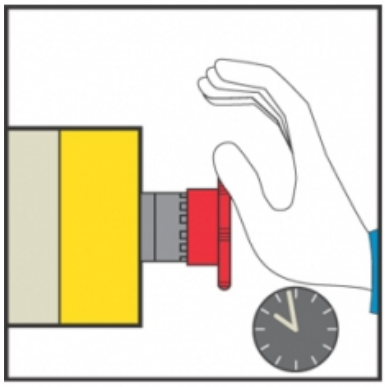
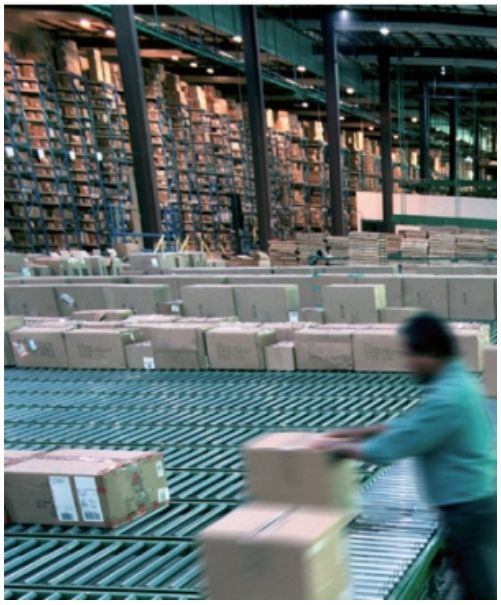
Safety Chain Solution – Safe Stop 1 - Variable speed drive

PL d, SIL 2

Safety integrated devices for an easier chain configuration





Function:

- Safety-related stop function initiated by a moveable guard that help protects access to the hazardous area.
- Controlled stopping with power maintained to the actuator (drive) to achieve stopping (i.e. braking), then cut-off of power when standstill is reached (Safe Stop 1).
- The hazardous movement is interrupted either if the stop button (S2) or the emergency stop device (S3) is actuated. (*)
- Opening of this guard is detected by a safety interlock switch, which initiates the functional stopping of the drive, i.e. by a braking ramp (stop category 1 in accordance with EN/IEC 60204-1).
- After the delay time monitored by the safety module has elapsed, the safety delayed outputs are deactivated. The drive is then halted, by the 'safe torque off' (STO) safety function integrated within it, which prevents the motor from restarting unintentionally.
- The safety module also monitors the consistent actuation of the redundant guard switch contacts to detect possible 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:

Machines that use drives in their movements due to high speed and precision needed (i.e. stacker-cranes used on automatic storage and retrieval systems), when the delayed initiation of the stopping in the event of a fault must not involve an unacceptably high residual risk.

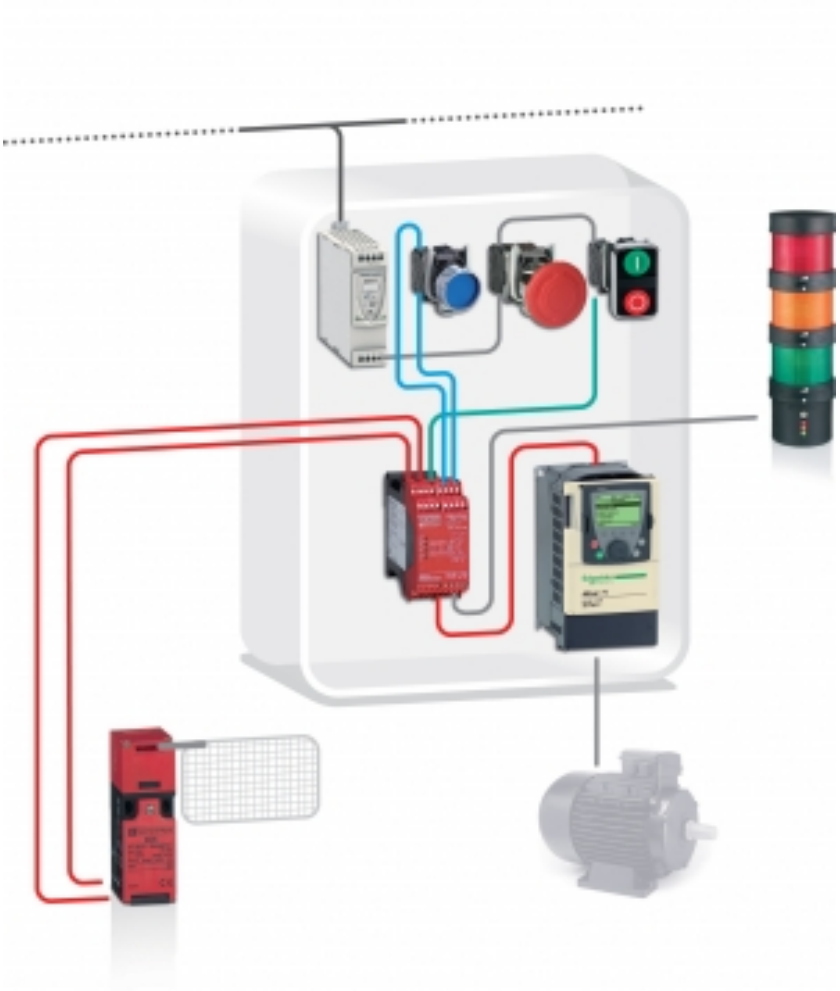
Safety Chain Solution – Safe Stop 1 - Variable speed drive

