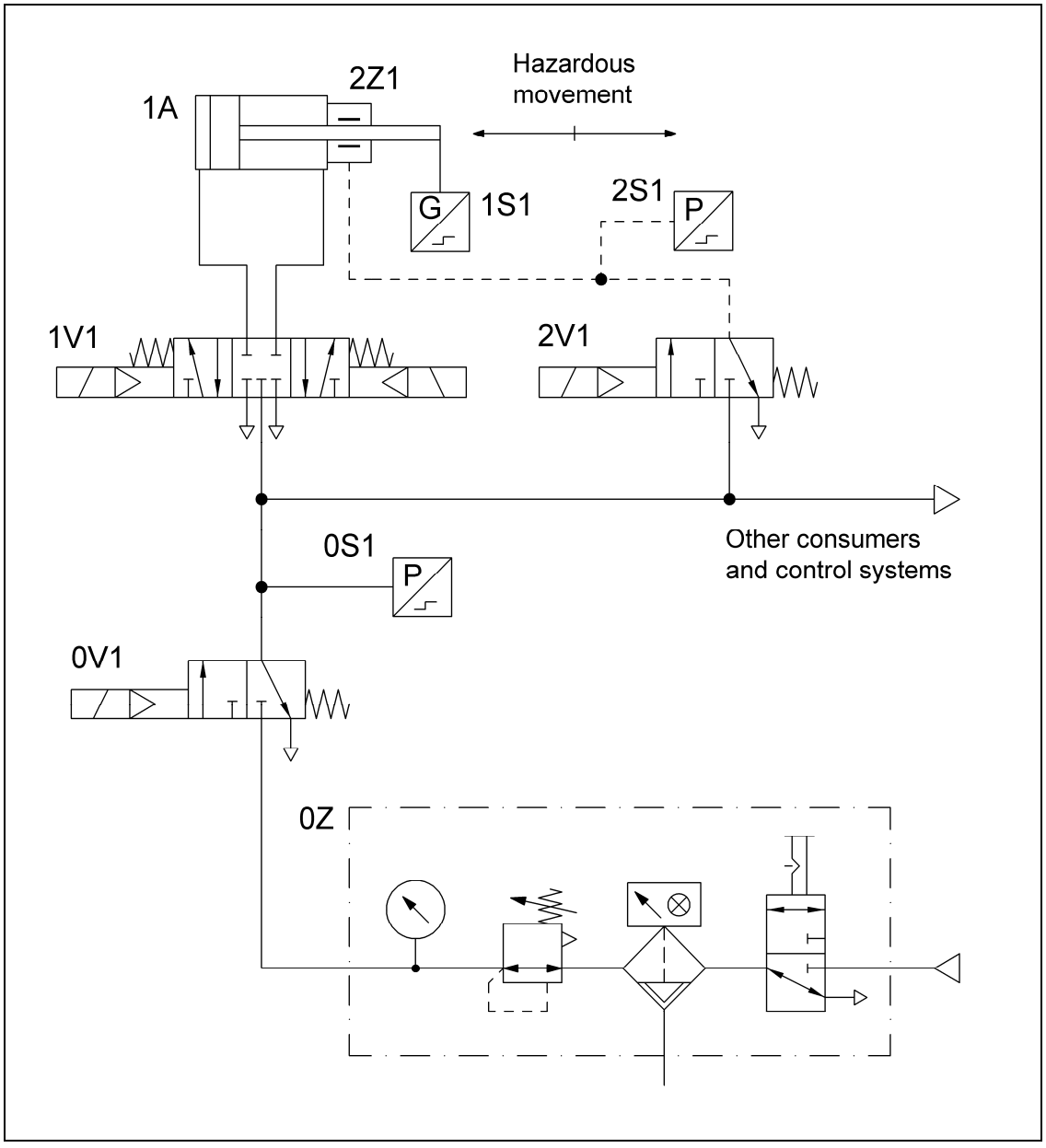
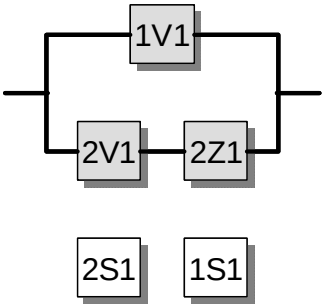
8.2.14 Pneumatic valve control (subsystem) – Category 3 – PL d (Example 14)

