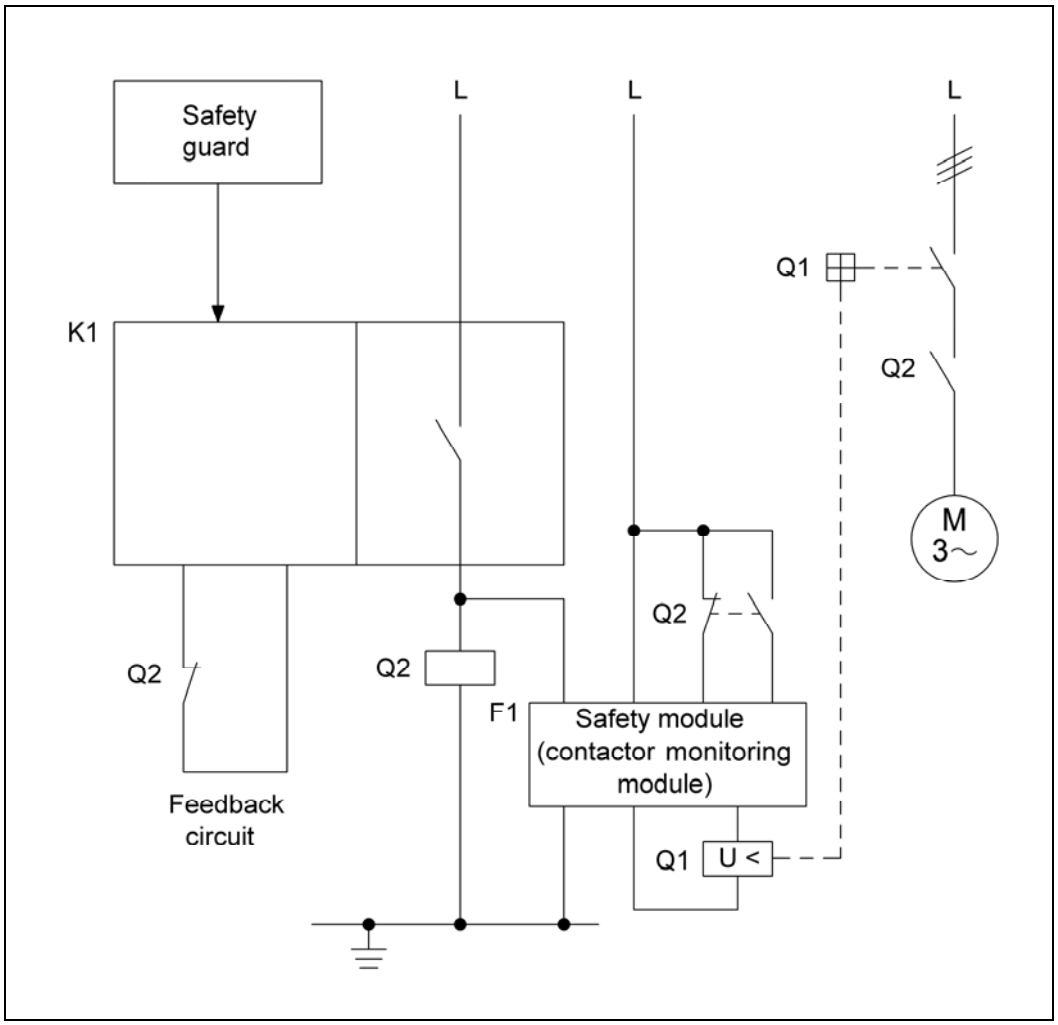
8.2.30 Contactor monitoring module – Category 3 – PL e (Example 30)

Figure 8.52:
Initiation of STO (safe torque off) by means of a safety module and contactor monitoring module

