Functional Example CD-FE-I-002-V20-EN

Safety-related controls

SIRIUS Safety Integrated

Emergency stop with monitored start
in Category 4 according to EN 954-1
(with evaluation according to EN 62061
and EN ISO 13849-1: 2006)

with a SIRIUS 3TK28 safety relay

safety INTEGRATED

SIEMENS

Comments

"Safety Integrated" Functional Examples are functional, tested automation configurations based on A&D standard products for the simple, quick and low-cost performance of automation tasks involving safety technology. Each of these Functional Examples covers one frequently occurring aspect of a typical customer problem in the field of safety technology.

In addition to containing a list of all of the necessary software and hardware components, and a description of their interwiring, the Functional Examples also contain tested and commented code. This enables the functions described here to be adapted quickly and thus used as a basis for individual extensions.

Important note

The Safety Functional Examples are not binding and do not claim to be complete regarding the circuits shown, equipping and any eventuality. The Safety Functional Examples do not represent customer-specific solutions. They are only intended to provide support for typical applications. You are responsible in ensuring that the described products are correctly used.

These Safety Functional Examples do not relieve you of the responsibility in safely and professionally using, installing, operating and servicing equipment. When using these Safety Functional Examples, you recognize that Siemens cannot be made liable for any damage/claims beyond the liability clause described above. We reserve the right to make changes to these Safety Functional Examples at any time without prior notice. If there are any deviations between the recommendations provided in these Safety Functional Examples and other Siemens publications - e.g. Catalogs - then the contents of the other documents have priority.

Table of Contents

1 Guarantee, Liability and Support

We do not accept any liability for the information contained in this document.

Any claims against us – based on whatever legal reason – resulting from the use of the examples, information, programs, engineering and performance data etc., described in this Safety Functional Example shall be excluded. Such an exclusion shall not apply in the case of mandatory liability, e.g. under the German Product Liability Act ("Produkthaftungsgesetz") in case of intent, gross negligence, or injury of life, body or health, guarantee for the quality of a product, fraudulent concealment of a deficiency or breach of a condition which goes to the root of the contract ("wesentliche Vertragspflichten"). However, claims arising from a breach of a condition which goes to the root of the contract shall be limited to the foreseeable damage which is intrinsic to the contract , unless caused by intent or gross negligence or based on mandatory liability for injury of life, body or health. The above provisions does not imply a change in the burden of proof to your detriment.

2 Function

2.1 Description of Functionality

If people (in production technology) are close to machines, then they must be protected using the appropriate equipment. The E-Stop command device represents a widely established component that protects people, plants/systems and the environment against potential hazards.

In this Safety Functional Example, the E-Stop command device is monitored using two positively-driven contacts using a safety relay in accordance with Category 4 to EN 954-1. If the E-Stop button is pressed, the safety relay opens the redundantly connected contactors via the safety-related relay outputs using positively-driven contacts in accordance with stop Category 0 according to EN 60204-1. In this particular example, a drive is stopped. Before restarting or acknowledging the E-Stop shutdown using the start button, a check is made as to whether both contacts of the E-Stop command device are closed and both contactors are de-energized (open).

Note

Equipment, functional aspects and design guidelines for the emergency stop are specified in EN ISO 13850: 2006. The standard EN 60204-1: 2006 must also be considered.

2.2 Advantages / Customer Benefits

- Pure hardware engineering without having to configure/program software
- Little wiring is required and it is simple
- Space-saving design using compact safety relay
- Can be simply expanded using expansion devices

