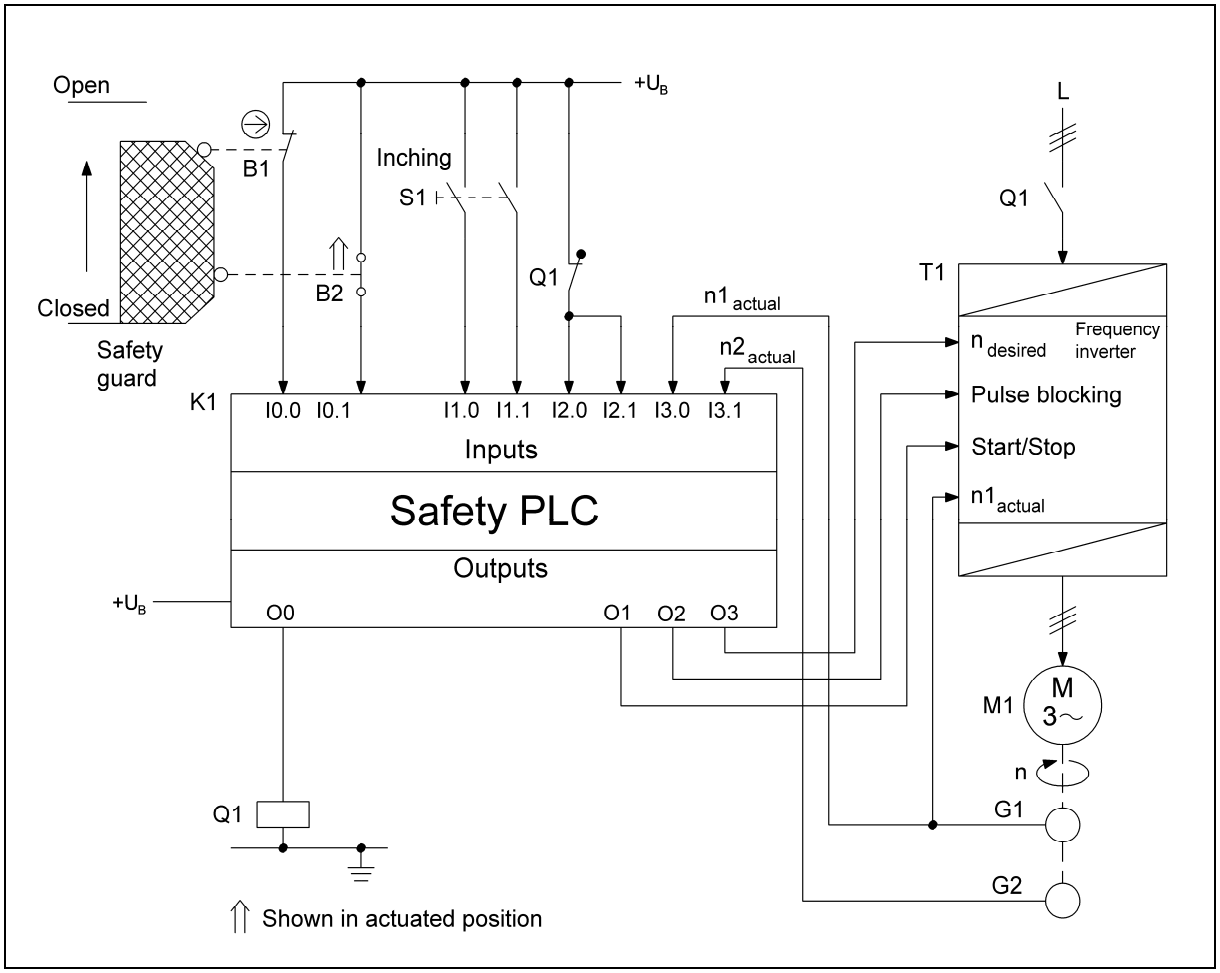
8.2.21 Safely limited speed for inching mode – Category 3 – PL d (Example 21)

Figure 8.37:
Inching mode with safely limited speed when the safety guard is open, with desired/actual value comparison and defined speed limit value within a safety PLC

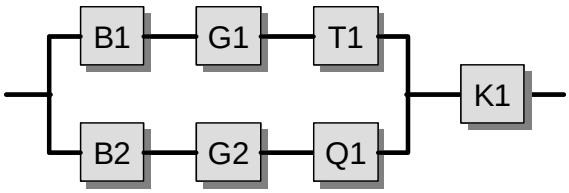


Safety function

- Safely limited speed (SLS): when the safety guard is open, exceeding of a permissible speed in inching mode is prevented.

Functional description

- A hazardous movement is safely prevented or interrupted when the safety guard is open. Opening of the safety guard is detected by two position switches B1 and B2 in a break contact/make contact combination. When the pushbutton S1 is actuated a safely limited speed is set on the frequency inverter T1 by means of the safety PLC K1. The two processing channels within the PLC each receive limit value settings independently of each other from their appli-

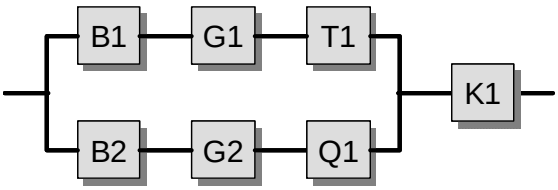


cation software. The actual rotational speed value of the inching speed on the inputs I3.0 and I3.1 of K1 is monitored by two separate tachogenerators G1 and G2. Each channel of the PLC performs the desired/actual speed comparison independently. Should the speed not be reduced successfully to the limited value by means of T1, K1 can initiate a halt by blocking of the start/stop signal and pulse blocking on the inverter. The power supply to T1 can also be interrupted by a mains contactor Q1.

