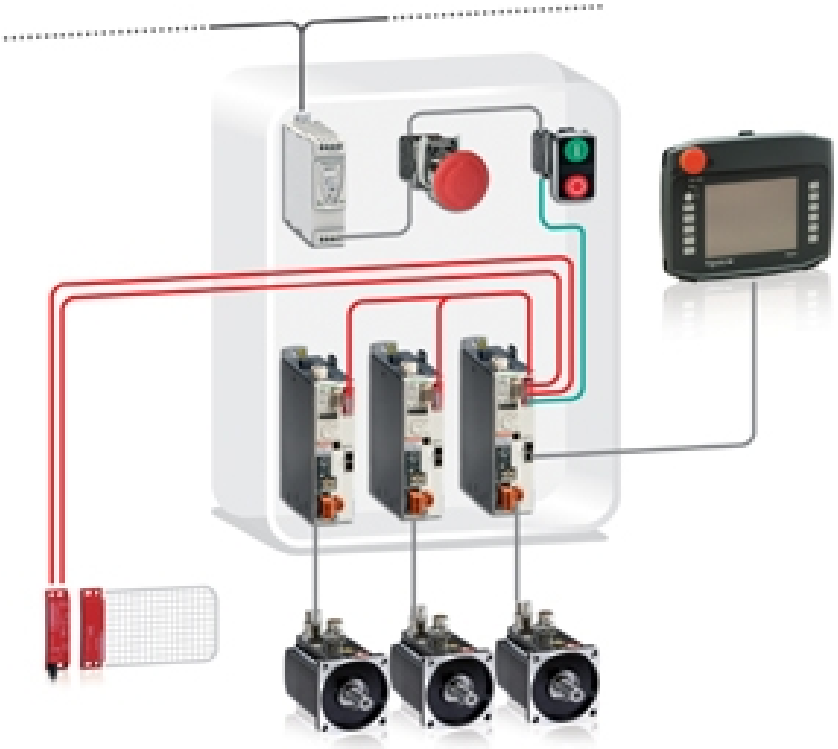
Typical applications:

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 2 – Servo enhanced safety

Design:

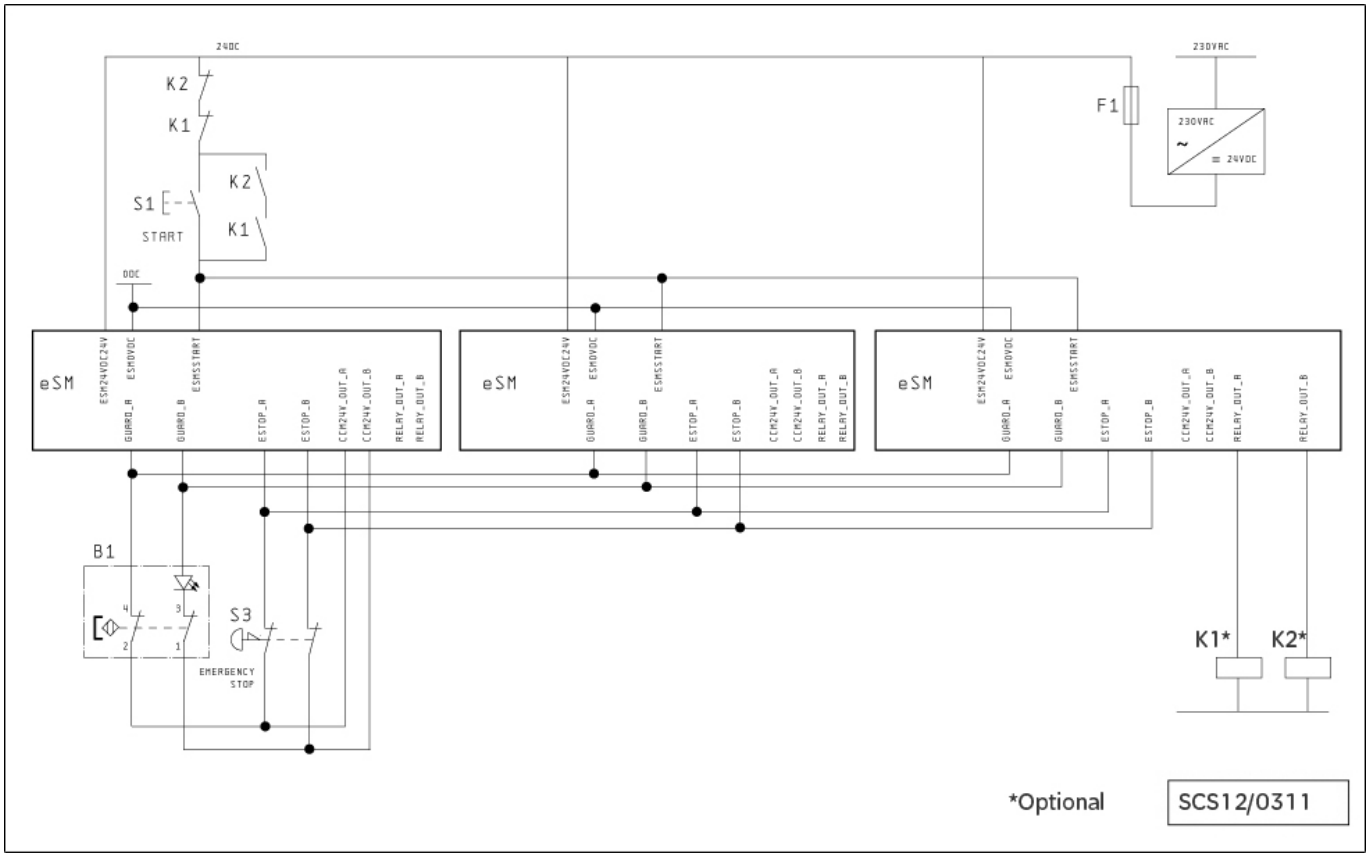
- The safety function employs well-tried safety principles and is robust in the event of a component failure by means of two redundant contacts on the magnetic switch device and two redundant internal circuits for the servo-drive safety function.
- The contact failure of the magnetic switch is detected by the enhanced safety module (eSM) integrated on the servo-drive at the next demand upon the safety function.
- The enhanced safety module (eSM) 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.
- The adjustable deceleration braking ramp must be selected so that under the most unfavorable operating conditions, the machine's movement is stopped before the immobilization of the motor by SOS function is triggered.
- Protection against over-current 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 (Safe Operating Stop - SOS), which is designed to monitor any deviation from the standstill position of the motor, preventing restart.
- The Safe Operating Stop (SOS) function meets the requirements of category 3 and PL e of EN ISO 13849-1, SIL 3 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
- Guard switches - Preventa XCSLE
- Enhanced Safety Module (eSM) - Lexium 32M
- Servo drive - Lexium 32M
- Human machine interface - Magelis XBT GH
- Modular beacon and tower lights - Harmony XVB
- Switch mode Power supply - Phaseo ABL8

