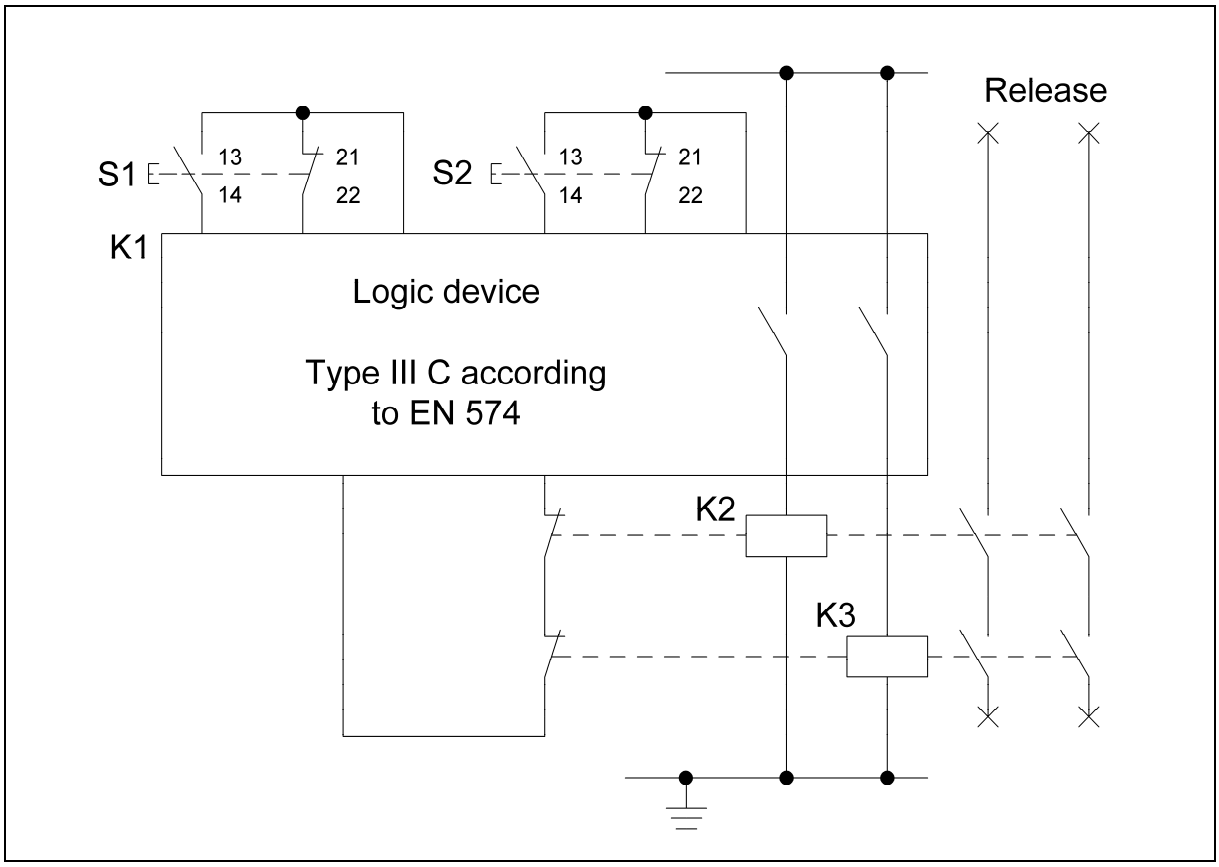
8.2.35 Two-hand control – Category 4 – PL e (Example 35)

Figure 8.59:
Two-hand control, signal processing by a logic device with downstream contactor relays

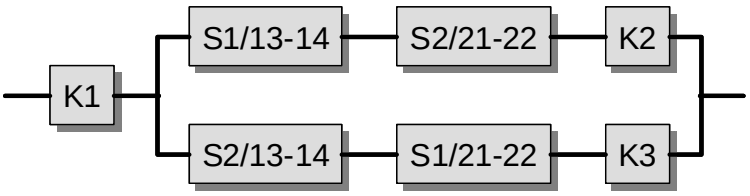


Safety function

- Controlled location of the operator's hands outside the hazardous area during a hazardous movement: when at least one of the two pushbuttons S1/S2 is released, enabling is cancelled and remains blocked until both pushbuttons are released and pressed again synchronously.

Functional description

- The logic device K1 monitors operation of the actuators (pushbuttons) S1 and S2. Only when both pushbuttons are operated synchronously (i.e. within a specified time) from the released state do the contactor relays K2 and K3 pick up and cause enabling. When at least one of the pushbuttons S1/S2 is released, K2/K3 cancel enabling.
- K2 and K3 have the function of contact multiplication/load adaptation. The actual prevention of the hazardous movement, for example by separation of the electrical or hydraulic energy, is dependent upon the application and is not shown here.



