8.2.6 Start/stop facility with emergency stop device – Category 1 – PL c (Example 6)

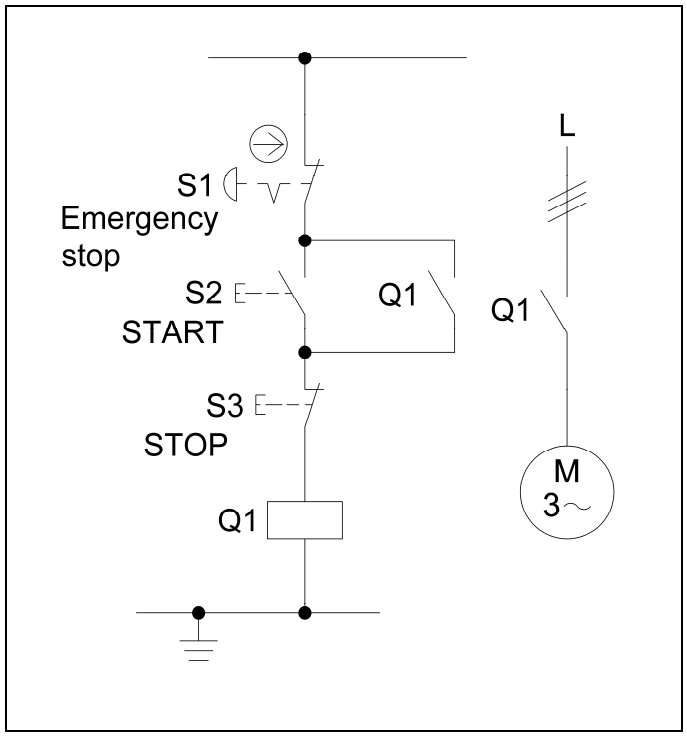


Figure 8.13:
Combined start/stop facility with emergency stop device

Safety function

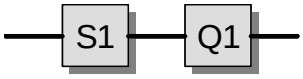
- Emergency stop function, STO – safe torque off by actuation of the emergency stop device

Functional description

- Hazardous movements or states are de-energized by interruption of the control voltage of contactor Q1 when the emergency stop device S1 is actuated.
- The safety function cannot be maintained with all component failures, and is dependent upon the reliability of the components.
- No measures for fault detection are implemented.

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 closed-circuit current principle is employed as a basic safety principle. The control circuit is also earthed, as a well-tried safety principle.



- The emergency stop device S1 is a switch with direct mode of actuation in accordance with IEC 60947-5-1, Annex K, and is therefore a well-tried component in accordance with Table D.4 of EN ISO 13849-2.
- The signal is processed by a contactor (stop category 0 to EN 60204-1).
- Contactor Q1 is a well-tried component provided the additional conditions in accordance with Table D.4 of EN ISO 13849-2 are observed.

Remark

- The function for stopping in an emergency is a protective measure which complements the safety functions for the safeguarding of hazardous zones.

Calculation of the probability of failure

- $MTTF_d$: 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. For contactor Q1, the B_{10} value corresponds under inductive load (AC 3) to an electrical lifetime of 1,300,000 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. If the start/stop facility is assumed to be actuated twice a day on 365 working days and the emergency stop device to be actuated three times a year, then at an n_{op} of 733 cycles per year, Q1 has an $MTTF_d$ of 35,470 years. This is also the $MTTF_d$ for the channel, which is capped to 100 years (“high”).
- DC_{avg} and measures against common cause failures are not relevant in Category 1.
- The electromechanical control system corresponds to Category 1 with a high $MTTF_d$ (100 years). This results in an average probability of dangerous failure of 1.14×10^{-6} per hour. This corresponds to PL c.

More detailed references

- EN ISO 13850: Safety of machinery – Emergency stop – Principles for design (11.06)
- EN 60204-1: Safety of machinery – Electrical equipment of machines. Part 1: General requirements (06.06)