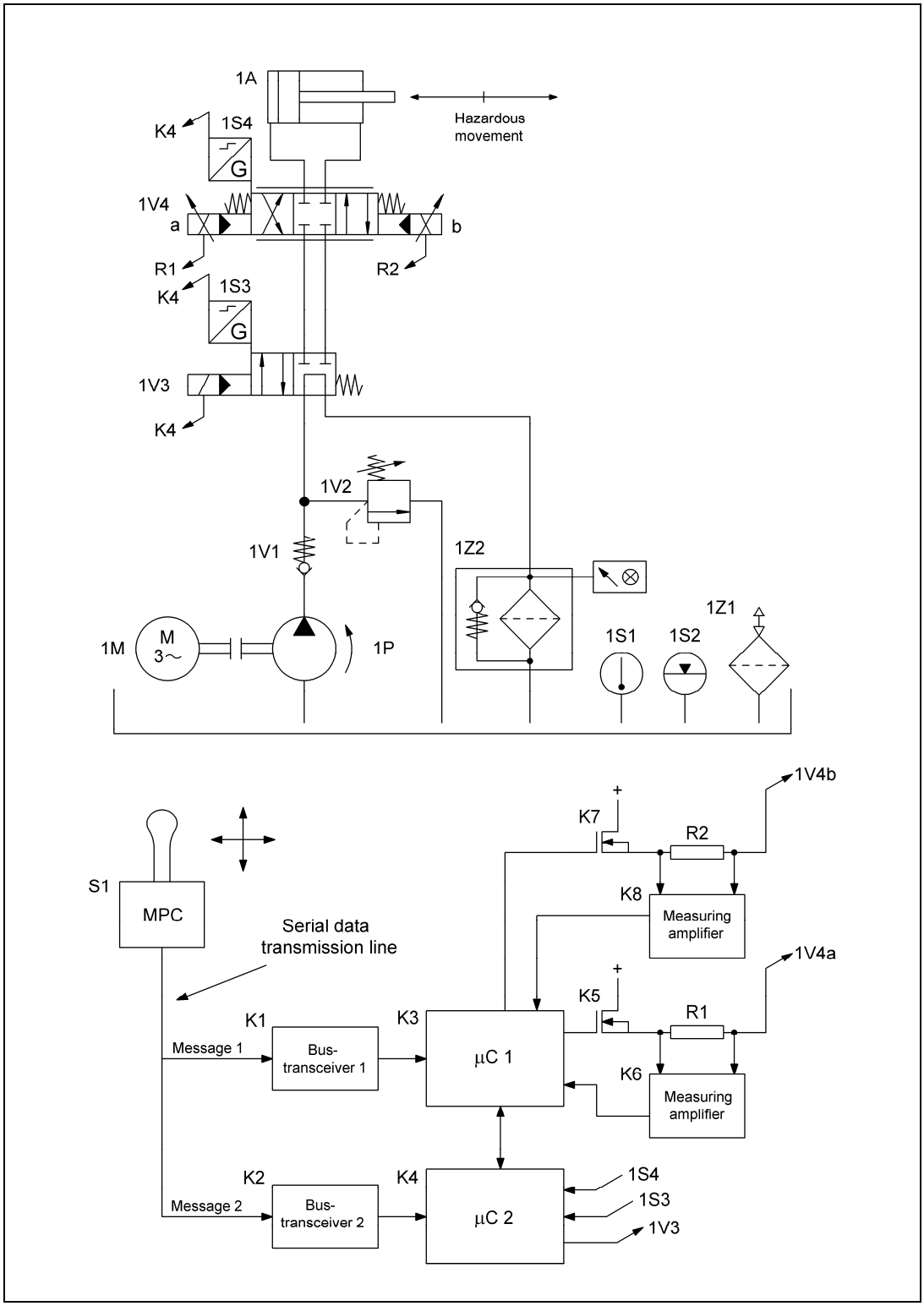
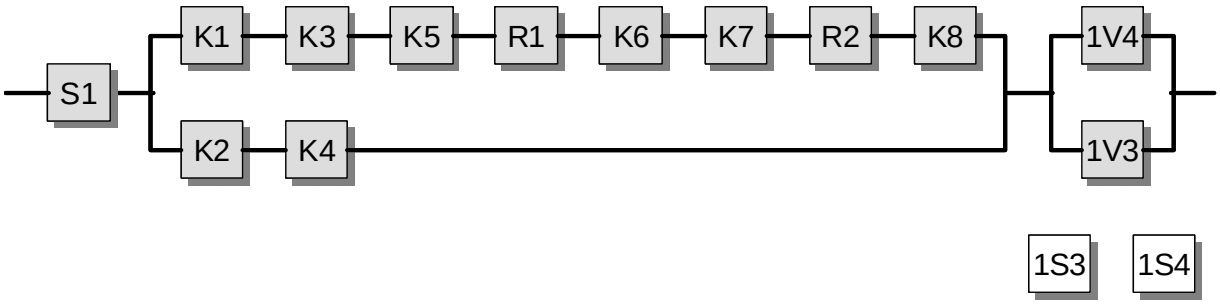
## 8.2.16 Earth-moving machine control system with bus system – Category 3 – PL d (Example 16)