Design:

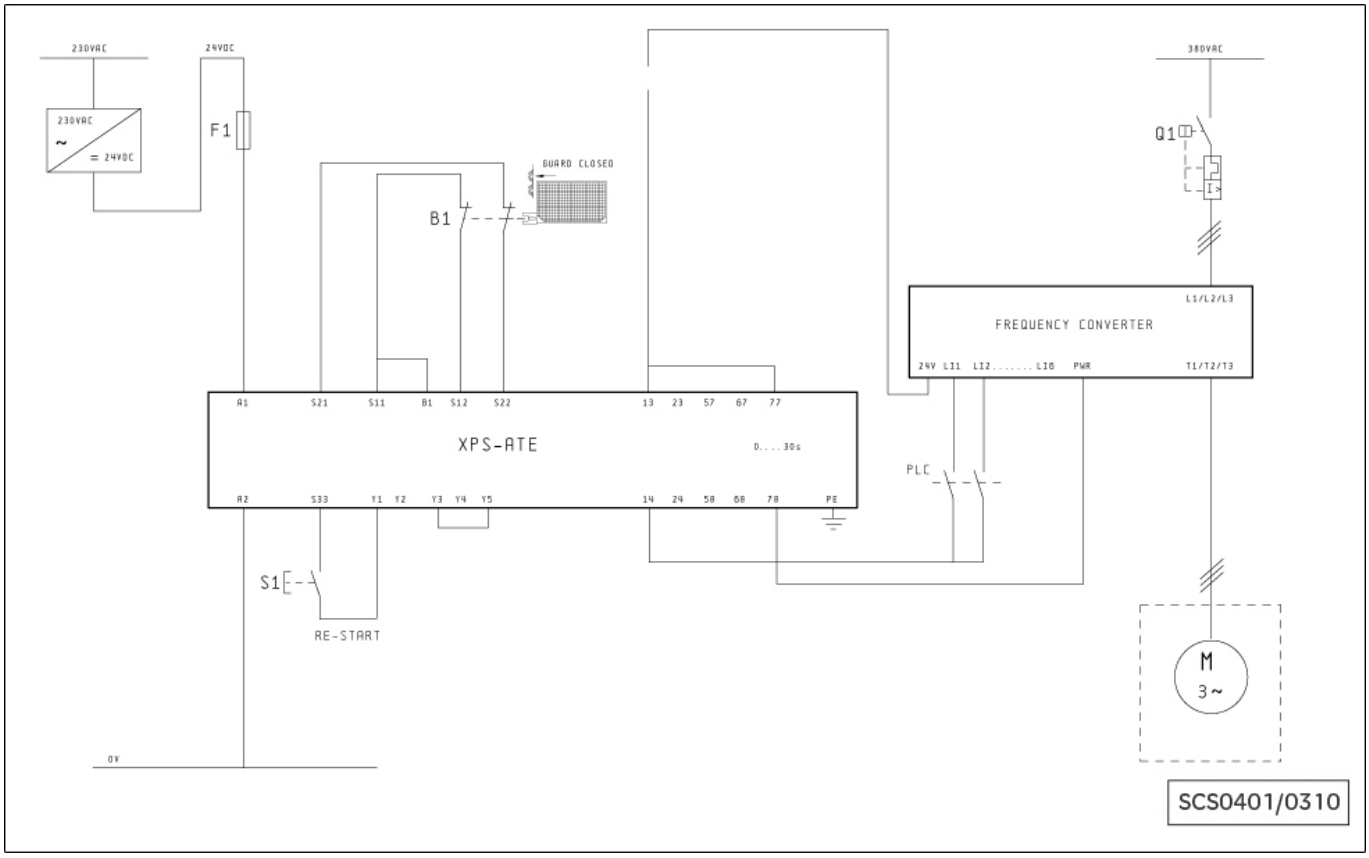
- The safety function employs well-tried safety principles and is robust in the event of a component failure by means of two redundant contacts on the safety interlock switch and two redundant internal circuits for the drive safety function.
- The emergency stop device is designed in accordance with EN ISO 13850 and it is considered a well-tried component with direct opening action in accordance with EN/IEC 60947-5-5.
- The guard switch (B1) has direct opening action in accordance with EN/IEC 60947-5-1 and it is also regarded as a well-tried component.
- A guard switch contact fault is detected by the safety module at the next demand upon the safety function.
- The safety module satisfies the requirements for performance level up to PL d in accordance with EN ISO 13849-1 and SILCL 2 in accordance with EN/IEC 62061 for the safety delayed outputs.
- The adjustable braking time in the safety module must be selected so that under the most unfavourable operating conditions, the machine's movement is stopped before power is removed from the drive.
- Protection against overcurrent must be provided in accordance with EN/IEC 60947-4-1.
- The variable speed 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 torque off - STO), which is designed to ensure a motor stop and prevent accidental restart.
- The STO function (named Power removal - PWR in the drive) meets the requirements of category 3 and PL d of EN ISO 13849-1, SIL2 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
- Emergency stop function - Harmony XALK
- Switch mode Power supply - Phaseo ABL8
- Safety Guard switches - Preventa XCS
- Safety module - Preventa XPSATE
- Variable speed drive - Altivar 71
- Modular beacon and tower lights - Harmony XVB



