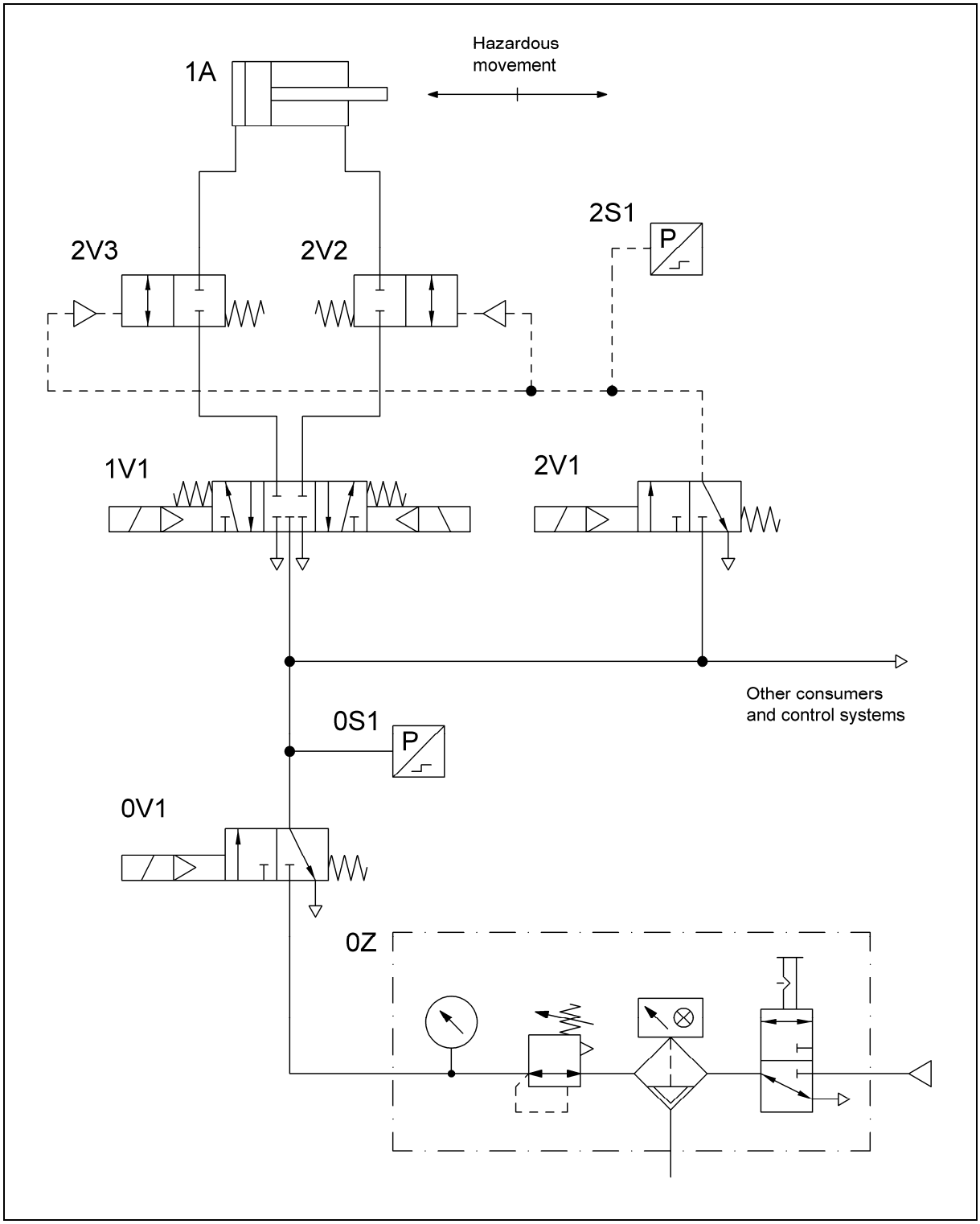
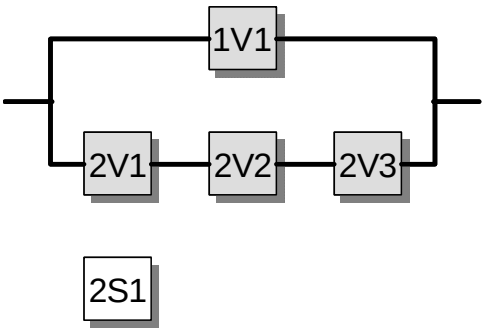
8.2.25 Pneumatic valve control (subsystem) – Category 3 – PL e (for PL d safety functions) (Example 25)

Figure 8.44:
Tested pneumatic valves for redundant control of hazardous movements





Safety functions

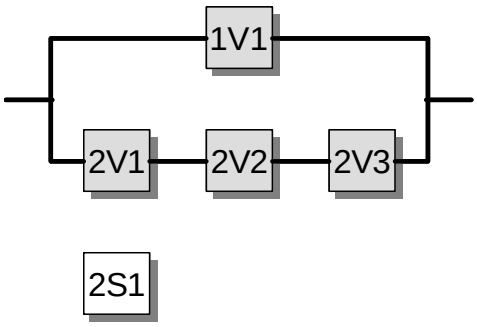
- Safety-related stop function: stopping of the hazardous movement and prevention of unexpected start-up from the rest position
- Only the pneumatic part of the control is shown here, in the form of a subsystem. Further safety-related control components (e.g. protective devices and electrical logic elements)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

Functional description

- Hazardous movements are controlled redundantly by directional control valves. Movements can be halted either by the directional control valve 1V1 or by the directional control valves 2V2 and 2V3. The latter are driven by the control valve 2V1.
- Failure of one of these valves alone does not result in loss of the safety function.
- All directional control valves 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 valves are recognized in the work process. The valves 2V2 and 2V3 should be equipped with position monitors, or – since this is not yet state of the art – their operation should be checked regularly. An accumulation of undetected faults may lead to loss of the safety function.
- 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 stop valves 2V2 and 2V3 are ideally screwed into the cylinder and driven by the valve 2V1 acting as a pilot valve.



- The safety-oriented switching position is assumed from any position by removal of the control signal.
- A single-channel PLC for example is employed for processing of signals from the pressure monitor 2S1.

Calculation of the probability of failure

- $MTTF_d$: B_{10d} values of 40,000,000 cycles [E] are assumed for the valves 1V1 and 2V1. B_{10d} values of 60,000,000 cycles [E] are assumed for the valves 2V2 and 2V3. At 240 working days, 16 working hours and a cycle time of 10 seconds, n_{op} is 1,382,400 cycles per year. The $MTTF_d$ of 1V1 and 2V1 is thus 289 years, and that of 2V2 and 2V3 434 years. Capping of the two channels to 100 years results in a symmetrized $MTTF_d$ value per channel of 100 years (“high”).
- DC_{avg}: pressure monitoring of the control signal for the stop valves results in a *DC* of 99% for 2V1. Fault detection via the process results in a *DC* of 60% for 1V1, and regular checking of operation in a *DC* of 60% for 2V2/2V3. Averaging thus results in a DC_{avg} of 71% (“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 $MTTF_d$ (100 years) and low DC_{avg} (71%). This results in an average probability of dangerous failure of 7.86×10^{-8} per hour. This corresponds to PL e. The addition of further safety-related control parts as subsystems for completion of the safety function generally results in a lower PL.