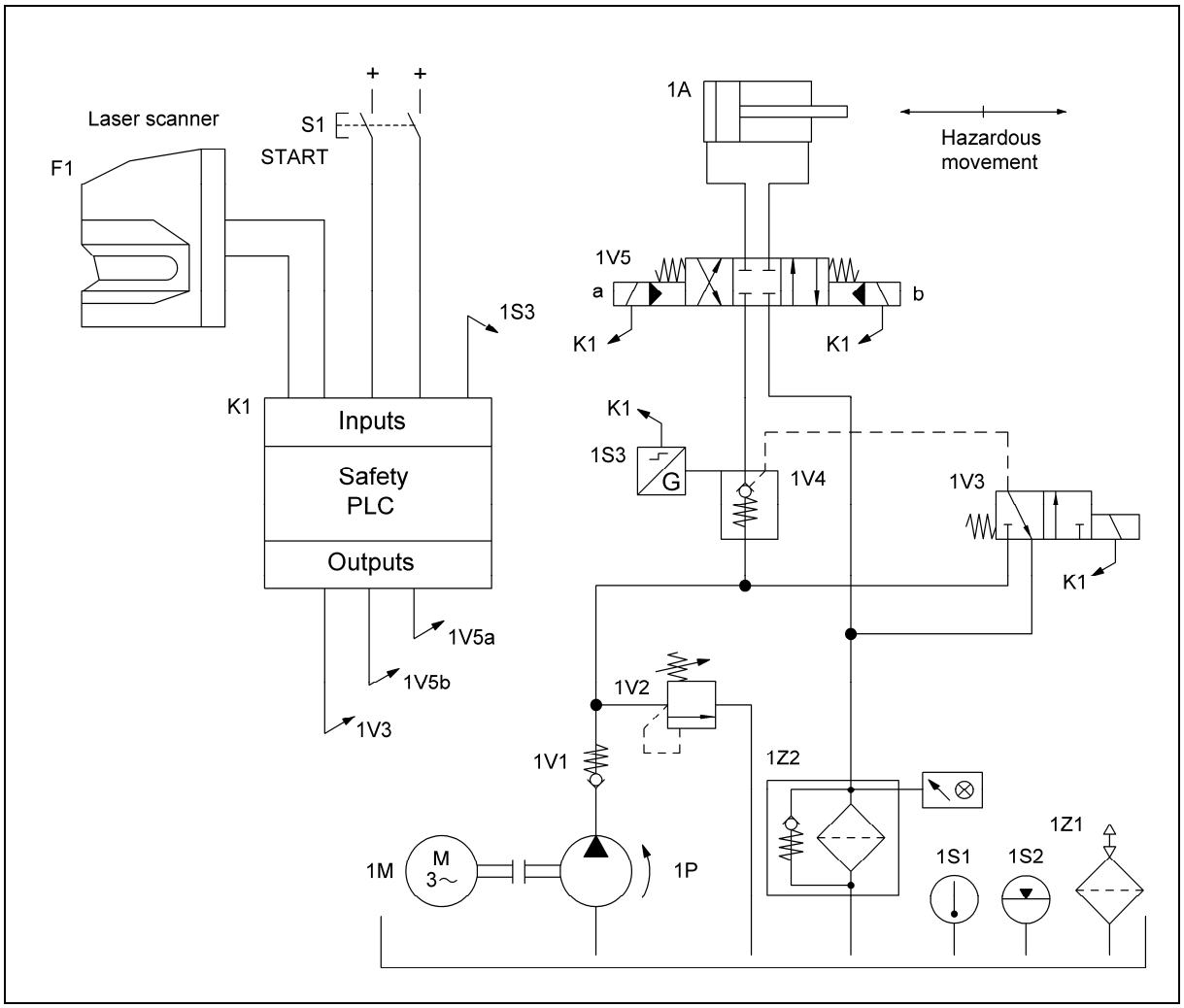
8.2.15 Protective device and hydraulics controlled by PLC – Category 3 – PL d (Example 15)

Figure 8.28:
Detection zone monitoring by laser scanner with
electro-hydraulic deactivation of the hazardous movement

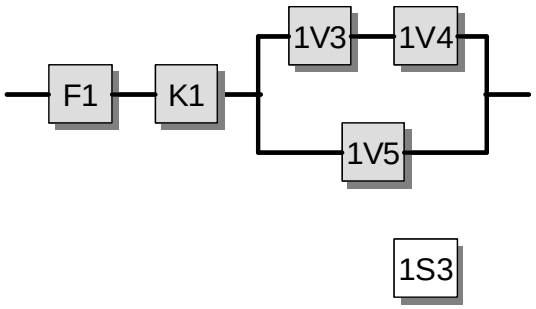


Safety function

- Safety-related stop function, initiated by a protective device: penetration of the laser scanner's detection zone results in stopping of the hazardous movement.

