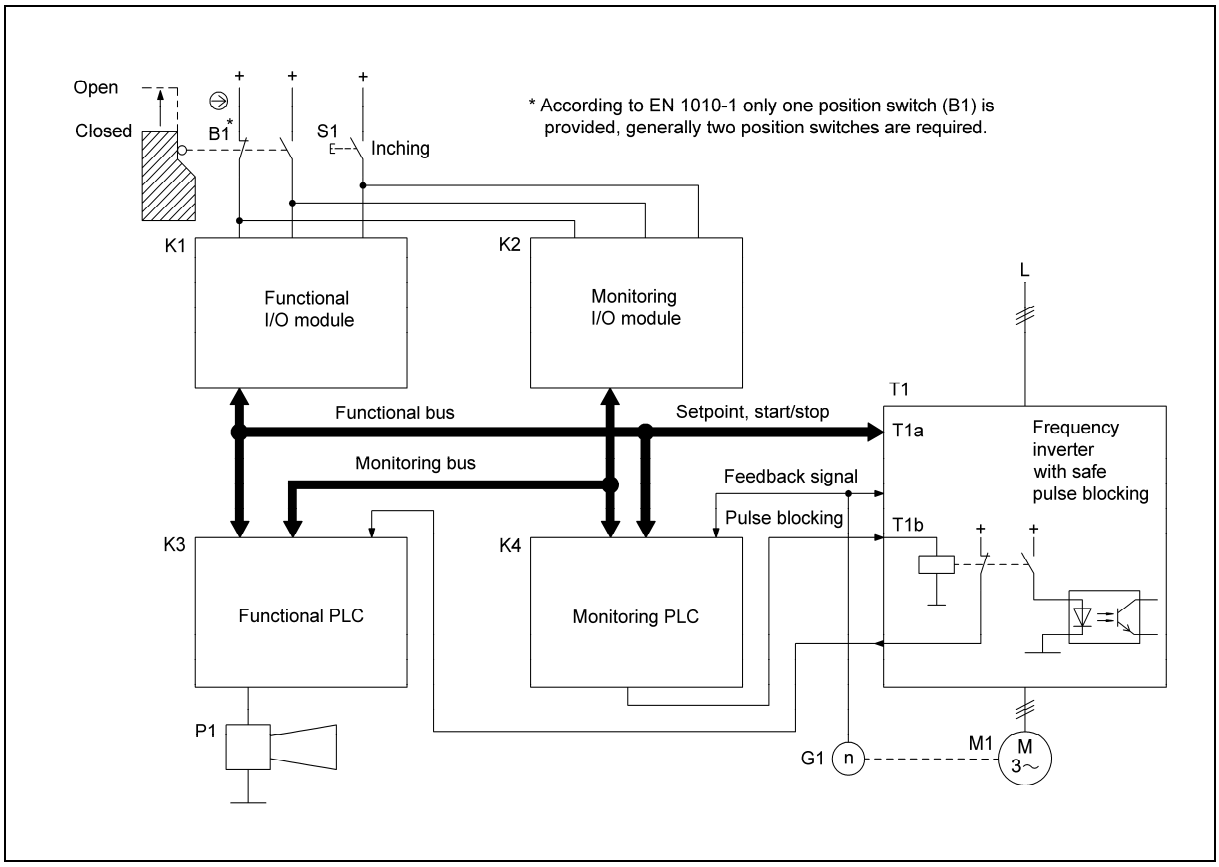
8.2.24 Inching mode with safely limited speed on a printing machine – Category 3 – PL d (Example 24)

Figure 8.42:
Inching mode with safely limited speed on a printing machine with two-channel microprocessor control

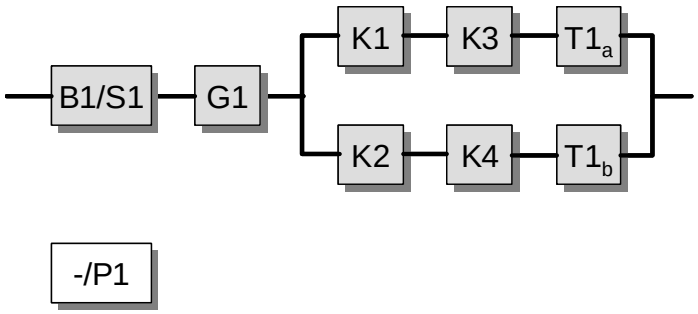


Safety functions

- Safety-related stop function, initiated by a protective device: the drive is to stop when the safety guard is opened (SS1 – safe stop 1).
- Safely limited speed (SLS): when the safety guard is open, machine movements may occur only at limited speed.
- Inching mode: when the safety guard is open, movements are possible only whilst an inching button is pressed.