Safety Chain Solution – Safe Stop 2 – Servo



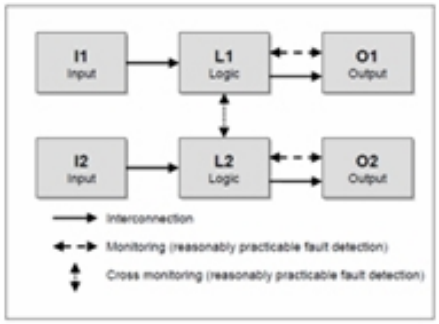


Figure 1

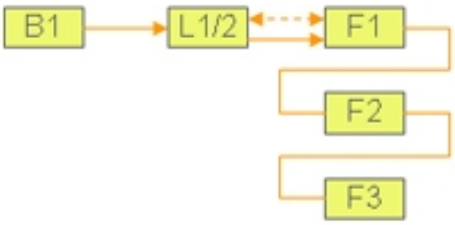


Figure 2

Chain structure:

- The circuit diagram SCS12/0311D 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 3, 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 magnetic switch device (B1) that correspond to the input block (see figure 2).
- The enhanced safety module (eSM) 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 the servo-drives (F1+F2+F3) with two redundant internal circuits and connected in cascade.
- 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 2 – Servo enhanced safety

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
	T10d (years)	157.8	157.8
	$MTTF_d$ (years)	1578.3	1578.3
	$MTTF_d$ resulting (years)	100	100
	PFH_d resulting (1/h)	2.47×10^{-9}	2.47×10^{-9}
	DC (%)	99	99
Logic (safety module) eSM and Lexium 32 output (actuator)	PFH_d (1/h)	7×10^{-9}	7×10^{-9}
	PFH_d (1/h)	7×10^{-9}	7×10^{-9}
	PFH_d (1/h)	7×10^{-9}	7×10^{-9}
	PFH_d resulting (1/h)	2.1×10^{-8}	2.1×10^{-8}
Safety function	$MTTF_{eq}$	**100 (high)**	
	DC_{avg}	**99 (high)**	
	PFH_d resulting (1/h)	**4.57×10^{-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 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.
- A B10d value of 50 000 000 cycles is stated for the coded magnetic switch. In accordance with the assumed above 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 7×10^{-9} is stated for the enhanced safety module (eSM). This value comes directly from the safety device data and is certified by an accepted standards body. This value already includes the servo drive PFHd value as it is using a safety function integrated on it (Safe Stop 2).
- A total value of 2.1×10^{-8} is therefore stated for the logic and output part as a results of using 3 servo-drives in cascade for the same safety function.
- 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 > 99 % (high) as we are monitoring the coded magnetic switch input contacts as well as the deceleration and the standstill position by means of Safe Operating Stop (SOS) function.
- The safety-related control system corresponds to category 3 with high MTTFd (> 30). The complete functional safety chain results in average probability of dangerous failure (PFHd) of 4.57 x 10-8.
- This corresponds to PL e and SIL 3.

SCS12/0311 - 17-03-2011

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