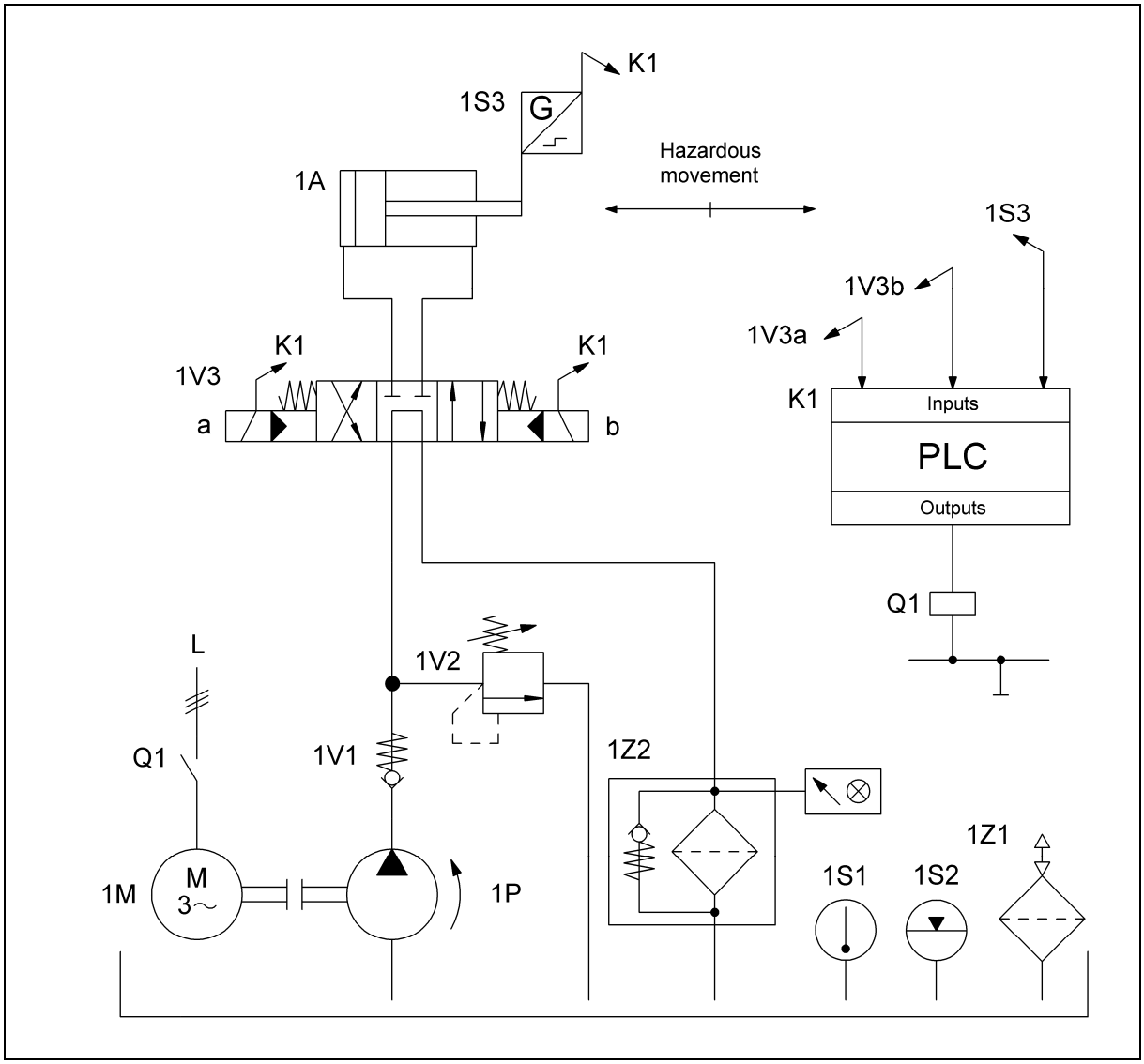
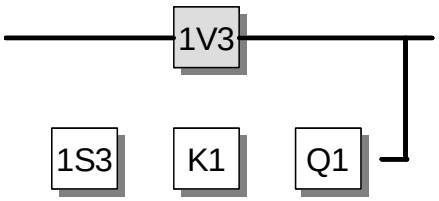
8.2.12 Tested hydraulic valve (subsystem) – Category 2 – PL d (for PL c safety functions) (Example 12)

Figure 8.23:
Hydraulic valve with electronic testing for the control of hazardous movements



Safety functions

- Safety-related stop function: stopping of a 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.

