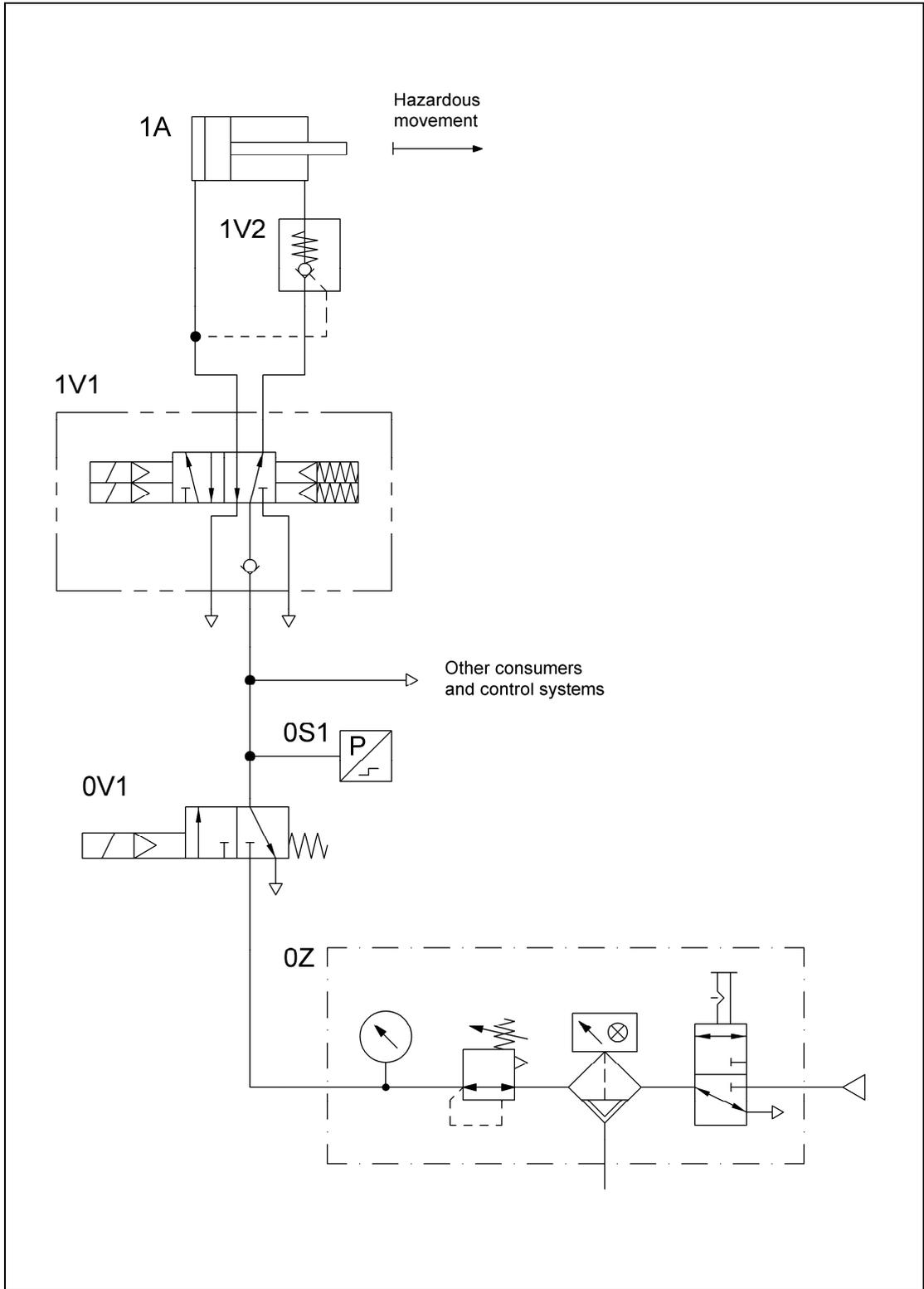
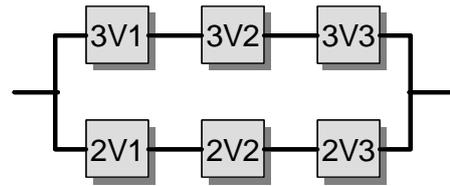




**8.2.31 Pneumatic valve control (subsystem) – Category 4 – PL e (Example 31)**

Figure 8.53:  
Tested pneumatic valves for redundant control of hazardous movements





### Safety functions

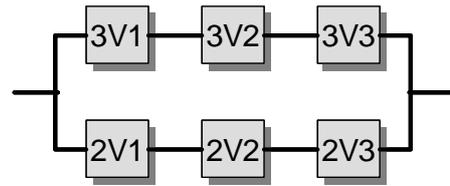
- Safety-related function: reversing of the hazardous movement and prevention of unexpected start-up from the rest position
- Only the pneumatic part of the control is shown here, in the form of a sub-system. Further safety-related control components (e.g. protective devices and electrical logic elements)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

### Functional description

- Hazardous movements are controlled by a valve combination 1V1 with self-monitoring, in conjunction with a pilot-operated non-return-valve 1V2 (relevant in the event of failure of the pneumatics and under external forces).
- A component failure within the valve combination does not result in loss of the safety function.
- The two pilot valves contained in the valve combination 1V1 are actuated separately. Should at least one of the control signals be removed, the movement is reversed.
- A single failure within the valve combination results in disablement in the safe state and is therefore detected in the working process; initiation of the next hazardous movement is prevented.
- The valve combination 1V1 can also be formed by several valves suitably linked and with suitable querying of the switching positions.
- 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.
- 1V1 is a self-monitoring valve combination with mechanically separate integrated pilot valves and pneumatic/mechanical fault detection with integrated non-return-valve in the P line.
- The safety-oriented switch position is attained by removal of the control signals.
- The pilot-operated non-return-valve 1V2 should ideally be screwed into the cylinder.
- Fault detection within the valve combination satisfies the corresponding requirements for the fault case.



### Calculation of the probability of failure

The valve combination 1V1 comprises two valve channels each with three interconnected valves. The valves are denoted on the block diagram as 2V1, 2V2 and 2V3 and 3V1, 3V2 and 3V3.

- $MTTF_d$ : a  $B_{10d}$  value of 20,000,000 cycles [S] is assumed for each valve in the valve combination 1V1. At 240 working days, 16 working hours and a cycle time of 10 seconds,  $n_{op}$  is 1,382,400 cycles per year and the  $MTTF_d$  is 144 years. This results in an  $MTTF_d$  value per channel of 48 years (“high”).
- $DC_{avg}$ : a  $DC$  of 99% for 1V1 is produced by mechanical linking of the two valve channels with simultaneous internal cross-checking of the control pressure. The  $DC_{avg}$  is thus also 99% (“high”).
- Adequate measures against common cause failure (65 points): separation (15), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the pneumatic control elements corresponds to Category 4 with a high  $MTTF_d$  (48 years) and a high  $DC_{avg}$  (99%). This results in an average probability of dangerous failure of  $5.60 \times 10^{-8}$  per hour. This corresponds to PL e. 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.
- Estimation erring on the safe side as described above results in a  $T_{10d}$  value of 14 years for the specified replacement of the valve combination 1V1, which is subject to wear.