Safety Chain Solution – Safe Stop 1 - Variable



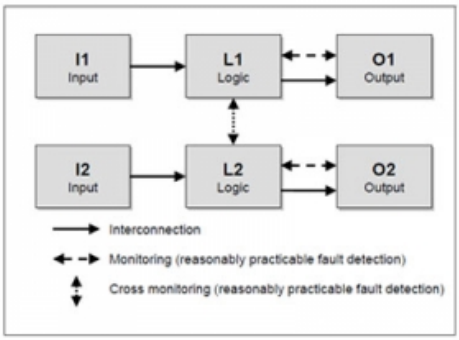


Figure 1

Figure 2

Chain structure:

- The circuit diagram SCS0401/0310D 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 guard switch (B1) that corresponds to the input block (see figure 2).
- The safety module (XPSATE) 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 drive (F1) with two redundant internal circuits related to the integrated ‘safe torque off' safety function (STO).
- 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 - Variable speed drive

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	5 000 000
	T10d (years)	158	158
	$MTTF_d$ (years)	1578.3	1578.3
	$MTTF_d$ resulting (years)	100	100
	PFH_d resulting (1/h)	1.01×10^{-7}	1.01×10^{-7}
	DC (%)	99	99
Logic (safety module) XPSATE (delay outputs)	PFH_d (1/h)	1.96×10^{-8}	1.96×10^{-8}
Output (actuator) ATV71 drive	PFH_d (1/h)	1×10^{-8}	1×10^{-8}
Safety function	$MTTF_{dC}$	**35.3 (high)**	
	DC_{avg}	**63.7 (low)**	
	PFH_d resulting (1/h)	**5.43×10^{-8}**	
	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.
- A fault exclusion is assumed for the emergency stop device in accordance with EN ISO 13849-2, since the maximum number of switching cycles of these devices is not exceeded within the mission time (20 years).
- 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 therefore limited to 100 years ("high").
- A PFHd value of 1.96×10^{-8} is stated for the safety delayed outputs of the safety module (XPSATE). This value comes directly from the safety device data and is certified by an accepted standards body.
- For the variable speed drive a PFHd value of 1×10^{-8} is stated. 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 63.7% (low) as no monitoring exists for the output states.
- 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 5.43×10^{-8}
- This corresponds to PL d and SIL 2.

SCS0401/0310 - 03-03-2010

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