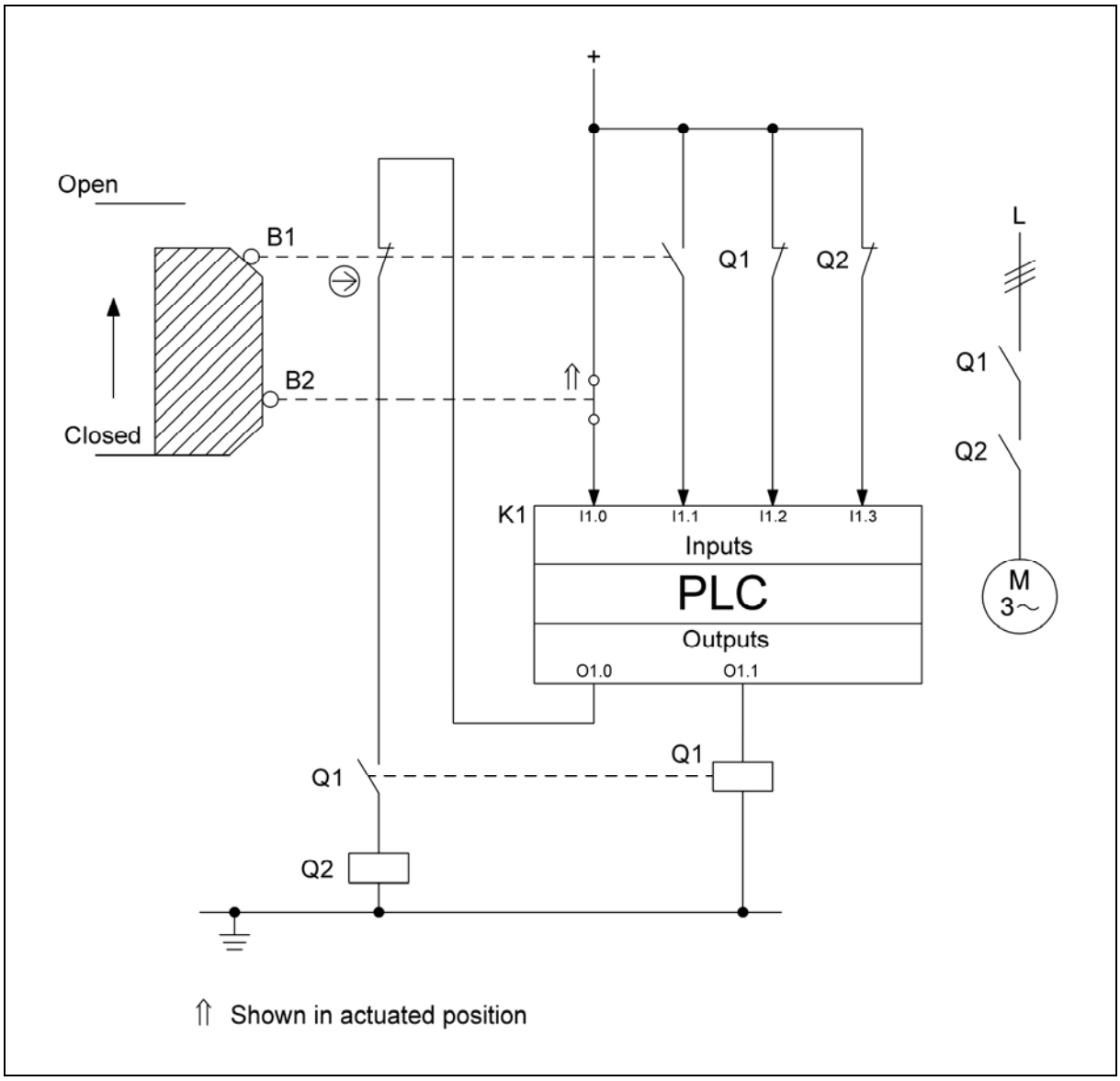
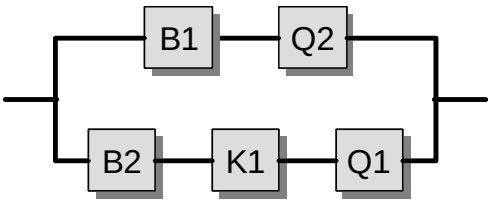
8.2.18 Position monitoring of a moveable guard – Category 3 – PL d (Example 18)

Figure 8.32:
Redundant position monitoring of a moveable guard employing diversity in its technical implementation (electromechanical and programmable electronic)



Safety function

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

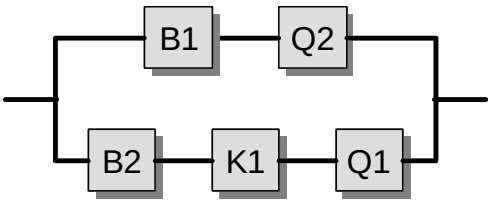


Functional description

- Opening of the moveable guard (e.g. safety guard) is detected by two position switches B1 and B2 in a break contact/make contact combination. The position switch B1 with direct opening contact actuates a contactor Q2 which interrupts/ prevents hazardous movements or states when it drops out. The position switch B2 with make contact is read in by a standard PLC K1, which can bring about the same de-energization response by actuation of a second contactor Q1.
- The safety function is retained in the event of a component failure.
- The switching position of B1 is also read into the PLC K1 by means of a make contact, and is compared for plausibility with the switching position of B2. The switching positions of the contactors Q1 and Q2 are likewise monitored in K1 by mechanically linked readback contacts. Component failures in B1, B2, Q1 and Q2 are detected by K1 and lead to operating inhibition owing to the dropping-out of Q1 and Q2. Faults in the PLC K1 are detected only by the function (fault detection by the process).

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 device is assured for actuation of the position switch.
- B1 is a position switch with direct opening contact in accordance with 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 contacts).
- 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

- $MTTF_d$: 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} 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 under inductive load (AC3) corresponds to an electrical life 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. The above assumed value for n_{op} results in an $MTTF_d$ of 4,452 years for Q1 and Q2. An MTTF value of 15 years [M] is substituted for the PLC, resulting through doubling in an $MTTF_d$ value of 30 years. The combination of B1 and Q2 results in an $MTTF_d$ of 1,236 years for the first channel; B2, K1 and Q2 contribute to an $MTTF_d$ of 28 years in the second channel. Altogether, the $MTTF_d$ value symmetrized over both channels is 70 years per channel (“high”).
- DC_{avg}: the DC of 99% for B1 and B2 is based upon plausibility monitoring of the two switching states in the PLC K1. The DC of 99% for the contactors Q1 and Q2 is derived from readback via mechanically linked contact elements, also in K1. Owing to the possibility of fault detection by the process, a DC of 60% is assumed for K1. Averaging thus results in a DC_{avg} of 62% (“low”).
- Adequate measures against common cause failure (65 points): separation (15), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the control elements corresponds to Category 3 with a high $MTTF_d$ (70 years) and low DC_{avg} (62%). This results in an average probability of dangerous failure of 1.66×10^{-7} per hour. This corresponds to PL d.

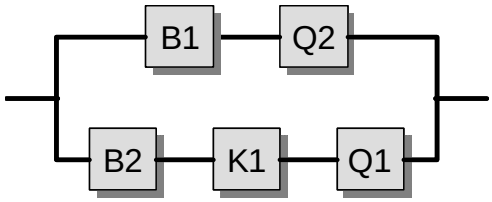


Figure 8.33:
Determining of the PL by means of SISTEMA