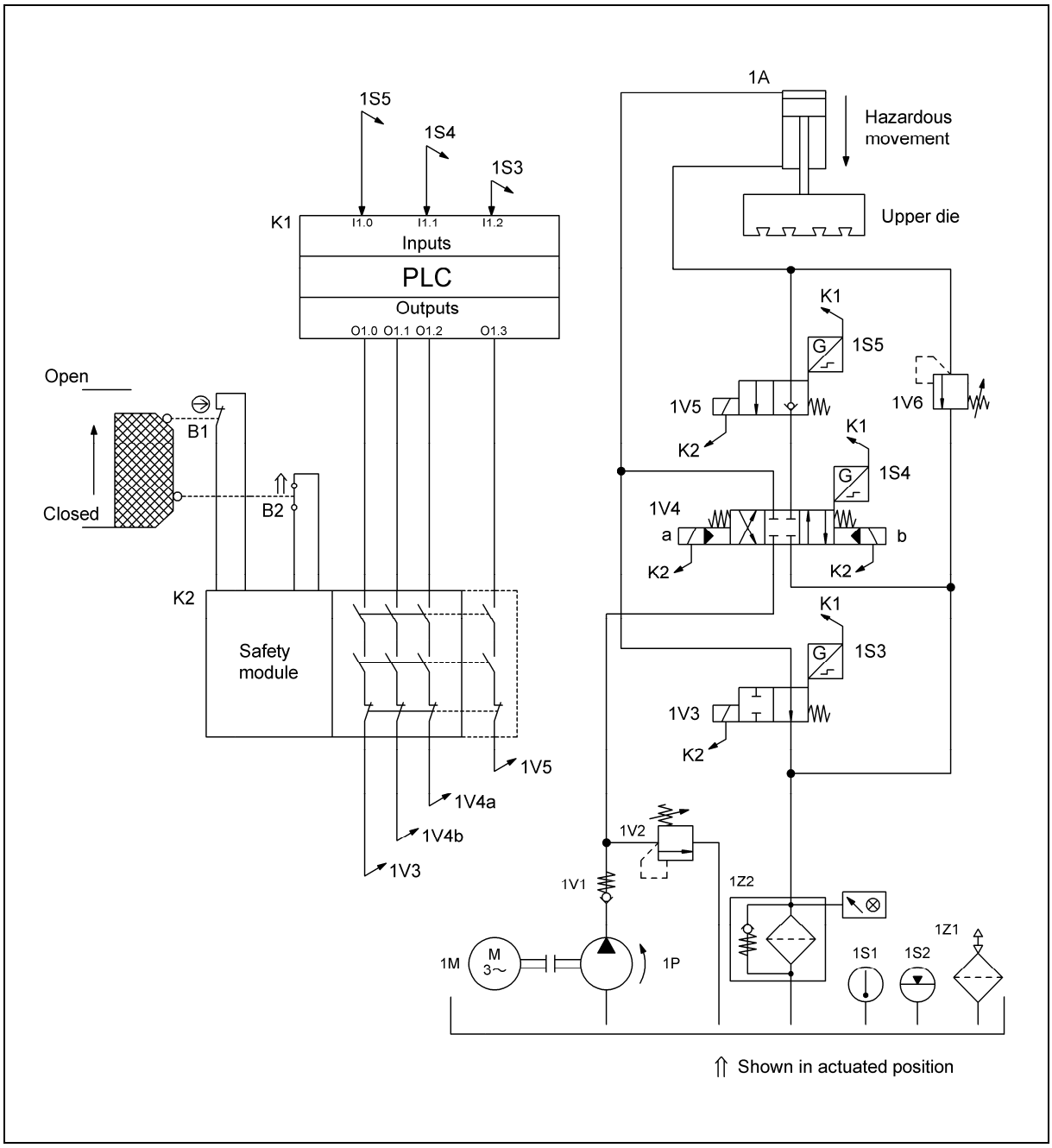
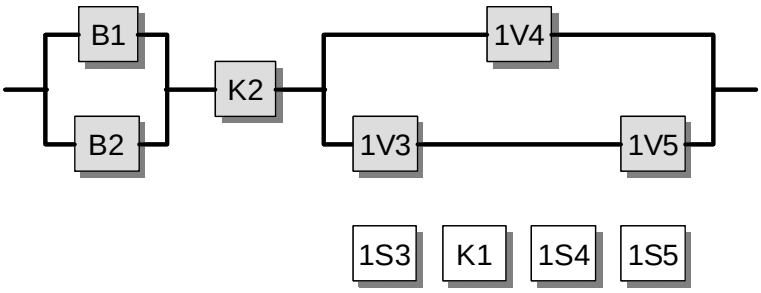
8.2.33 Electrohydraulic press control – Category 4 – PL e (Example 33)

Figure 8.56:
Press control, electrical monitoring of a moveable guard with hydraulic stopping of the hazardous movement



Safety function

- Safety-related stop function, initiated by a protective device: stopping of the hazardous movement