Functional description

- The laser scanner F1 monitors, with its detection zone, the area in which movement of the cylinder 1A may present a danger to the operator. The output signal of the laser scanner is read in on two channels by the safety PLC K1. Following any violation of the detection zone, the next movement must be enabled by actuation of a start button evaluated in K1 (restart interlock). With the aid of the hydraulic control part, K1 controls the movement of 1A.



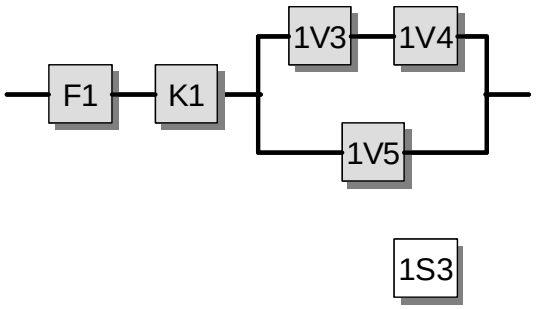
- The hydraulic control part comprises a two-channel arrangement. The first channel comprises directional control valve 1V3, which acts upon the pilot-operated non-return valve 1V4. In the closed position, 1V4 blocks movements by 1A. The second channel consists of the directional control valve 1V5, which in its closed centre position also prevents movement of 1A.
- 1V5 is actuated cyclically; 1V3 and 1V4 close only when the detection zone is violated.
- Direct position monitoring 1S3 is implemented on 1V4 and evaluated in K1 as a measure for fault detection. Faults in 1V5 can be detected via the process owing to the function. An accumulation of undetected faults in the hydraulic control part may lead to loss of the safety function.

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.
- Faults in the conductors to F1 and K1 must not be hazardous in their effects. For this purpose, faults are detected as they arise, and the safe state is initiated. Alternatively, fault exclusion to EN ISO 13849-2, Table D.4 must be possible for conductor short-circuits.
- The laser scanner F1 and safety PLC K1 are tested safety components for use in PL d which satisfy Category 3 and the relevant product standards.
- The directional control valve 1V5 features a closed centre position with sufficient overlap and spring-centering. 1V4 employs electrical position monitoring, since 1V4 is not switched cyclically.
- 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 driven by both processing channels of the PLC. Should this not be the case, the outputs which drive 1V3 and 1V4 are driven by one channel of the PLC, and the output which drives 1V5 by the other.

Calculation of the probability of failure

- Since the laser scanner F1 and the safety PLC K1 are available for purchase as safety components, their probabilities of failure are added at the end of the



calculation (F1: 3.0×10^{-7} per hour [E], K1: 1.5×10^{-7} per hour [E]). For the hydraulic part of the control system, the probability of failure is calculated as shown below.

- $MTTF_d$: values of 150 years [S] are assumed for valves 1V3 to 1V5. Overall, this results in a symmetrized $MTTF_d$ value per channel of 88 years ("high").
- DC_{avg}: a *DC* of 99% for 1V4 is produced by direct monitoring in K1 with the aid of the position monitor 1S3. Owing to the close coupling of 1V3 and 1V4, this results in 1V3 being monitored indirectly at the same time with a *DC* of 99%. The *DC* of 60% for 1V5 is based upon fault detection in the process with cyclical actuation. Averaging thus results in a DC_{avg} of 86% ("low").
- Adequate measures against common cause failure (90 points): separation (15), diversity (20), FMEA (5), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the control elements in the hydraulic part corresponds to Category 3 with a high $MTTF_d$ per channel (88 years) and low DC_{avg} (86%). This results in an average probability of dangerous failure of 6.2×10^{-8} per hour for the hydraulic system.
- Altogether, the average probability of dangerous failure is $(3.0 + 1.5 + 0.62) \times 10^{-7} = 5.12 \times 10^{-7}$ per hour. This corresponds to PL d.

More detailed reference

- *Bömer, T.*: Hinweise zum praktischen Einsatz von Laserscannern. In: BGIA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. Kennzahl 310 243. 36th suppl. XII/99. Ed.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin 1985 – loose-leaf ed.
  www.bgia-handbuchdigital.de/310243

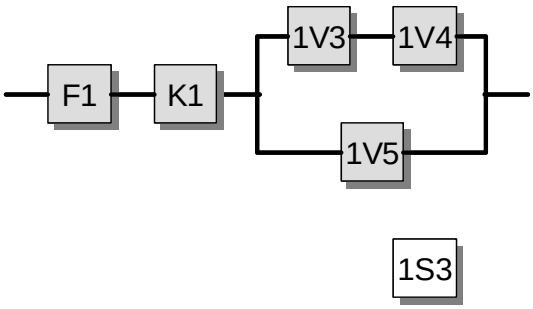


Figure 8.29:
Determining of the PL by means of SISTEMA