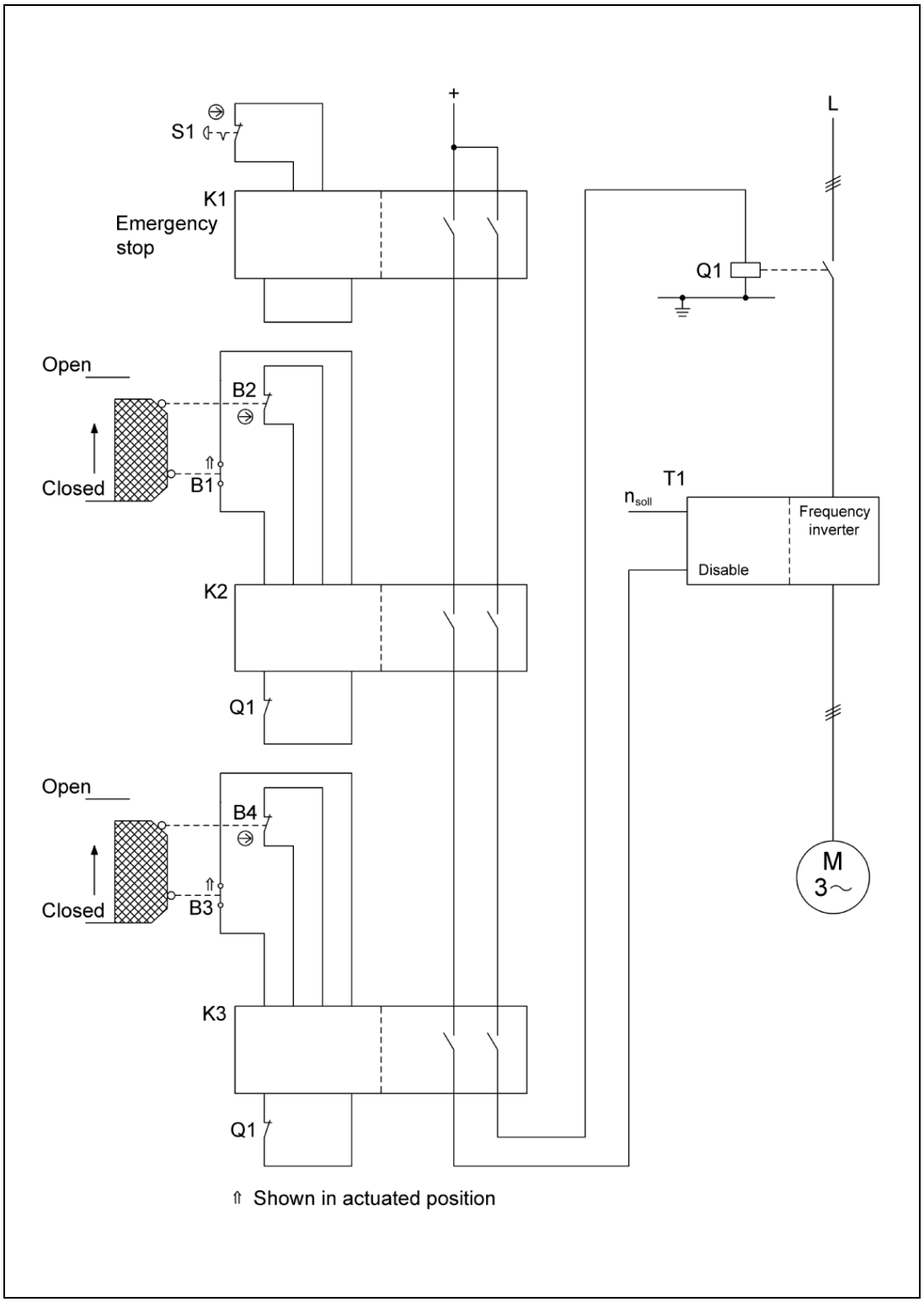
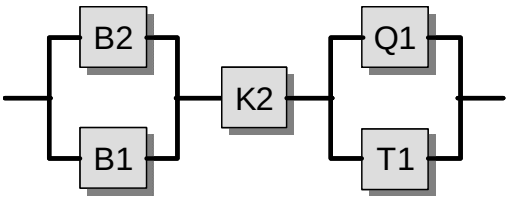
8.2.17 Cascading of protective devices by means of safety modules – Category 3 – PL d (Example 17)

Figure 8.31:
Cascading of protective devices by means of safety modules (emergency stop function, STO)





Safety functions

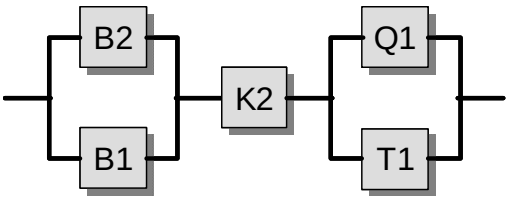
- Emergency stop function, STO – safe torque off by actuation of the emergency stop device
- Safety-related stop function, initiated by a protective device: opening of the moveable guard initiates the safety function STO – safe torque off.