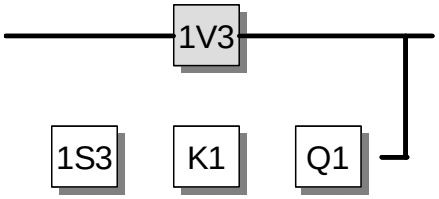


Functional description

- Hazardous movements are controlled by a directional control valve 1V3.
- Failure of the directional control valve 1V3 between function tests may result in loss of the safety function. The probability of failure is dependent upon the reliability of the directional control valve.
- Testing of the safety function is implemented via the PLC K1 by means of a displacement sensor system 1S3. Testing takes place at suitable intervals and in response to a demand upon the safety function. Detection of a failure of 1V3 leads to the hydraulic pump 1M/1P being switched off by the contactor Q1.
- Hazardous movement interruption by the hydraulic pump generally results in a longer overrun. The distance from the hazardous area must be selected in consideration of the longer overrun.
- The test function must not be impaired by failure of the directional control valve. Failure of the test function must not lead to failure of the directional control valve.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met.
- 1V3 is a directional control valve with closed centre position, sufficient overlap and spring centering.
- The safety-oriented switching position is attained by removal of the control signal.
- Testing may for example take the form of checking of the time/distance characteristic (displacement sensor system 1S3) of the hazardous movements in conjunction with the switching position of the directional control valve, with evaluation in a PLC (K1).
- In order to prevent systematic failure, the higher-level de-energization function (acting upon the hydraulic pump in this instance) is checked at suitable intervals, e.g. daily.
- It is implemented for use in applications with infrequent operator intervention in the hazardous area. This enables the requirement of the designated architecture for Category 2 to be satisfied, i.e. “testing much more frequent than the demand upon the safety function” (cf. Annex G).
- The standard component K1 is employed in accordance with the instructions in Section 6.3.10.



- The software (SRASW) is programmed in accordance with the requirements for PL b (downgraded owing to diversity) and the instructions in Section 6.3.

Calculation of the probability of failure

- $MTTF_d$ of the functional channel: an $MTTF_d$ of 150 years is assumed for the directional control valve 1V3 [S]. This is also the $MTTF_d$ value for the functional channel, which is first capped to 100 years.
- $MTTF_d$ of the test channel: an $MTTF_d$ value of 150 years [E] is assumed for the displacement sensor system 1S3. An $MTTF_d$ value of 50 years [E] is assumed for the PLC K1. A B_{10d} value of 2,000,000 cycles [S] applies for the contactor Q1. At actuation once daily on 240 days, the $MTTF_d$ value for Q1 is 83,333 years. The $MTTF_d$ of the test channel is thus 37.5 years. The $MTTF_d$ of the functional channel must therefore be reduced to 75.0 years in accordance with the underlying analysis model.
- DC_{avg}: the DC of 60% for 1V3 is based upon the comparison of the distance/time characteristic of the hazardous movement in conjunction with the switching status of the directional control valve. This is also the DC_{avg} (“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 control elements corresponds to Category 2 with a high $MTTF_d$ (75.0 years) and low DC_{avg} (60%). This results in an average probability of dangerous failure of 7.31×10^{-7} per hour. This corresponds to PL d. Following the addition of further safety-related control parts (subsystems) for completion of the safety function, PL c is generally attained for the complete safety function.

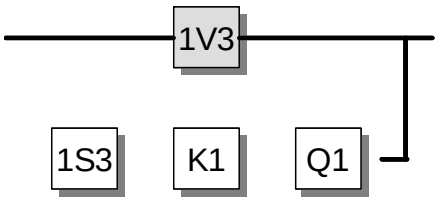


Figure 8.24:
Determining of the PL by means of SISTEMA