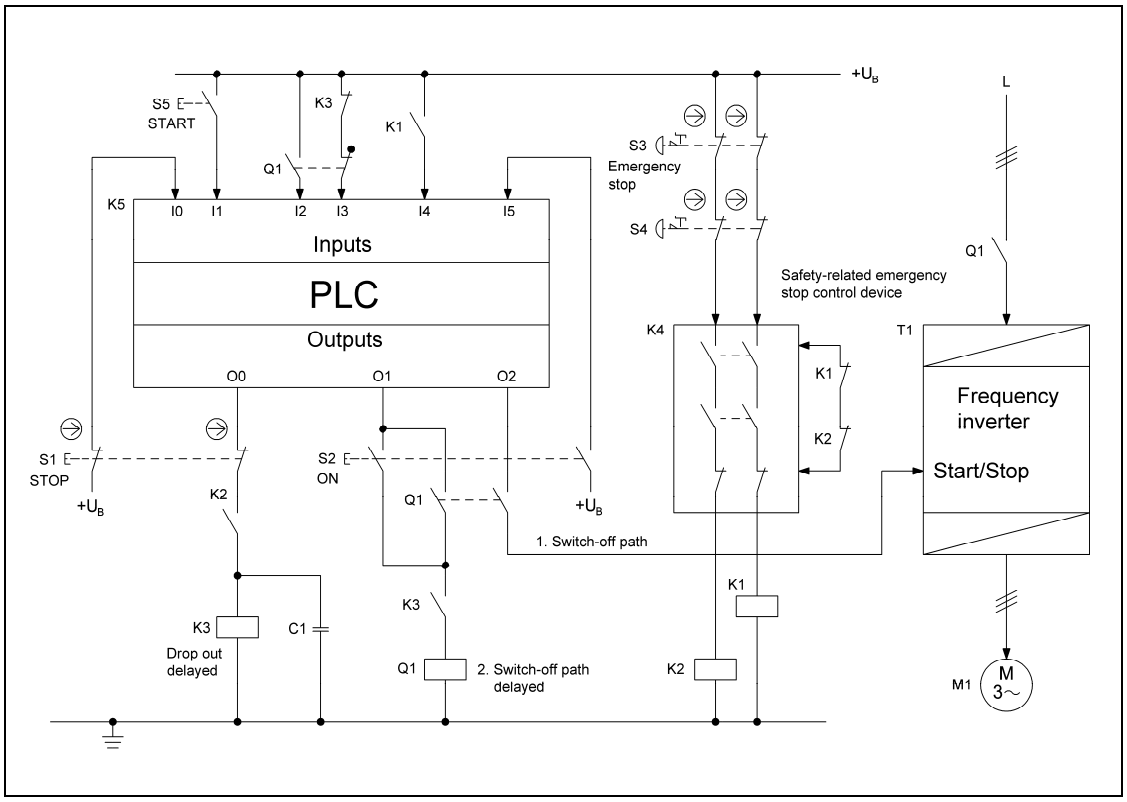
8.2.10 Safe stopping of a PLC-driven drive with emergency stop – Category 3 – PL c (Example 10)

Figure 8.19:
Stopping of a PLC-driven frequency inverter drive following a stop or emergency stop command

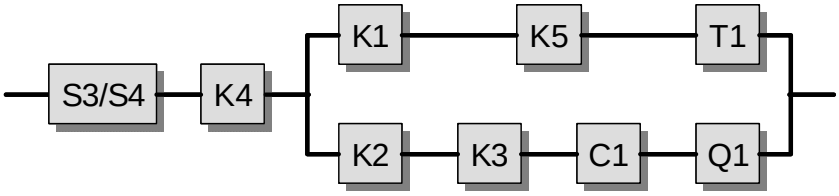


Safety function

- Safety-related stop function/emergency stop function: following a stop or emergency stop command, the drive is halted (SS1 – safe stop 1).

Functional description

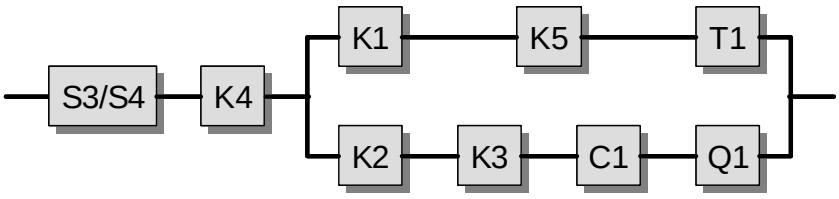
- The hazardous movement is interrupted redundantly if either the stop button S1 or one of the emergency stop devices S3 or S4 is actuated. The drive is halted in an emergency following actuation of S3/S4, resulting in deactivation of the safety-related emergency stop control device K4 and de-energization of the contactor relays K1 and K2. Opening of the make contact K1 on input I4 of the PLC K5 causes the starting signal on the frequency inverter (FI) T1 to be cancelled via the PLC output O2. Redundantly to the K1-K5-T1 chain, opening of the make contact K2 upstream of the contactor relay K3 (with drop-out delay) initiates a braking timer. Upon timeout of the braking timer the actuating signal for the mains contactor Q1 is interrupted. The timer setting is selected such that under unfavourable operating conditions, the machine movement is halted before the mains contactor Q1 has dropped out.