Functional description

- Actuation of the emergency stop device S1 causes hazardous movements or states to be de-energized redundantly via the safety module K1, by interruption of the control voltage of the contactor Q1 and selection of the controller inhibit of the frequency inverter T1. A hazardous zone is also guarded by two moveable guards (e.g. one each for loading and unloading). Opening of the safety guard is detected by two position switches B1/B2 in a break contact/make contact combination, and evaluation by a central safety module K2. The latter can interrupt or prevent hazardous movements or states in the same way as K1. The second safety guard is monitored in the same way by the two position switches B3/B4 and a safety module K3, also acting upon Q1 and T1.
- The safety function is retained in the event of a component failure.
- The majority of component failures are detected and lead to operating inhibition. The two position switches on a safety guard are monitored for plausibility in the associated safety module. The safety module also employs internal diagnostics measures. Faults in the contactor Q1 are detected by means of mechanically linked contacts and their readback in K2 and K3. Additional readback in K1 is not necessary, since a demand for the emergency stop function is much less frequent. A part of the faults in T1 are detected by the process. A small number of faults are not detected by the controller.

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.
- A stable arrangement of the protective devices is assured for actuation of the position switches.
- The emergency stop device S1 corresponds to EN ISO 13850; B2 and B4 are position switches with direct opening contact to IEC 60947-5-1, Annex K.
- The supply conductors to the position switches B1 and B4 are laid separately or with protection.



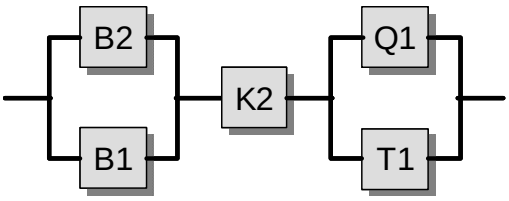
- The contactor Q1 possesses mechanically linked contact elements in accordance with IEC 60947-5-1, Annex L.
- The safety modules K1, K2 and K3 satisfy all the requirements for Category 4 and PL d.
- The frequency inverter T1 has no integral safety function.

Remark

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

Calculation of the probability of failure

- The circuit arrangement can be divided into three safety functions, each of which is assigned to three subsystems. The safety-related block diagram shows the safety-related stop function with reference to an example for one protective device, since only one protective device is open at any one time. The same safety function and an identical calculation of the probability of failure apply to the second protective device. For the emergency stop function, the emergency stop device S1 and the safety module K1 take the place of the first two subsystems. The probability of failure of the standard safety modules K1, K2 and K3 is added at the end of the calculation (2.31×10^{-9} per hour [M], suitable for PL e). For the remaining subsystems, the probability of failure is calculated as follows.
- S1 is a standard emergency stop device to EN ISO 13850. Fault exclusion applies for the direct opening contact and the mechanical elements, provided the number of operations indicated in Table D.2 of this report is not exceeded. Three actuations per year is assumed for n_{op}. This value is ignored for the purpose of further calculation for both safety functions with regard to the overall circuitry of Q1 and the frequency inverter.
- $MTTF_d$: fault exclusion is possible for the electrical contact of the position switch B2 with direct opening action. For the electrical make contact of the position switch B1, the B_{10d} value is 1,000,000 switching operations [M]. A B_{10d} value of 1,000,000 cycles [M] is stated for the mechanical part of B2 and B1. At 365 working days, 16 working hours and a cycle time of 10 minutes, n_{op} is 35,040 cycles per year for these components, and the $MTTF_d$ is 285 years for B2 and 142 years for B1. For the contactor Q1, the B_{10} value corresponds under inductive load (AC 3) to an electrical life 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. Since Q1 is involved in both safety-related stop functions,



double the value assumed above for n_{op} results in an $MTTF_d$ of 285 years. The $MTTF_d$ for the frequency inverter T1 is 20 years [M]. Altogether, the symmetrized $MTTF_d$ value per channel in the subsystem Q1/T1 is 68 years (“high”).

- DC_{avg}: the DC of 99% for B1 and B2 is based upon plausibility monitoring of the break contact/make contact combination in K2. This corresponds to the DC_{avg} for the subsystem. The DC of 99% for the contactor Q1 is derived from readback of the contact position in the safety modules. Fault detection by the process yields a DC of 60% for the frequency inverter T1. Averaging thus results in a DC_{avg} of 62% (“low”) for the subsystem Q1/T1.
- Adequate measures against common cause failure in subsystems B1/B2 and Q1/T2 (70 and 85 points respectively): separation (15), protection against overvoltage etc. (15) and environmental conditions (25 + 10), well-tried components in B2/B1 (5), diversity in Q1/T1 (20)
- The subsystem B1/B2 corresponds to Category 3 with a high $MTTF_d$ (100 years) and high DC_{avg} (99%). This results in an average probability of dangerous failure of 2.47×10^{-8} per hour. The subsystem Q1/T1 corresponds to Category 3 with a high $MTTF_d$ (68 years) and low DC_{avg} (62%). This results in an average probability of dangerous failure of 1.73×10^{-7} per hour.
- For the safety-related stop function, the resulting average probability of dangerous failure is 2.00×10^{-7} per hour. This corresponds to PL d.
- The resulting average probability of dangerous failure for the emergency stop function is 1.75×10^{-7} per hour. This corresponds to PL d.