Figure 8.26:
Tested pneumatic valves for redundant control of hazardous movements



Safety functions

- Safety-related stop function: stopping of the hazardous movement and prevention of unexpected start-up from the rest position
- Only the pneumatic part of the control is shown here, in the form of a subsystem. Further safety-related control components (e.g. protective devices and electrical logic elements) must be added in the form of subsystems for completion of the safety function.

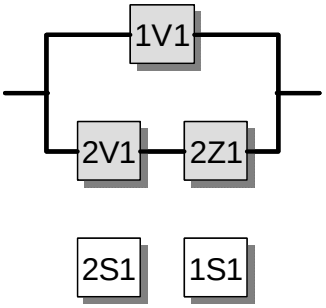


Functional description

- Hazardous movements are controlled/halted redundantly by a directional control valve 1V1 and a brake 2Z1 on the piston rod. The brake 2Z1 is actuated by a control valve 2V1.
- Failure of one of these valves or of the brake alone does not result in loss of the safety function.
- The directional control valve and the brake are actuated cyclically in the process.
- The functioning of the control valve 2V1 is monitored by means of a pressure switch 2S1. Certain faults on the unmonitored valve 1V1 and on the unmonitored brake 2Z1 are detected in the work process. In addition, the overrun (distance/time characteristic) during the braking process (dynamic) and/or at start-up of the machine (static) is monitored with the aid of a displacement sensor system 1S1 on the piston rod. An accumulation of undetected faults may lead to loss of the safety function.
- Testing of the safety function is implemented at suitable intervals, for example at least every eight working hours.
- The test function must not be impaired by failure of the brake. Failure of the test function must not lead to failure of the brake.
- Should trapped compressed air pose a further hazard, additional measures are required.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met.
- The directional control valve 1V1 features a closed centre position with sufficient overlap and spring-centering.
- The safety-oriented switching position is assumed from any position by removal of the control signal.
- The upstream electrical logic for example is employed for signal processing for the pressure monitor 2S1 and the displacement sensor system 1S1.



Calculation of the probability of failure

- $MTTF_d$: B_{10d} values of 40,000,000 cycles [E] are assumed for the directional control valves 1V1 and 2V1. At 240 working days, 16 working hours and a cycle time of 10 seconds, n_{op} is 1,382,400 cycles per year. The $MTTF_d$ for 1V1 and 2V1 is thus 289 years. A B_{10d} value of 5,000,000 switching operations [M] is substituted for the mechanical brake on the piston rod 2Z1. This results in an $MTTF_d$ of 36 years for the mechanical brake. Overall, the resulting symmetrized $MTTF_d$ value per channel is 71 years (“high”).
- DC_{avg}: pressure monitoring of the control signal for the brake results in a *DC* of 99% for the valve 2V1. The *DC* for the valve 1V1 is 60% owing to fault detection through the process. A *DC* of 75% for 2Z1 is produced by start-up testing of the mechanical brake. Averaging thus results in a DC_{avg} of 75% (“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 pneumatic control elements corresponds to Category 3 with a high $MTTF_d$ per channel (71 years) and low DC_{avg} (75%). This results in an average probability of dangerous failure of 1.21×10^{-7} per hour. This corresponds to PL d. Following the addition of further safety-related control components in the form of subsystems for completion of the safety function, the PL may under certain circumstances be lower.
- The wearing brake 2Z1 should be replaced at intervals of approximately three years (T_{10d}).

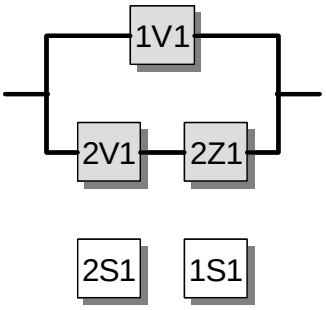


Figure 8.27:
Determining of the PL by means of SISTEMA