- Functional stopping of the drive following a stop command is caused by the opening of the two break contacts of the stop button S1. As with stopping in an emergency, the status is first queried by PLC K5, in this case via input I0, and the FI is shut down by resetting of the PLC output O2. Redundantly to this process, the contactor relay K3 is de-energized – with drop-out delay provided by the capacitor C1 – and following timeout of the set braking time, the activation signal to mains contactor Q1 is interrupted.
- In the event of failure of the PLC K5, the frequency inverter T1, the mains contactor Q1, the contactor relays K1/K2 or the contactor relay with drop-out delay K3, stopping of the drive is assured since two mutually independent de-energization paths are always present. Failure of the contactor relays K1 and K2 to drop out is detected, at the latest, following resetting of the actuated emergency stop device. This is achieved by monitoring of the mechanically linked break contacts within the safety-related emergency stop control device K4. Failure of the auxiliary contactor K3 to drop out is detected, at the latest, before renewed start-up of the machine movement through feedback of the mechanically linked break contact to the PLC input I3. Failure of the mains contactor Q1 to drop out is detected by the mirror contact read in on PLC input I3.

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.
- The contactor relays K1, K2 and K3 possess mechanically linked contact elements in accordance with IEC 60947-5-1, Annex L.
- The contacts of the pushbuttons S1, S3 and S4 are mechanically linked in accordance with IEC 60947-5-1, Annex K.
- The contactor Q1 possesses a mirror contact according to IEC 60947-4-1, Annex F.
- The standard components K5 and T1 are employed in accordance with the instructions in Section 6.3.10.
- The software (SRASW) is programmed in accordance with the requirements for PL b (downgraded owing to diversity) and the instructions in Section 6.3.
- The delayed initiation of the stopping by the second de-energization path alone in the event of a fault must not involve an unacceptably high residual risk.
- The safety-related control part of the safety-related emergency stop control device K4 satisfies all requirements for Category 3 and PL d.



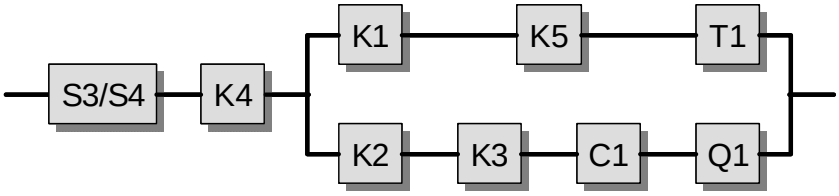
Calculation of the probability of failure

Only the probability of failure of the emergency stop function is calculated. For analysis of the safety-related stop function, S3/S4 and K4 must be replaced by S1, and K1 and K2 omitted.

- Fault exclusion is assumed for the emergency stop devices S3/S4, since the maximum number of 6,050 switching cycles within the mission time of the switching device as stated in Table D.2 is not exceeded. The safety-related emergency stop control device K4 is a tested safety component. Its probability of failure is 3.0×10^{-7} per hour [M], and is added at the end of the calculation. The value applies for a maximum number of 6,050 switching cycles within the mission time of the switching device.

The following applies for the probability of failure of the two-channel structure below:

- $MTTF_d$: the following $MTTF_d$ values are estimated: 25 years for K5 and 50 years for T1 [E]. The capacitor C1 is included in the calculation with an $MTTF_d$ of 45,662 years [D]. At a B_{10d} value of 400,000 cycles [S] and a switching frequency of daily energization on 240 working days, the result is an $MTTF_d$ of 16,667 years for K1 and K2. At a B_{10d} value of 400,000 cycles [S] and at 240 working days, 16 working hours and a cycle time of 3 minutes, the result for n_{op} is 76,800 cycles per year and for the $MTTF_d$ 52 years in each case for K3 and Q1. These values produce a symmetrized $MTTF_d$ of the channel of 21 years ("medium").
- DC_{avg}: fault detection by the process in the event of failure in the actuation of the deceleration ramp leads to a DC of 30% for K5. For T1, the DC is 60%, likewise as a result of fault detection by the process. K1 and K2 yield a DC of 99% owing to the integral fault detection in K4, and K3 a DC of 99% owing to fault detection by K5. For C1, the DC is 60% owing to testing of the timing element with the Fl de-energized. For Q1, the DC is thus 99% owing to direct monitoring in K5. The averaging formula for DC_{avg} produces a result of 63% ("low").
- Adequate measures against common cause failure (75 points): separation (15), diversity (20), FMEA (5) and environmental conditions (25 + 10)
- The two-channel combination of the control elements satisfies Category 3 with a medium $MTTF_d$ per channel (21 years) and low DC_{avg} (63%). This results in an average probability of dangerous failure of 1.04×10^{-6} per hour. This corresponds to PL c. The overall probability of failure is determined by addition of the probability of dangerous failure of K4, and is equal to 1.34×10^{-6} per hour. This then likewise corresponds to PL c.



- The wearing elements K3 and Q1 should be replaced at intervals of approximately five years (T_{10d}).

More detailed references

- *Apfeld, R.; Zilligen, H.*: Sichere Antriebssteuerungen mit Frequenzumrichtern. BIA-Report 5/2003. Ed.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin 2003.
  www.dguv.de/bgia, Webcode d6428
- IEC 61800-5-2: Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional (07.07)

Figure 8.20:
Determining of the PL by means of SISTEMA