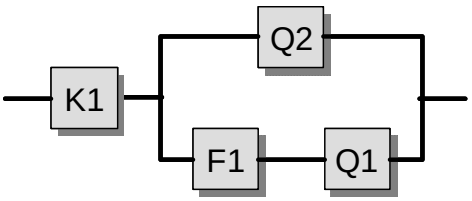


Safety function

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

Functional description

- A hazardous zone is safeguarded by means of a protective device the opening of which is detected by a safety module K1. The latter actuates a contactor Q2 and a combination of a contactor monitoring module F1 and an undervoltage release Q1. The dropping-out of Q2 interrupts hazardous movements and prevents hazardous states. The contactor monitoring module F1 has the function of monitoring the main contacts of contactor Q2 for contact welding. Should Q2 fail to drop out, F1 trips the upstream circuit-breaker or motor starter Q1 via the



latter's undervoltage release. The circuit-breaker or motor starter then switches off the motor.

- The safety function is retained in the event of a component failure.
- An accumulation of faults between two successive actuations may lead to loss of the safety function.

Design features

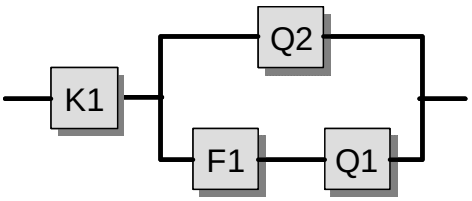
- Circuit-breaker Q1 is checked regularly by means of a test function which is to be implemented manually. The interval between the tests should not exceed one-hundredth of the $MTTF_d$ of Q1; the test could be performed for example during maintenance of the machine. The contactor Q2 is tested continually by the contactor monitoring module. Loss of the safety function between the tests, as is possible with Category 2, cannot occur. The single-fault tolerance is thus assured and the requirements of Category 3 are met.
- 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.
- For reasons of simplification, details of the protective device have been omitted from the presentation.
- The protective device acts upon a safety module K1 which satisfies all requirements for Category 3 or 4 and PL e.
- Contactor Q2 features mirror contacts to IEC 60947-4-1, Annex F, and is integrated into the feedback of safety module K1 for contactor fault detection.
- Fault consideration for Q2 (with mirror contacts) and for the internal relay of the contactor monitoring module F1 is as for mechanically linked contacts.

Remark

- Consideration must be given to the response time caused by contactor monitoring module F1 with regard to the dropping-out of Q1.

Calculation of the probability of failure

- The safety function permits division into two subsystems. The subsystem consisting of the protective device and safety module K1 is not considered in this example.
- $MTTF_d$: for the contactor monitoring module F1, the $MTTF_d$ is 125 years at a maximum n_{op} of 350,400 cycles per year [M]. Under inductive load (AC 3), the B_{10d} value for Q1 is 10,000 switching cycles, and the B_{10d} value for Q2



1,300,000 switching cycles. Assuming a once daily actuation on 365 working days, n_{op} is 365 cycles per year for Q1, and the $MTTF_d$ is 274 years. At 365 working days, 16 working hours per day and a cycle time of 1 minute, n_{op} is 350,400 cycles per year for Q2, and the $MTTF_d$ is 37 years. For the channel consisting of F1 and Q1, this results in an $MTTF_d$ of 85 years. Overall, the resulting symmetrized $MTTF_d$ value per channel is 64 years (“high”).

- DC_{avg}: the *DC* of 99% for Q2 is based upon testing by means of the contactor monitoring module F1. A *DC* of 99% for F1 is achieved by fault-detection measures within the contactor monitoring module. The circuit-breaker is tested by means of the manual test function which is to be implemented; this produces a *DC* of 90%. A *DC* of 99% is substituted for F1. Averaging thus yields a DC_{avg} of 98% (“medium”).
- Adequate measures against common cause failure (65 points): separation (15), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The subsystem comprising Q1, Q2 and F1 corresponds to Category 3 with a high $MTTF_d$ (64 years) and medium DC_{avg} (98%). This results in an average probability of dangerous failure of 4.45×10^{-8} per hour. This corresponds to PL e. Following addition of the subsystem comprising protective device and safety module K1, the PL may under certain circumstances be lower.
- In consideration of estimation erring on the safe side as described above, a T_{10d} value of 3.7 years is produced for the wearing element Q2 when replaced as specified.