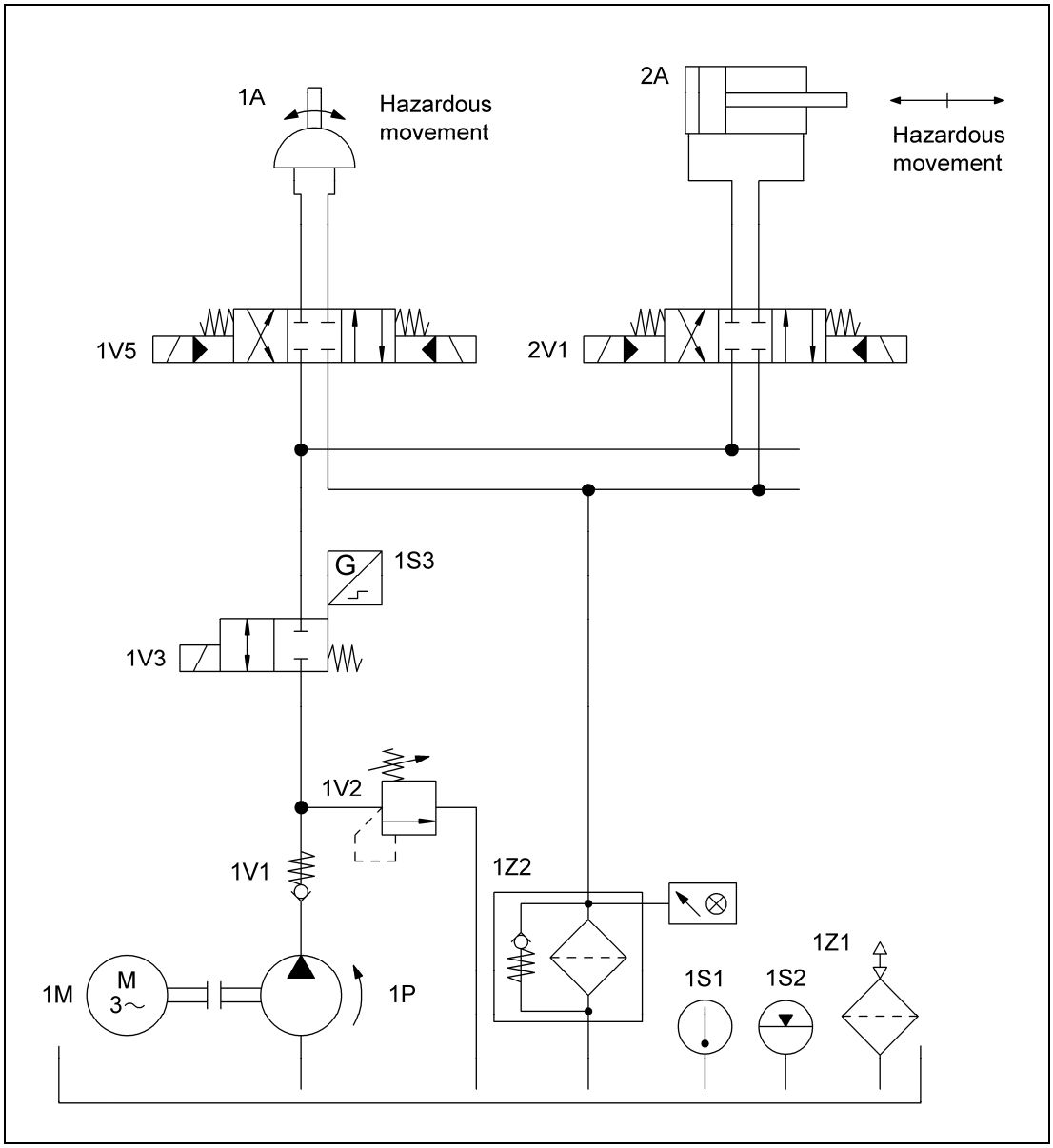
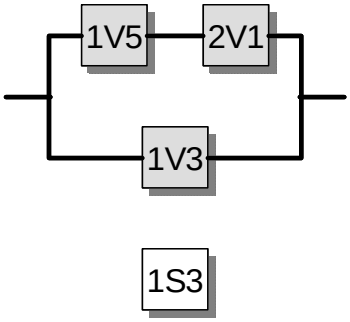
## 8.2.27 Hydraulic valve control (subsystem) – Category 3 – PL e (for PL d safety functions) (Example 27)

Figure 8.47:
Tested hydraulic 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 hydraulic 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**

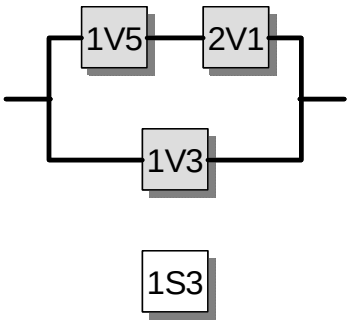
- Hazardous movements are executed in the same hazardous area by two actuators, 1A and 2A. The two movements can be stopped either by the two directional control valves 1V5 and 2V1, or at a higher level by directional control valve 1V3.
- Failure of one of these valves alone does not result in loss of the safety function.
- 1V5 and 2V1 are actuated cyclically in the process. 1V3 closes only in response to a demand upon the safety function, but at least once per shift.
- A technical measure for fault detection is implemented only on 1V3 (position monitoring by 1S3). Certain faults on the unmonitored valves are recognized in the work process. An accumulation of undetected faults 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.
- The directional control valves 1V5 and 2V1 possess a closed centre position with sufficient overlap and spring-centering. 1V3 features electrical position monitoring, since 1V3 is not switched cyclically.
- The safety-oriented switch position is attained in each case by removal of the control signal (electrical or hydraulic).
- A single-channel PLC may be used for signal processing of the electrical position monitoring.

**Calculation of the probability of failure**

- $MTTF_d$: an $MTTF_d$ of 150 years [S] is assumed for the directional control valves 1V3, 1V5 and 2V1. Capping of the second channel (1V3) to 100 years produces a symmetrized $MTTF_d$ value of 88 years (“high”).
- $DC_{avg}$: a *DC* of 99% for 1V3 is based upon the direct monitoring of the switching state by 1S3. The *DC* of 60% for the directional control valves 1V5 and 2V1 is based upon indirect monitoring by the process. Averaging thus produces a $DC_{avg}$ of 73% (“low”).




- Adequate measures against common cause failure (65 points): separation (15), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the hydraulic control elements corresponds to Category 3 with a high $MTTF_d$ (88 years) and low $DC_{avg}$ (73%). This results in an average probability of dangerous failure of $9.35 \times 10^{-8}$ per hour. This corresponds to PL e. The addition of further safety-related control parts in the form of subsystems for completion of the safety function generally results in a lower PL.

Figure 8.48:
Determining of the PL by means of SISTEMA