Functional description

- The remote I/O module K1 registers the states of the position switch with personnel safety function B1 and of the inching button S1, and makes this information available on the functional bus. The information is evaluated by the functional PLC K3 and results in the frequency inverter T1 being actuated (functional actuation T1a) via the functional bus. The I/O module K2 and the monitoring PLC K4, which communicate over a dedicated monitoring bus,

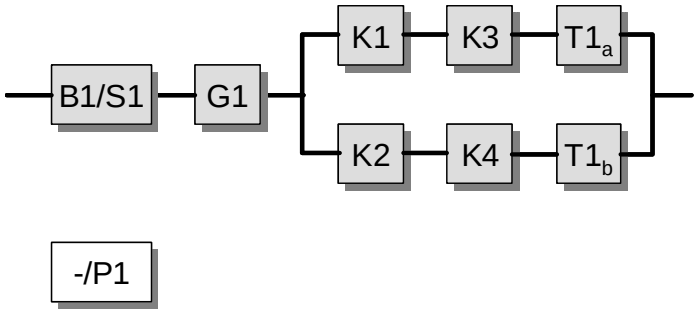


operate redundantly to K1 and K3. K4 can bring about an uncontrolled stopping (coasting down) by addressing the safe pulse blocking of T1 (safety shutdown T1b).

- With B1 open, only inching mode using S1 with safely limited speed is permitted.
- In accordance with EN 1010-1, a single position switch B1 is sufficient. The majority of faults in S1 are detected and controlled by an acoustic start-up warning involving P1 and forced dynamics: when S1 is pressed for the first time, an acoustic warning (P1) is output; only when S1 is released and pressed again does the drive start up again, with delay.
- Faults in K1 and K2 are detected by a status comparison in K4. K4 also monitors K3 by monitoring the input and output information. In addition, the faults in K3 are partly revealed by faults in the process. Self-tests (e.g. program sequence monitoring by an internal watchdog) are performed in K4; in addition, K3 uses K4 for regular addressing of the pulse blocking and monitors feedback from the latter via the mechanically linked break contact of the pulse blocking relay of T1.
- Together with the sin/cos encoder G1, the frequency inverter T1 forms a closed-loop control system in which faults (printing errors, paper tearing) are detected by the production process, which is highly synchronous. For monitoring or the safely limited speed, G1 is also read back into K4 and monitored for plausibility of the sin/cos information ($\sin^2 + \cos^2 = 1$) and for compliance with the setpoint for T1.

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 break contact of B1 satisfies IEC 60947-5-1, Annex K. Measures are implemented for prevention of displacement and reasonably foreseeable misuse (see EN 1088 with Annex A1). A stable arrangement of the protective device is assured for actuation of the position switch.
- Despite the warning at start-up and forced dynamics, S1 may hang during inching operation. An additional requirement is therefore that an emergency stop device be installed within the operator's reach.



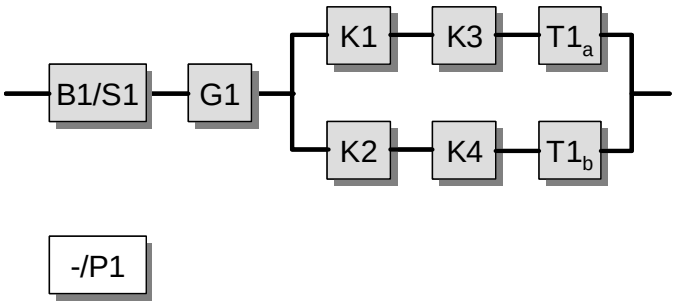
- The conditions for fault exclusion for conductor short-circuits to EN ISO 13849-2, Table D.4 must be observed for the connecting lines to S1. Faults in the connecting lines to B1 are detected by non-equivalence monitoring of the break and make contact in K1 and K2.
- The programmable components K1 to K4 satisfy the normative requirements in accordance with Section 6.3.
- G1 supplies redundant position information (e.g. sin/cos encoder) and is integrated into the closed-loop control circuit (acquisition of the commutation).
- T1 possesses safe pulse blocking (T1b), successful addressing of which is read back by a mechanically linked break contact.
- The standard components G1 and T1 are employed in accordance with the instructions in Section 6.3.10.
- The bus systems (functional bus, monitoring bus) are employed in accordance with the instructions in Section 6.2.17.

Remarks

- Application for example for the safeguarding of entrapment points on rotary printing machines. For non-cyclical operator intervention in the hazardous area, i.e. less frequently than one intervention per hour, EN 1010-1 requires only one position switch for monitoring of the guard position. The fault-tolerance criterion for Category 3 generally requires the use of two position switches (e.g. one break contact, one make contact) for similar machine control systems.
- For inching mode subject to the condition that safely limited speed is already guaranteed, the possibility of avoiding the hazard can be assumed under certain conditions.