3 Components Required

Hardware components

Table 3-1

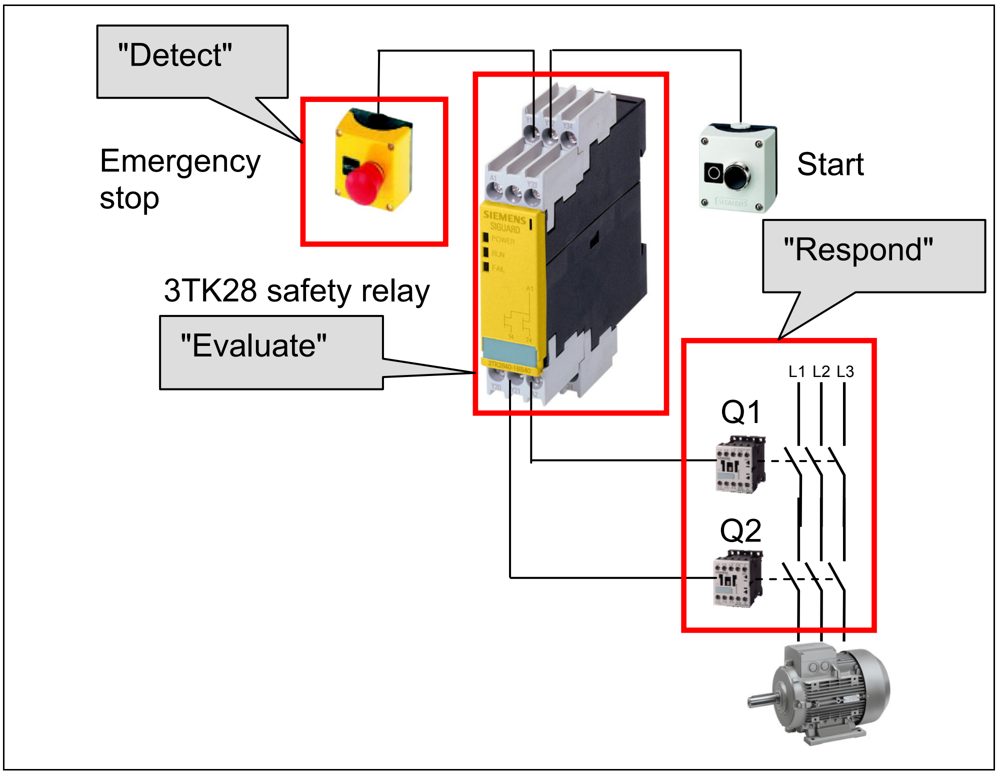
Component	Type	Order No. / Order Information	Qty.	Manufacturer
Emergency stop	1NC 40mm mushroom pushbutton with yellow top, without protective collar	3SB3 801-0DG3	1	SIEMENS
	1NC contact block for base mounting	3SB3 420-0C	1	
Safety relay	3TK2823	3TK2823-1CB30	1	
Start button	Empty command point enclosure	3SB3 801-0AA3	1	
	1NO contact block for base mounting	3SB3 420-OB	1	
	Black pushbutton with flat button, 22 mm nominal diameter	3SB3 000-0AA11	1	
	Optional: "Start" inscription label	3SB3 906-1EL	1	
Contactors Q1/Q2	Contactor, AC-3, 3KW/400V, 1NC, 24 V DC, 3-pole, size S00, screw terminal	3RT1015-1BB42	2	

Note

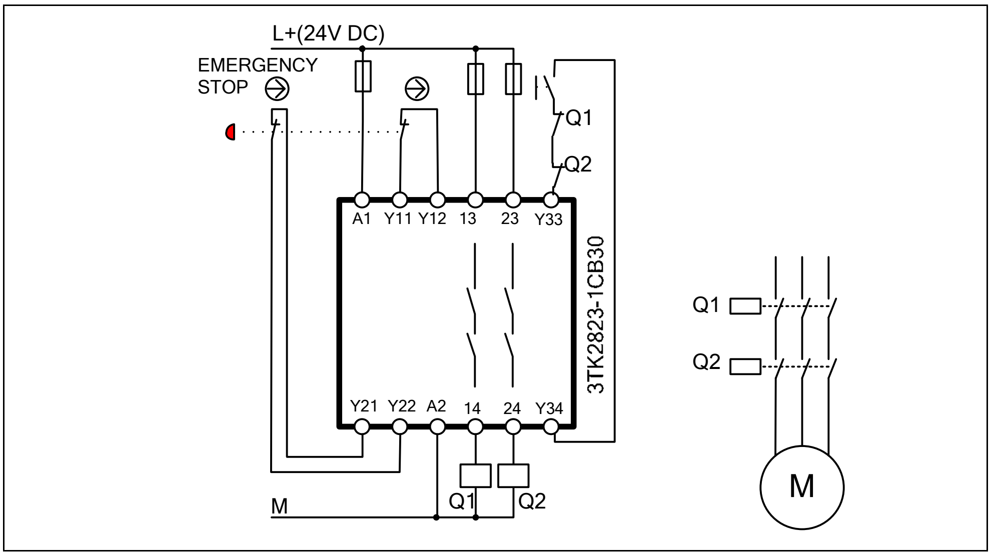
Functionality was tested with the specified hardware components. Similar products not found in this list may also be used (e.g. a different safety relay 3TK28). If this is the case, please consider that changes to the wiring of the hardware components (e.g. different terminal assignment) might be required.

4 Structure and wiring

4.1 Overview of Hardware Setup



4.2 Connecting-up the hardware components



5 Evaluation according to EN 62061 and EN ISO13849-1:2006

5.1 Safety Function

Comments

- Emergency stop is not a means of risk mitigation.
- Emergency stop is a "supplementary safety function"

Supplementary Safety Function

Further considerations are based on the following supplementary safety function:

Supplementary safety function	
SF 1	The motor must be switched off when "emergency stop" is actuated.

The safety function listed above is evaluated below according to the two standards EN 62061 and EN ISO 13849-1: 2006.