- Safety-related data is exchanged through an internal interface in the safety PLC K1. Such data is employed for example for fault detection by a state comparison between the two processing channels. Should one processing channel fail, the remaining functioning processing channel reduces the speed of the inverter T1 and de-energizes the mains contactor Q1. A failure of the inverter which could for example lead to unexpected start-up, continued running or an increase in the speed is detected by separate monitoring of the speed by the tachogenerators G1 and G2 in both processing channels. Failure of the mains contactor Q1 to drop out is detected by the break contacts present in both processing channels (inputs I2.0 and I2.1 of K1), and leads both to blocking of the start/stop signal and to pulse blocking on the inverter by both processing channels.

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.
- The position switch B1 features direct opening action in accordance with IEC 60947-5-1, Annex K. The position switch B2 also complies with IEC 60947-5-1.
- The contactor Q1 possesses a mirror contact according to IEC 60947-4-1, Annex F.
- The supply conductors to the position switches are laid either separately or with protection against mechanical damage.
- For the safety function “safely limited speed”, a fault exclusion is assumed for the fault condition of encoder shaft breakage (G1/G2). Details of the possibility of a fault exclusion can be found for example in IEC 61800-5-2, Table D.16.
- The standard components G1 and G2 (where relevant for the rotary signal encoders) and T1 are employed in accordance with the instructions in Section 6.3.10.



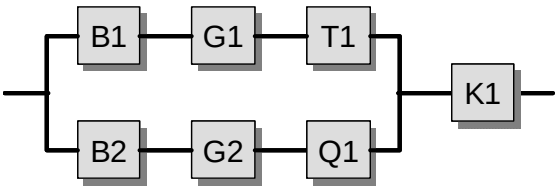
- The safety component K1 satisfies all requirements for Category 3 and PL d. The software (SRASW) is programmed in accordance with the requirements for PL d and the instructions in Section 6.3.
- It is assumed that each output of the safety PLC is actuated by both processing channels of the PLC (exception: O3).

Remarks

- According to EN 1010-1, the use of one position switch with direct opening action to IEC 60947-5-1, Annex K for each interlocked guard is sufficient on machines without routine operator intervention at danger points. Fault exclusion in this context is conditional upon the switch being installed in accordance with EN 60204-1.
- For full implementation of inching mode, the safety function “no unexpected start-up in inching mode” must also be considered.

Calculation of the probability of failure

- The SRP/CS is divided into the two subsystems sensor/actuator and PLC. For the PLC subsystem, a tested safety PLC suitable for PL d is employed. This PLC's probability of failure of 1.5×10^{-7} per hour [E] is added at the end of the calculation for the sensor/actuator subsystem. For production of the block diagram, refer also to Figure 6.14 and the corresponding comments in the associated text. The probability of failure for the sensor/actuator subsystem is calculated below.
- $MTTF_d$: at 240 working days, 8 working hours and a cycle time of one hour, n_{op} is 1,920 cycles per year. A B_{10d} value of 20,000,000 cycles [S] is assumed for the position switch B1 owing to its direct opening action; the associated $MTTF_d$ value is 104,116 years. Owing to the defined control current (low load; the mechanical lifetime of the contacts is the determining factor), for the position switch B2 a B_{10d} value of 1,000,000 cycles [E] is assumed (see also Table D.2), and therefore an $MTTF_d$ of 5,208 years. The contactor Q1 with a B_{10d} value of 400,000 cycles switches operationally only once daily, corresponding to a n_{op} of 240 cycles per year and an $MTTF_d$ of 16,667 years. The following values are estimated: an $MTTF_d$ of 100 years for T1 and an $MTTF_d$ of 50 years for G1/G2 [E]. These values produce a symmetrized $MTTF_d$ for each channel of 41 years (“high”).
- DC_{avg}: for each of the components used, a DC of 99% is assumed. For the position switches and the tachogenerators, this value is based upon cross-checking of input signals in K1. For the inverter T1, fault detection is provided by the



process; the mains contactor Q1 is monitored directly by the PLC. These values produce a DC_{avg} of 99% (“high”).

- Adequate measures against common cause failure (70 points): separation (15), FMEA (5), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The sensor/actuator subsystem corresponds to Category 3 with a high $MTTF_d$ per channel (41 years) and high DC_{avg} (99%). This results in an average probability of dangerous failure of 6.56×10^{-8} per hour. This corresponds to PL e. PL_r d is thus surpassed, which with the required two-channel design of the hardware with few components, the use of B_{10d} values in accordance with the standard, a *DC* of “high” and a “moderate” switching frequency will virtually always be the case.
- The overall probability of failure is determined by addition of the probability of dangerous failure of K1 (1.5×10^{-7} per hour) and is 2.16×10^{-7} per hour. This corresponds to PL d.

More detailed references

- *Grigulewitsch, W.; Reinert, D.*: Schaltungsbeispiele mit programmierbaren Steuerungen zur Umsetzung der Steuerungskategorie 3. In: BGIA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. Kennzahl 330 227. 27th suppl. I/95. Ed.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin 1985 – loose-leaf ed.
  www.bgia-handbuchdigital.de/330227
- IEC 61800-5-2: Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional (07.07)
- EN 1010-1: Safety of machinery – Safety requirements for the design and construction of printing and paper converting machines – Part 1: Common requirements (12.04)