- Faults in the actuating mechanism are detected in S1/S2 to the greatest extent possible by the use of two contacts employing different principles (break and make contact combination). With regard to mechanical faults for this application, a fault exclusion is possible for failure of the break contact to open, provided the pushbuttons satisfy IEC 60947-5-1.
- Faults in S1/S2 and in K2/K3 (with break contacts in the feedback circuit) are detected in K1 and lead to sustained de-energization via K2 and K3. All individual faults are detected at or prior to the next demand upon the safety function.
- Frequent actuation of the electromechanical elements results in a sufficiently high test rate (forced dynamics).

Design features

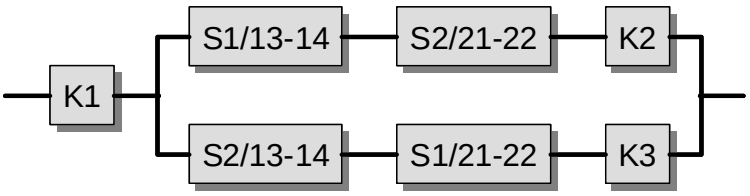
- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in Section 8.1 are implemented.
- The actuators S1 and S2 of the two-hand control satisfy IEC 60947-5-1.
- Faults in the conductors to S1 and S2 are detected in the logic device. If this were not possible, the conditions to EN ISO 13849-2, Table D.4 for a fault exclusion for conductor short-circuits would have to be observed. Owing to the low currents, pushbuttons with gold-plated contacts are recommended.
- Refer to EN 574 Section 8 with regard to fitting of the pushbuttons and to measures for the avoidance of accidental actuation and manipulation. The distance from the hazardous area must be sufficiently large.
- The logic device K1 corresponds to Type III C in accordance with EN 574, with self-monitoring and detection of internal faults. K1 is a tested safety component for use in Category 4 and PL e.
- K2 and K3 possess mechanically linked break contacts for readback.

Remark

- Application for example on mechanical presses (EN 692)

Calculation of the probability of failure

- K1 is treated as a subsystem with a probability of failure of 2.47×10^{-8} per hour [E]. The remaining part of the control system is grouped to form a Category 4 subsystem the probability of failure of which is calculated below.
- Since S1 and S2 must trigger de-energization independently of each other when released, they are connected logically in series. For this purpose, one



make contact 13-14 and one break contact 21-22 for each pushbutton were assigned to a control channel. The safety-related block diagram differs substantially in this respect from the functional circuit diagram. If the reliability data is available only for the pushbuttons as a whole (actuation mechanism and break and make contacts), the failure values for the pushbuttons may be employed as the failure values for the contacts (plus operating mechanism), constituting an estimation erring on the safe side.

- $MTTF_d$: owing to the defined control current generated by K1 (small load, the mechanical lifetime of the contacts is the determining factor), B_{10d} values of 20,000,000 switching operations [M] are assumed in each case for S1 and S2. Since K2 and K3 also switch control currents, B_{10d} values of 20,000,000 cycles [S] apply to each of them. At 240 working days, 8 working hours and a cycle time of 20 seconds, n_{op} is 345,600 cycles per year for these components and the $MTTF_d$ is 579 years. Should the requirements be higher (longer working hours or a shorter cycle time), higher B_{10d} values validated by the manufacturer may be required for K2/K3. Overall, the resulting $MTTF_d$ value per channel is 193 years, capped to 100 years (“high”).
- DC_{avg}: a *DC* of 99% for S1 and S2 is produced by virtue of direct monitoring with the aid of the break and make contact combinations in K1. The *DC* of 99% for K2 and K3 is based upon readback of the mechanically linked break contacts in the feedback circuit of K1. The high frequency of actuation in the application constitutes effective testing. Averaging results in a DC_{avg} of 99% (“high”).
- Adequate measures against common cause failure (70 points): separation (15), FMEA (15), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the control elements corresponds to Category 4 with a high $MTTF_d$ per channel (100 years) and high DC_{avg} (99%). For the combination of S1, S2, K2 and K3, the average probability of dangerous failure is calculated at 2.47×10^{-8} per hour. If a value of 2.47×10^{-8} per hour [E] for K1 is added, the result is an average probability of dangerous failure of 4.94×10^{-8} per hour. This corresponds to PL e. The probability of failure of downstream power components may have to be added for completion of the safety function.

More detailed references

- EN 574: Safety of machinery – Two-hand control devices – Functional aspects – principles for design (11.96)
- Recommendation for Use. Ed.: Vertical Group 11 (VG 11) in the Co-ordination of Notified Bodies. CNB/M/11.033/R/E Rev 05, p. 252, April 2006. http://europa.eu/comm/enterprise/mechan_equipment/machinery/vertical_rfu.pdf