5.2 Evaluation according to EN 62061

Parameters for the calculation of PFH_D for **"Detect" (emergency stop) and "Respond" (contactor)**

Parameter	Value	Reason	Definition
B10 Emergency stop Contactor	 $1 * 10^5$ $1 * 10^6$	Manufacturer specifications	Siemens
Proportion of hazardous failures Emergency stop Contactor	 0.2 0.75	Manufacturer specifications (20%) (75%)	
T1 Service life	175,200h (20 years)	Manufacturer specifications	
C Number of emergency stop operations Number of operations of contactors	 $6 * 10^{-3}$ / h $6 * 10^{-3}$ / h	Assumptions: Actuated once per week (7 * 24 hours) (test emergency stop). Actuations can take place every day of the year (365 days). The contactors are always activated and are only operated when the emergency stop is actuated.	User
T2 Diagnostics test interval emergency stop Diagnostics test interval contactor	 168h 168h	When the emergency stop is actuated, a defective contact is detected in the 3TK. An actuation takes place every week (7 * 24 hours) (see "**C**"). When actuated, a defective contactor is detected in the 3TK. An actuation takes place every week (7 * 24 hours) (see "**C**").	
β (CCF Factor) Proneness toward failures as a result of common cause	0.1	If installed according to EN 62061, a CCF factor of 0.1 (10%) can be assumed. With this value the user plays it safe ("conservative value").	
DC Degree of diagnostic coverage	0.99 (99%)	Discrepancy evaluation at emergency stop; Evaluation of read-back signals (positively-driven contacts) of both contactors.	

Evaluation parameter

Parameter	Component	Value	Definition
PFH_D (3TK)	3TK2823	$3 * 10^{-8}$	Siemens

Summary

	EN 62061			
	SIL CL		PFH_D	
Detect	3	Hardware error tolerance: HFT = 1 Proportion of safe failures: SFF ≥ 0.99 (99%)	$1.2 * 10^{-10}$	Architecture: Basic sub-system architecture D
Evaluate	3	Manufacturer specifications	$3 * 10^{-08}$	Manufacturer specifications
Respond	3	Hardware error tolerance: HFT = 1 Proportion of safe failures: SFF ≥ 0.99 (99%)	$4.5 * 10^{-11}$	Architecture: Basic sub-system architecture D
Results	3	SIL CL of all tasks of the supplementary safety function is at least 3. PFH_D (= 3.02*10-08) of the entire supplementary safety function fulfills SIL 3.		

Evaluation according to ISO 13849-1:2006

Parameters for the calculation of $MTTF_d$ for "Detect" (emergency stop) and "Respond" (contactor)

Parameter	Value	Reason	Definition
B10 Emergency stop Contactor	 $1 * 10^5$ $1 * 10^6$	Manufacturer specifications	Siemens
Proportion of hazardous failures Emergency stop Contactor	 0.2 0.75	Manufacturer specifications (20%) (75%)	
$\mathbf{d_{op}}$ Mean operating time in days per year	365 days per year	Assumption: Actuation takes place every day of the year.	User
$\mathbf{h_{op}}$ Mean operating time in hours per day	24 hours per day		
$\mathbf{T_{Cycle}}$ Mean time between the start of two consecutive cycles of the component Emergency stop Contactor	 168 h/Cycle 168 h/Cycle	Assumption: There is an interval of one week between actuations of the emergency stop (emergency stop test) and contactors (7 * 24 hours).	

Interim results (are identical in this example for emergency stop and contactor):

Interim results		Reason
$MTTF_d$	High	$MTTF_d$ ≥30 years
DC	High	DC=99% Discrepancy evaluation for emergency stop; evaluation of read-back signals (positively-driven contacts) of both contactors
Measures against CCF	Fulfilled	It is assumed that the necessary measures are taken by the user.
Category	4	System behavior: A single fault does not cause the loss of the safety function. The single fault is detected. $MTTF_d$: High, DC: High, measures against CCF: Fulfilled

Evaluation parameter

Parameter	Component	Value	Definition
PFH_D (3TK)	3TK2823	$3*10^{-8}$	Siemens

Results

	ISO 13849-1:2006	
	PL	**Average probability of a hazardous failure per hour**
Detect	e	$2.47*10^{-08}$ (from Annex K; see note)
Evaluate	e	$3*10^{-08}$
Respond	e	$2.47*10^{-08}$ (from Annex K; see note)
Results	e	PL of all tasks of the supplementary safety function is at least e. Number of tasks is less than or equal to 3.

Note: The $MTTF_d$ for each channel is limited to max. 100 years!

5.3 Summary

	EN 62061		ISO 13849-1:2006	
	SIL CL	PFH$_D$	PL	Average probability of a hazardous failure per hour
Detect	3	$1.2 * 10^{-10}$	e	$2.47 * 10^{-08}$
Evaluate	3	$3 * 10^{-08}$	e	$3 * 10^{-08}$
Respond	3	$4.5 * 10^{-11}$	e	$2.47 * 10^{-08}$

Results	SIL3	PL e

6 Contacts

Technical Assistance for Low-Voltage Controls and Distribution

In person from Mon. - Fri. 8 a.m. to 5 p.m. (CET)
Phone: +49 (911)-895-5900
e-mail: technical-assistance@siemens.com
Internet: http://www.siemens.de/lowvoltage

By fax around the clock
Fax: +49 (911)-895-5907

7 History

Table 7-1 History

Version	Date	Change
V1.0	02.06.2005	First issue
V2.0	30.04.2008	- Revision of the hardware configuration overview - New chapter: Evaluation according to EN 62061 and EN ISO 13849-1