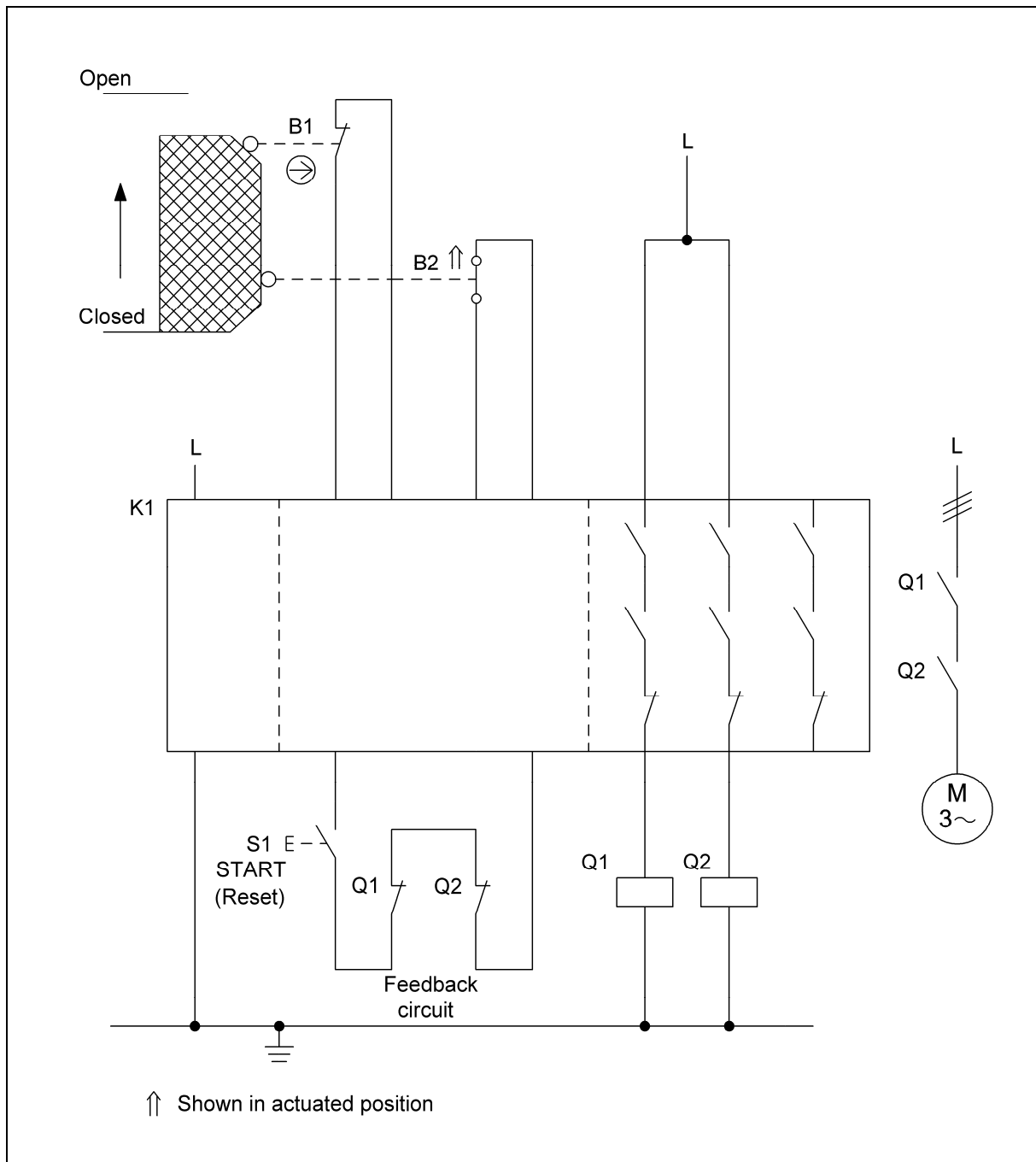


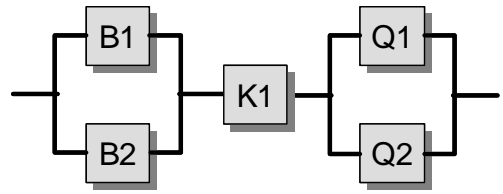
8.2.34 Position monitoring of moveable guards – Category 4 – PL e (Example 34)

Figure 8.58:
Position monitoring of moveable guards by means of a safety module



Safety function

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



Functional description

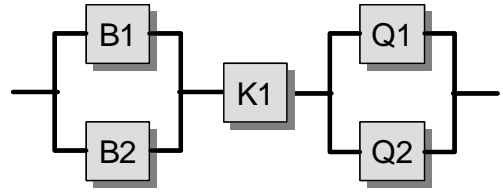
- A hazardous zone is safeguarded by a moveable guard (safety guard). Opening of the safety guard is detected by two position switches B1/B2, employing a break contact/make contact combination, and evaluation by a central safety module K1. K1 actuates two contactors, Q1 and Q2, dropping out of which interrupts or prevents hazardous movements or states.
- The position switches are monitored for plausibility in K1 for the purpose of fault detection. Faults in Q1 and Q2 are detected by a start-up test in K1. A start command is successful only if Q1 and Q2 had previously dropped out. Start-up testing by opening and closing of the protective device is not required.
- The safety function remains intact in the event of a component failure. Faults are detected during operation or at actuation (opening and closing) of the protective device by the dropping out of Q1 and Q2 and operating inhibition.
- An accumulation of more than two faults in the period between two successive actuations may lead to loss of the safety function.

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.
- Switch B1 is a position switch with direct opening contact in accordance with IEC 60947-5-1, Annex K.
- The supply conductors to position switches B1 and B2 are laid separately or with protection.
- The safety module K1 satisfies all requirements for Category 4 and PL e.
- The contactors Q1 and Q2 possess mechanically linked contact elements to IEC 60947-5-1, Annex L.

Remark

- Category 4 is observed only if multiple mechanical position switches for different protective devices are not connected in a series arrangement (i.e. no cascading), since faults in the switches cannot otherwise be detected.



Calculation of the probability of failure

- The circuit arrangement can be divided into three subsystems as shown in the safety-related block diagram. The probability of failure of the standard safety module K1 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.
- *MTTF_d*: fault exclusion is possible for the electrical contact of the position switch B1 with direct opening action. For the electrical make contact of the position switch B2, 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 B1 and B2. At 365 working days, 16 working hours per day and a cycle time of 1 hour, n_{op} is 5,840 cycles per year for these components, and the *MTTF_d* is 1,712 years for B1 and 856 years for B2. For the contactors Q1 and Q2, 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. The value assumed above for n_{op} results in an *MTTF_d* of 3,424 years per channel for Q1 and Q2. Altogether, the symmetrized *MTTF_d* value per channel in the two subsystems is 100 years ("high").
- *DC_{avg}*: the *DC* of 99% for B1 and B2 is based upon plausibility monitoring of the break/make contact combination in K1. The *DC* of 99% for contactors Q1 and Q2 is derived from regular monitoring by K1 during start-up. The *DC* values stated correspond to the *DC_{avg}* for each subsystem.
- Adequate measures against common cause failure in the subsystems B1/B2 and Q1/Q2 (70 points): separation (15), well-tried components (5), protection against overvoltage etc. (15) and environmental conditions (25 + 10)
- The subsystems B1/B2 and Q1/Q2 each correspond to Category 4 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. Following addition of the subsystem K1, the average probability of dangerous failure is 5.16×10^{-8} per hour. This corresponds to PL e.