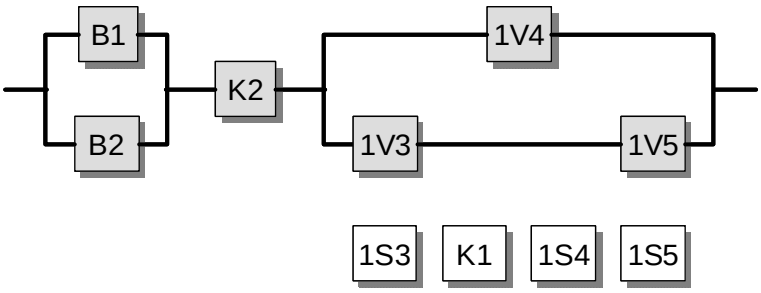


Functional description

- The hazardous area is safeguarded by means of a moveable guard, the position of which is detected by two position switches B1 and B2 in the form of a break contact/make contact combination. The signals are read into a standard safety module K2 which is looped into the enabling path for the electrical pilot control K1 (a conventional PLC) for the hydraulic actuators. Hazardous movements or states are controlled by three directional control valves (1V3, 1V4 and 1V5) on the actuator side.
- In response to a demand upon the safety function, all valves are de-energized by K2, and are placed by their return springs in the closed centre position (1V4) or closed position (1V3 and 1V5). The oil return from the lower piston side of the cylinder to the reservoir is interrupted by 1V4 and 1V5 at the same time. 1V5 is a poppet valve which is designed to shut off the volumetric flow without leakage. Valve 1V4, which also controls the direction of movement of the cylinder, is a piston-type directional control valve which also exhibits a certain degree of leakage in the closed centre position. Although 1V3 is only indirectly involved in the stop function, it can influence the safety function dangerously. Should 1V3 and 1V4 get stuck at the same time, there would be pressure on the upper side of the cylinder while the lower side is shut off by 1V5. Due to the pressure translation in the cylinder the pressure-relief valve 1V6 would open and the upper die descend.
- Failure of one of the valves does not result in loss of the safety function. All valves are actuated cyclically.
- Each valve is equipped with a position monitoring, 1S3, 1S4 and 1S5, for fault detection purposes. Failure of either of the valves is detected in the conventional PLC K1, which prevents initiation of the next hazardous movement following a fault.
- A single fault in one safety component does not result in loss of the safety function. In addition, single faults are detected at or prior to the next demand. An accumulation of undetected faults does not result in loss of the safety function.

Design features

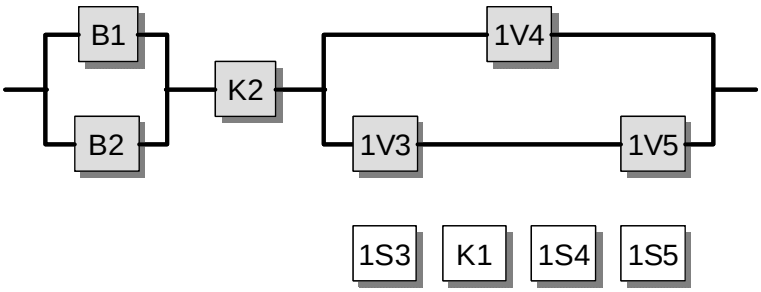
- Basic and well-tried safety principles and the requirements of Category B are observed. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.



- A stable arrangement of the protective device is assured for actuation of the position switch.
- Switch B1 is a position switch with a direct opening contact in accordance with IEC 60947-5-1, Annex K.
- The safety module K2 satisfies all requirements for Category 4 and PL e.
- The supply conductors to the position switches are laid separately or with protection.
- A standard PLC without safety functions is employed for K1.
- The valves 1V3, 1V4 and 1V5 possess a closed centre position and closed position respectively with sufficient overlap, spring-centering/return and position monitoring.
- The safety-oriented switching position is assumed from any position by removal of the control signal.
- The pressure-relief valve 1V6 to protect the cylinder 1A and the components below against “pressure intensifier effect” fulfils the requirements of EN 693:2001, cl. 5.2.4.4.

Calculation of the probability of failure

- K2 is considered as a subsystem with a probability of failure of 2.31×10^{-9} per hour [M]. The remainder of the control system is grouped separately by electromechanical and hydraulic components to form two Category 4 subsystems, the probability of failure of which is calculated below.
- $MTTF_d$: fault exclusion is possible for the electrical contact of the position switch B1 with direct opening action. For the electrical make contact of the position switch B2, the B_{10d} is 1,000,000 switching operations [M]. A B_{10d} value of 1,000,000 cycles [M] is stated for the mechanical part of B1 and B2. At 365 working days, 16 working hours per day and a cycle time of 10 minutes, n_{op} is 35,040 cycles per year for these components, and the $MTTF_d$ is 285 years for B1 and 142 years for B2. An $MTTF_d$ of 150 years [S] is assumed for each of the valves 1V3, 1V4 and 1V5. This results in $MTTF_d$ values per channel of 100 or 88 years (“high”) for the two subsystems.
- DC_{avg}: the DC of 99% for B1 and B2 is based upon the plausibility monitoring of the two switching states in K2. The DC of 99% for the valves is based upon direct monitoring of the switching states by the PLC K1. This results in a DC_{avg} of 99% (“high”) for the two subsystems.



- Measures against common cause failures (75 points) for the two subsystems: separation (15), well-tried components (5), FMEA (5), protection against over-voltage etc. (15) and environmental conditions (25 + 10)
- The electromechanical and the hydraulic parts of the control system correspond to Category 4 with a high $MTTF_d$ per channel (100 or 88 years) and a high DC_{avg} (99%). This results in an average probability of dangerous failure of 2.47 x 10^{-8} per hour and 2.84 x 10^{-8} per hour for each subsystem. Addition inclusive of K2 produces an average probability of dangerous failure for the complete safety function of 5.54 × 10^{-8} per hour. This corresponds to PL e.

Figure 8.57:
Determining of the PL by means of SISTEMA