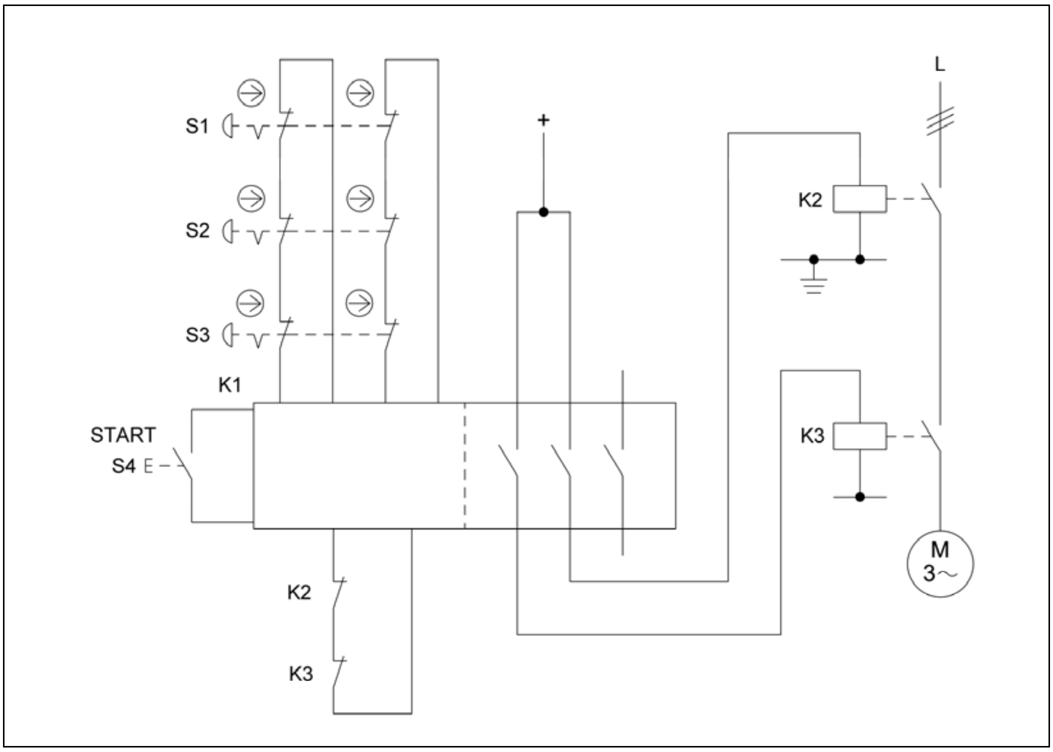
8.2.29 Cascading of emergency stop devices by means of a safety module – Category 3 – PL e (Example 29)

Figure 8.50:
Cascading of emergency stop devices by means of a safety module (emergency stop function, STO)

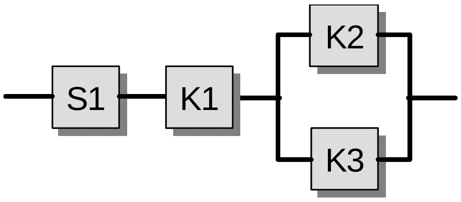


Safety function

- Emergency stop function, STO by actuation of an emergency stop device

Functional description

- Hazardous movements or states are interrupted or prevented by actuation of an emergency stop device. As shown by Example 3 in Section 5.3.2, each emergency stop device triggers a safety function of its own. S1 is considered below as being representative of all the devices. S1 is evaluated in a safety module K1, which actuates two redundant contactor relays K2 and K3.
- The signals from the emergency stop devices are read redundantly into the safety module K1 for fault detection. K1 also features internal test measures. The contactor relays K2 and K3 are also monitored in K1, by means of mechanically linked readback contacts. K2 and K3 are operated by switch S4 at each start-up command, approximately twice each month. An accumulation of more than two faults in the period between two successive actuations may lead to loss of the safety function.
- It is not assumed that more than one emergency stop device is pressed simultaneously.



Design features

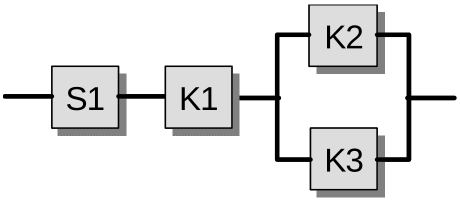
- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- The emergency stop devices S1, S2 and S3 are switching devices with direct opening contacts in accordance with IEC 60947-5-1, Annex K.
- The supply conductors to the switching devices are laid separately or with protection.
- The safety module K1 satisfies all requirements for Category 4 and PL e.
- K2 and K3 possess mechanically linked contact elements to IEC 60947-5-1, Annex L.

Remark

- The emergency stop function is a complementary protective measure to EN ISO 12100-2:2004.

