8.2.5 Position monitoring of moveable guards – Category 1 – PL c (Example 5)
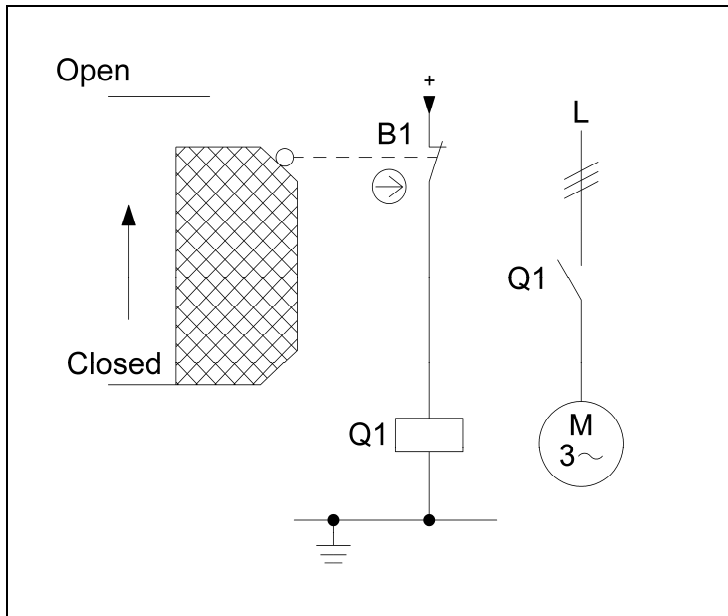

Figure 8.11:
Position monitoring of move-able guards for the prevention of hazardous movements (STO – safe torque off)
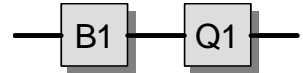
Safety function

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

Functional description

- Opening of the moveable guard (e.g. safety guard) is detected by a position switch B1 with direct opening action which actuates a contactor Q1. The dropping out of Q1 interrupts or prevents hazardous movements or states.

- 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.

- Removal of the protective device is not detected.

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. Earthing of the control circuit is regarded as a well-tried safety principle.

B1 — Q1

- Switch B1 is a position switch with direct opening action in accordance with IEC 60947-5-1, Annex K and is therefore regarded as a well-tried component. The break contact interrupts the circuit directly mechanically when the protective device is not in the safe position.

- Contactor Q1 is a well-tried component provided that the additional conditions in accordance with Table D.4 of EN ISO 13849-2 are observed.

- A position switch is employed for position monitoring. A stable arrangement of the protective device is assured for actuation of the position switch. The actuating elements of the position switch are protected against displacement. Only rigid mechanical parts (no spring elements between actuator and contact) are employed.

- The actuating stroke for the position switch complies with the manufacturer's specification.

Calculation of the probability of failure

- $MTTF_d$: fault exclusion for the direct opening electrical contact is possible for B1. A B_{10d} value of 1,000,000 cycles [M] is stated for the mechanical part of B1. At 365 working days, 16 working hours per day and a cycle time of 10 minutes, n_{op} is 35,045 cycles per year and the $MTTF_d$ is 285 years for these components. For contactor Q1, the B_{10} value corresponds under inductive load (AC 3) to an electrical lifetime of 1,300,000 switching cycles [M]. If 50% of failures are assumed to be dangerous, the B_{10d} value is produced by doubling of the B_{10} value. The above assumed value for n_{op} results in an $MTTF_d$ of 742 years for Q1. The combination of B1 and Q1 results in an $MTTF_d$ of 206 years for the channel. This value 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. The PL_r of b is therefore surpassed.

More detailed reference

- IEC 60947-5-1: Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices (11.03)
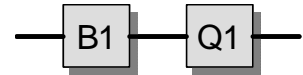
Figure 8.12:
Determining of the PL by means of SISTEMA