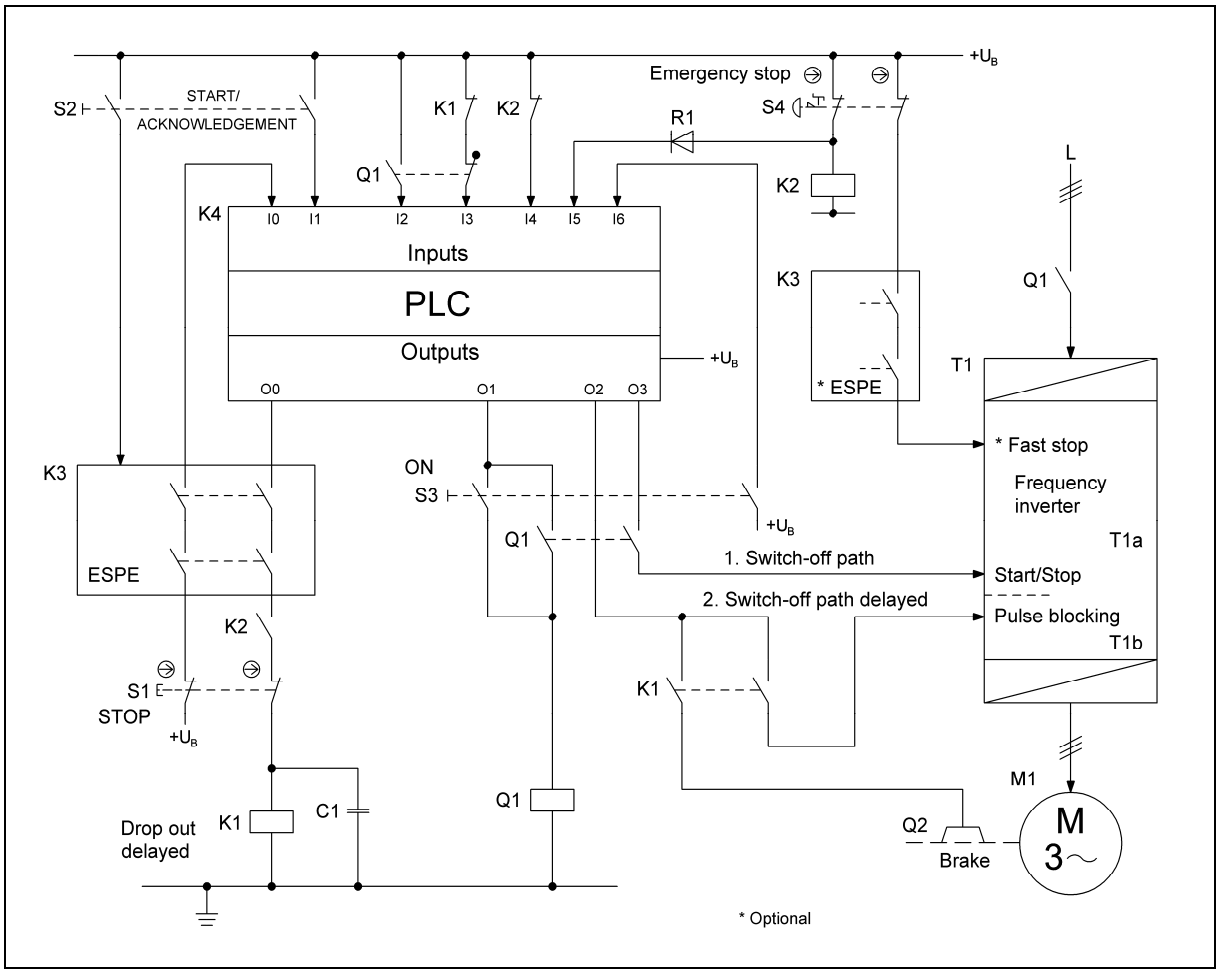
8.2.20 Safe stopping of a PLC-driven drive – Category 3 – PL d (Example 20)

Figure 8.36:
Safe stopping of a PLC-driven frequency inverter drive following a stop or emergency stop command or following tripping of a protective device (in this case, an ESPE)

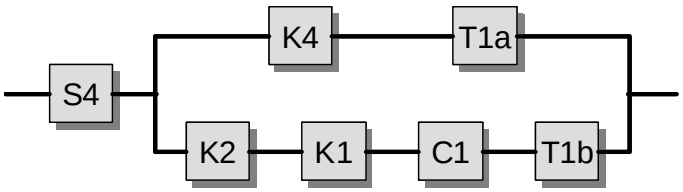


Safety function

- Safety-related stop function, initiated by a protective device: following a stop or emergency stop command or tripping of a protective device, the drive is halted (SS1 – safe stop 1).

Functional description

- The hazardous movement is interrupted redundantly if either the stop button S1 or the protective device K3 (shown in the circuit diagram as electro-sensitive protective equipment (ESPE)) is actuated. The drive is halted in an emergency following actuation of the emergency stop device S4. In all three cases, the first set braking time is implemented via the output O3 of the PLC K4 by deactivation of the “Start/Stop” input (T1a) on the frequency inverter (FI) T1. Redundantly to this arrangement, the second set braking time takes the form of deactivation of

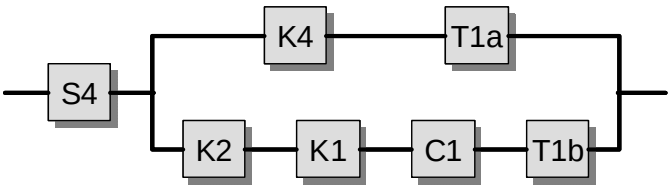


the “pulse blocking” input (T1b) on T1, which is achieved by de-energization of the contactor relay K1 (with the use of the capacitor C1 for drop-out delay), and application of the brake Q2. The first de-energization path is thus implemented directly by the PLC K4; conversely, the second de-energization path employs relay technology and delayed drop-out. The timer settings for O2 in the PLC program and for K1 are selected such that the machine movement is halted even under unfavourable operating conditions.

