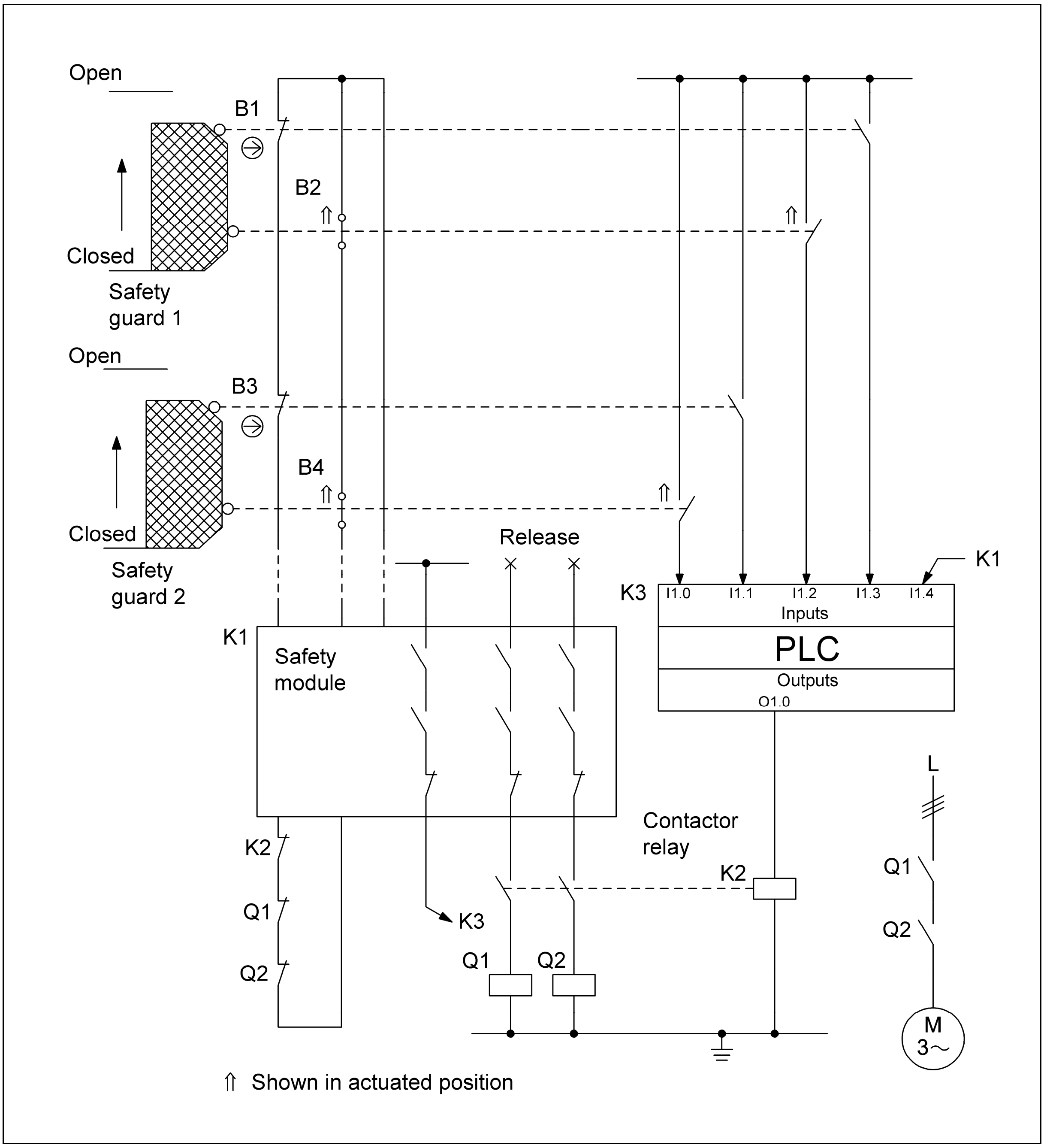
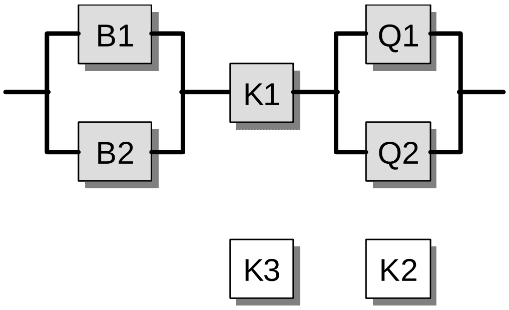
8.2.28 Position monitoring of moveable guards – Category 4 – PL e (Example 28)

Figure 8.49:
Position monitoring of moveable guards for the prevention of hazardous movements



Safety function

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

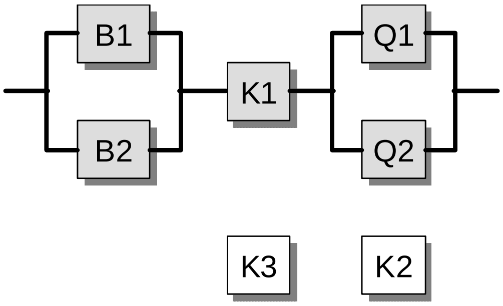


Functional description

- A hazardous zone is safeguarded by two moveable guards (safety guards). Opening of the two safety guards is detected by two position switches B1/B2 and B3/B4 comprising break contact/make contact combinations and evaluated by a central safety module K1. K1 actuates two contactors, Q1 and Q2, dropping out of which interrupts or prevents hazardous movements or states.
- For fault detection purposes, all position switch states are read by a second contact into a standard PLC K3, the chief purpose of which is functional control. In the event of a fault, K3 can de-energize the contactors Q1 and Q2 independently of K1 by means of a contactor relay K2. Faults in K2, Q1 and Q2 are detected by the safety module K1. A small number of faults are not detected (e.g. failure of the contacts in B2 and B4 to break).
- The safety function is retained in the event of a component failure. The majority of component failures are detected and lead to operating inhibition. An accumulation of undetected faults does not result in 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.
- B1 and B3 are position switches with direct opening contacts according to IEC 60947-5-1, Annex K.
- The supply conductors to the position switches are laid separately or with protection.
- Faults in the start-up and actuation mechanism are detected by the use of two position switches differing in the principle of their actuation (break and make contact combination).
- Several protective devices may be cascaded.
- The safety module K1 satisfies all requirements for Category 4 and PL e.
- The contactors K2, Q1 and Q2 possess mechanically linked contact elements to IEC 60947-5-1, Annex L.



- The PLC K1 satisfies the normative requirements described in Section 6.3.

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 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. Since each safety guard forms part of a dedicated safety function, calculation is shown here by substitution for protective device 1.
- $MTTF_d$: fault exclusion is possible for the electrical contact of the position switch B1 with direct opening contact. 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 combinations in the PLC K3. The *DC* of 99% for the contactors Q1 and Q2 is derived from monitoring at each energization of K1. The DC values stated correspond to the DC_{avg} of the subsystem concerned.
- 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 both 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 in each case 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.