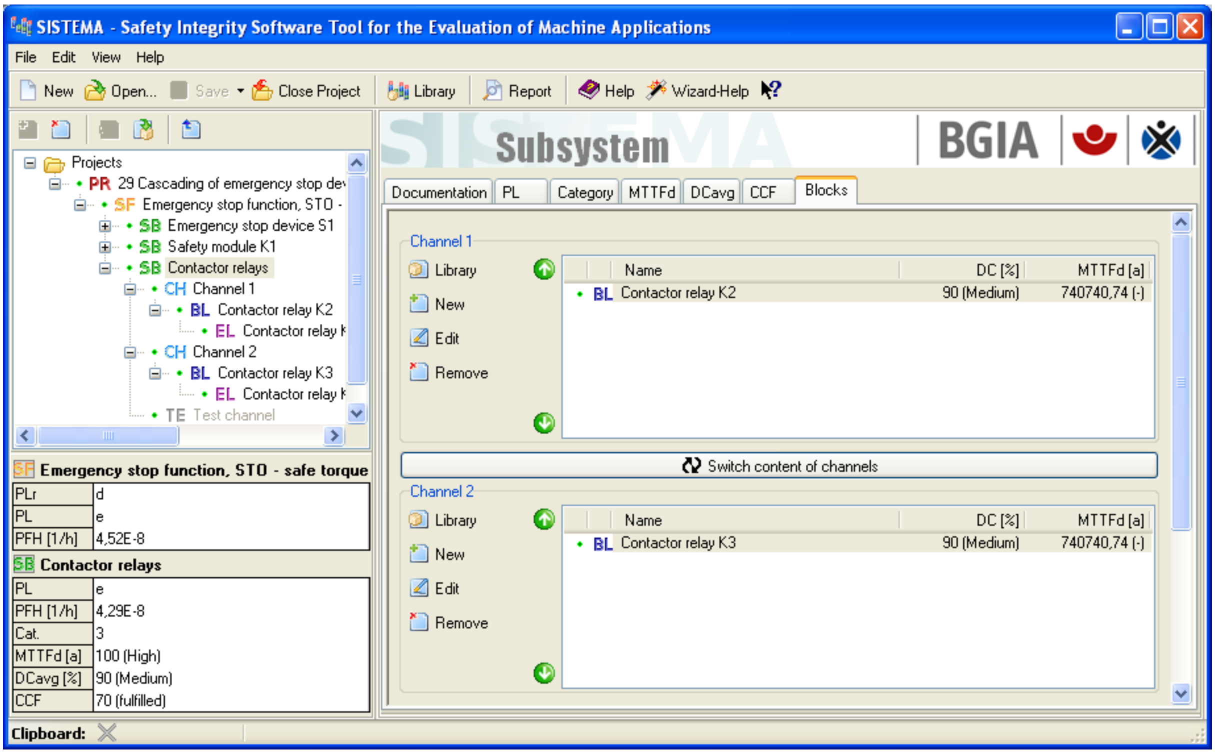
Calculation of the probability of failure:

- S1, S2 and S3 are standard emergency stop devices to EN ISO 13850. Fault exclusions apply for the direct opening contacts and for the mechanical elements, provided the number of operations stated in Table D.2 of this report is not exceeded.
- The probability of failure of the final safety module K1 is added at the end of the calculation (2.31 × 10^{-9} per hour [M], suitable for PL e). For the subsystem K2/K3, the probability of failure is calculated as follows.
- $MTTF_d$: for the contactor relays K2 and K3, the B_{10} value corresponds under inductive load (AC 3) to an electrical lifetime of 1,000,000 switching operations [M]. If 50% of failures are assumed to be dangerous, the B_{10d} value is produced by doubling of the B_{10} value. With three demands upon the emergency stop function and 24 start commands per year, n_{op} is 27 cycles per year and the $MTTF_d$ is 740,740 years. This is also the symmetrical $MTTF_d$ for the channel, which is capped to 100 years ("high").
- DC_{avg}: the *DC* of 90% for K2 and K3 is based upon testing by the safety module K1. This is also the DC_{avg} ("medium").
- Adequate measures against common cause failure (70 points): separation (15), well-tried components (5), overvoltage protection etc. (15) and environmental conditions (25 + 10)



- The subsystem K2/K3 corresponds to Category 3 with a high *MTTF*$_d$ (100 years) and medium *DC*$_{avg}$ (90%). This results in an average probability of dangerous failure of 4.29 × 10^{-8} per hour. Following addition of the subsystem K1, the average probability of dangerous failure is 4.52 × 10^{-8} per hour. This corresponds to PL e. The PL$_r$ of d is thus surpassed.

Figure 8.51:
Determining of the PL by means of SISTEMA



Projects
PR 29 Cascading of emergency stop dev
SF Emergency stop function, STO -
SB Emergency stop device S1
SB Safety module K1
SB Contactor relays
CH Channel 1
BL Contactor relay K2
EL Contactor relay K
CH Channel 2
BL Contactor relay K3
EL Contactor relay K
TE Test channel

SF Emergency stop function, STO - safe torque

PLr	d
PL	e
PFH [1/h]	4,52E-8

SB Contactor relays

PL	e
PFH [1/h]	4,29E-8
Cat.	3
MTTFd [a]	100 (High)
DCavg [%]	90 (Medium)
CCF	70 (fulfilled)

Channel 1

	Name	DC [%]	MTTFd [a]
BL	Contactor relay K2	90 (Medium)	740740,74 (-)

Channel 2

	Name	DC [%]	MTTFd [a]
BL	Contactor relay K3	90 (Medium)	740740,74 (-)