- Should a “fast stop” input with a particularly rapid speed reduction be available on the FI, the emergency stop device and ESPE may be connected to it if desired, as shown on the circuit diagram. This option is not considered further below.
- In the event of failure of the PLC K4, the frequency inverter inputs T1a/T1b, the contactor relay K1 with drop-out delay or the contactor relay K2, stopping of the drive is assured, since two mutually independent de-energization paths are always present. Failure of the auxiliary contactors K1 or K2 to drop out is detected, at the latest before renewed start-up of the machine movement, by the feedback of the mechanically linked break contacts to the PLC inputs I3 and I4.

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.
- Owing to the use of a frequency inverter with safe pulse blocking, the contactor Q1 is no longer absolutely essential for de-energization of the supply voltage. The frequency inverter must be suitable for ramping up and braking.
- The contactor relays K1 and K2 possess mechanically linked contact elements in accordance with IEC 60947-5-1, Annex L.
- The contacts of the pushbuttons S1 and S4 are mechanically linked in accordance with IEC 60947-5-1, Annex K.
- The standard components K4 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 c (downgraded owing to diversity) and the instructions in Section 6.3.
- If the brake Q2 is provided for functional reasons only, i.e. it is not involved in execution of the safety function, it is disregarded in the calculation of the probability of failure, as in this example. This procedure requires that coasting down of the drive in the event of a failure of T1a (see below), in which case



de-energization is effected by means of pulse blocking alone, is not associated with an unacceptably high residual risk. The involvement of a brake in execution of the safety function in conjunction with the use of an FI is described in the example of a revolving door control (Example 23).

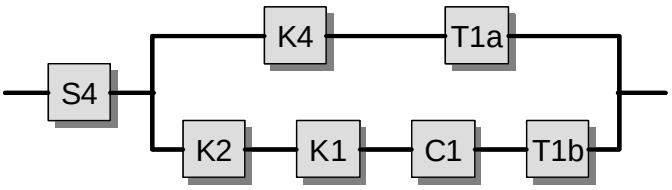
- The ESPE K3, for example in the form of a light curtain, satisfies the requirements for Type 4 to EN 61496-1 and IEC 61496-2, and for PL e.

Calculation of the probability of failure

- The probability of failure of safe stopping triggered by the emergency stop device S4 or by the ESPE, which is also shown on the safety-related block diagram, is calculated. The “fast stop” function of the FI and the facility for de-energization of the power supply to the FI via Q1 are not considered in the calculation of the probability of failure of the safety function.
- The frequency inverter T1 is broken down into the blocks T1a and T1b. The block T1a contains the functions Start and Stop and their implementation in the control system. The block T1b contains the pulse blocking, which is achieved by a low number of components.

Safe stop triggered by the emergency stop device S4:

- A fault exclusion is assumed for the emergency stop device, since the number of actuations stated in Table D.2 is not exceeded.
- $MTTF_d$: the following $MTTF_d$ values are estimated: 50 years for K4, 100 years for T1a and 1,000 years for T1b [E]. At a B_{10d} value of 400,000 cycles [S] and at 240 working days, 8 working hours and a cycle time of 6 minutes, the n_{op} is 19,200 cycles per year and the $MTTF_d$ 208 years for K1. At a B_{10d} value of 400,000 cycles [S] and daily actuation on 240 working days, the $MTTF_d$ for K2 is 16,667 years. The capacitor C1 is included in the calculation with an $MTTF_d$ of 45,662 years [D]. These values produce a symmetrized $MTTF_d$ for each channel of 72 years (“high”).
- DC_{avg}: fault detection by the process results in a *DC* of 30% for K4, a *DC* of 90% for T1a and a *DC* of 60% for T1b. A *DC* of 99% for K1 and a *DC* of 60% for C1 are derived by testing of the timing element with the FI de-energized. The *DC* for K2 is 99% owing to plausibility testing in K4 with the switching status of S4. The averaging formula for DC_{avg} yields 56.9 % (within the tolerance for “low”).
- Adequate measures against common cause failure (85 points): separation (15), diversity (20), overvoltage protection etc. (15) and environmental conditions (25 + 10)



- The combination of the control elements corresponds to Category 3 with a high $MTTF_d$ per channel (72 years) and a low DC_{avg} (56.9%). This results in an average probability of dangerous failure of 1.76×10^{-7} per hour. This corresponds to PL d.

Safe stop triggered by the ESPE K3:

- The ESPE K3 is a standard safety component. Its probability of failure is 3.0×10^{-8} per hour [M], and is added at the end of the calculation.
- The probability of failure of the “PLC/electromechanical” two-channel structure is calculated using the same $MTTF_d$ and DC values as those described above. The component K2 however is not involved in execution of this safety function. The results are: an $MTTF_d$ for one channel of 72 years (“high”) and a DC_{avg} of 56.8% (within the tolerance for “low”). For Category 3, this results in an average probability of dangerous failure of 1.77×10^{-7} per hour. The overall probability of failure is determined by addition, producing a result of 2.07×10^{-7} per hour. This also corresponds to PL d.

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
- EN 61496-1: Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests (05.04)
- IEC 61496-2: Safety of machinery – Electro-sensitive protective equipment – Part 2: Particular requirements for equipment using active opto-electronic protective devices (AOPDs) (04.06)
- IEC 61800-5-2: Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional (07.07)