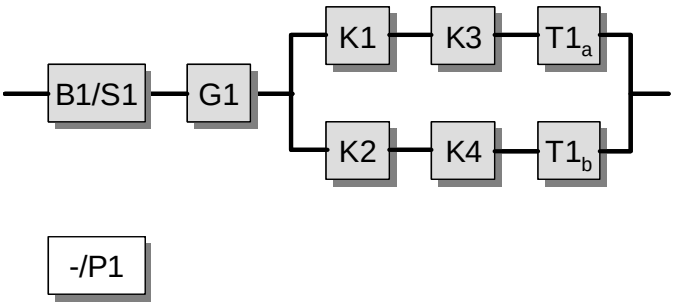
Calculation of the probability of failure

- The sensor level B1, S1 and G1 lies outside the redundant logic and actuator level and is therefore considered separately.
- Fault exclusion for the direct opening electrical contact is possible for B1. A B_{10d} value of 20,000,000 cycles [S] is assumed for the mechanical part of B1. At 10 operations per week, n_{op} is 520 cycles per year and the $MTTF_d$ is 384,615 years. This corresponds mathematically to an average probability of dangerous failure of 2.97×10^{-10} per hour. In order for consideration to be given



to the particular aspects of EN 1010-1, this value is downgraded to the upper marker value of 1.00×10^{-7} per hour for PL d, instead of the $MTTF_d$ for one channel being capped to 100 years as usual.

- S1 has a B_{10d} value of 100,000 cycles [M]. At 10 operations per week, n_{op} is 520 cycles per year and the $MTTF_d$ is 1,923 years. Owing to forced dynamics and the start-up warning, a *DC* of at least 60% is assumed (hanging following repeated inching is not detected, however). By incorporation into a Category 2 structure, S1 thus attains an average probability of dangerous failure of 5.28×10^{-7} per hour.
- Owing to evaluation of the sin/cos signals and its use in the closed-loop control circuit (for commutation), G1 is integrated in accordance with Category 3. At an $MTTF_d$ per channel of 30 years [E] and a *DC* of 90% owing to plausibility testing and fault detection in the process, the average probability of dangerous failure is 2.65×10^{-7} per hour.
- $MTTF_d$: 100 years [E] is allowed for K1 and K2, 50 years [E] for K4, and 30 years [E] for K3. In addition, 30 years [E] is substituted for T1a and 1,000 years [E] for T1b. Overall, this produces a symmetrized $MTTF_d$ value per channel of 24 years (“medium”).
- DC_{avg}: the *DC* of 99% for K1 and K2 is produced by direct comparison of the supplied status information in K4. The *DC* of 99% for K3 is based upon parallel processing of all safety-related information in K4 and upon the direct comparison in K4 with the intermediate results and output signals formed by K3. The self-tests implemented in K4 together with partial monitoring by the reading back of pulse blocking by K3 result in a *DC* of 60% for K4. The *DC* of 99% for T1a is based upon comparison in K4 between the setpoint and actual value of the shaft position. For T1b, assumption of a fault exclusion for the internal optocoupler owing to readback of addressing of pulse blocking results in a *DC* of 60%. Averaging then produces a DC_{avg} of 91% (“medium”).
- Adequate measures against common cause failure (70 points): separation (15), FMEA (5), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of K1 to K4 and T1 corresponds to Category 3 with a medium $MTTF_d$ per channel (24 years) and a medium DC_{avg} (91%). This results in an average probability of dangerous failure of 3.33×10^{-7} per hour. The values for B1 and of G1 must be added to this figure for the safety-related stop function



and the safely limited speed. (1.00 + 2.65 + 3.33) × 10^{-7} per hour = 6.98 × 10^{-7} per hour thus results in a PL of d. The values for S1 and G1 must be added for inching mode: a value of (5.28 + 2.65 + 3.33) × 10^{-7} per hour = 1.13 × 10^{-6} per hour is thus produced. This corresponds to PL c.

More detailed references

- 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)
- Safety in Construction and Design of Printing and Paper Converting Machines. Electrical Equipment and Control Systems. Ed.: Berufsgenossenschaft Druck und Papierverarbeitung, Wiesbaden, 2004.
  www.bgdp.de/pages/service/download/medien/220-2e.pdf
- *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

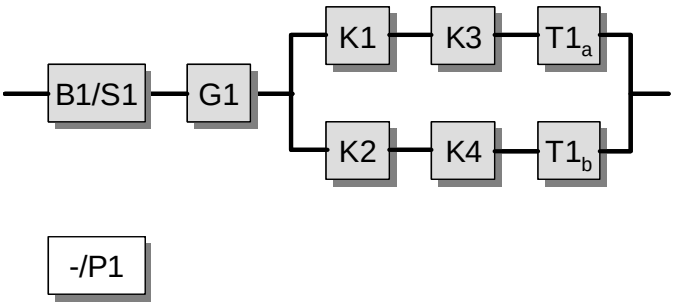


Figure 8.43:
Determining of the PL by means of SISTEMA