Figure 8.30:
Control of hazardous movements of an earth-moving machine






**Safety function**

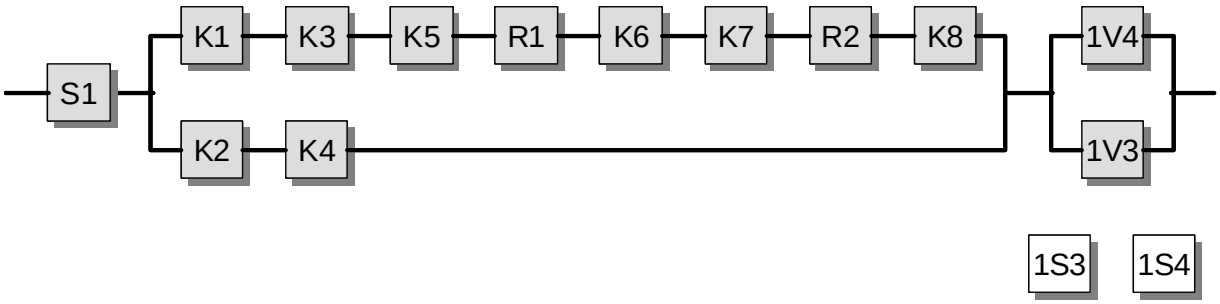
- Prevention of unexpected start-up: avoidance of unexpected movements of tools on earth-moving machines

**Functional description**

- The multi-purpose control (MPC) S1 converts the operator's manual movement of it into electronic messages. It sends these messages cyclically over a serial data communications line (bus system) to the logic control, which generates control signals for the hydraulics which then execute the working movements of the earth-moving machine desired by the user.
- The message 1 sent by the MPC S1 reaches the microcontroller K3 via the bus transceiver K1. From message 1 and in accordance with the algorithms stored in the software, K3 generates the analogue signals required for actuation of the proportional valve 1V4. The resistances R1/R2 and the measuring amplifiers K6/K8 have the function of controlling the output currents for the proportional valve. The microcontroller K4 receives a redundant message 2 from S1 over the bus transceiver K2. K4 checks the correct displacement of the proportional valve 1V4, as signalled by the position measuring system 1S4 integrated into 1V4, for plausibility against the desired position determined from message 2. Should faults be detected, K4 switches off the hydraulic pressure at a higher level by means of a directional control valve 1V3, and places the system in the safe state.

**Design features**

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- The MPC is a safety component suitable for use in PL d and satisfies the requirements for Category 3.
- The proportional valve 1V4 and the directional control valve 1V3 have a closed position/closed centre position, spring return/spring-centering, and sufficient overlap.
- The software (SRESW) for K3 and K4 is programmed in accordance with the requirements for PL d and the instructions in Section 6.3.



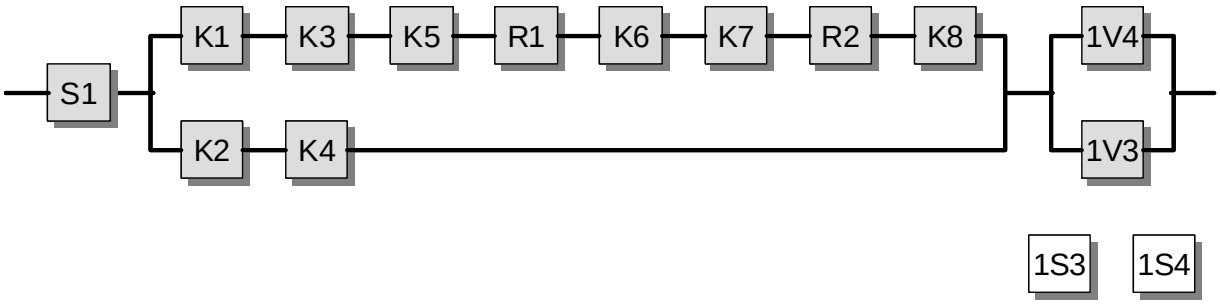

- Data transfer from the MPC to the logic control is safe in accordance with GS-ET-26 and IEC 61784-3. The data communications protocol employed contains redundant messages and measures for detection of the following transmission errors: repetition, loss, insertion, incorrect sequence, corruption and delay (see also Section 6.2.17). The residual error rate $\Lambda$ is lower than $1 \times 10^{-8}$ per hour and thus contributes, as specified in the principles for assessment, less than 1% towards the maximum permissible probability of failure of the safety function. This low percentage can be disregarded within the calculation of the overall probability of failure.

**Remarks**

- An emergency motion function of the earth-moving machine, which is not shown here, may be required; if so, it must be implemented at a higher level.

**Calculation of the probability of failure**

- The multi-purpose control S1 is a standard safety component. The associated probability of failure is added at the end of the calculation ($PFH_{MPC} = 3.0 \times 10^{-7}$ per hour [E]). For the remaining part of the control system, the probability of failure is calculated below.
- $MTTF_d$ of the logic control: an $MTTF_d$ of 11,415 years [D] is assumed for the bus transceivers K1 and K2. In accordance with SN 29500-2, an $MTTF_d$ of 878 years [D] is considered for the microcontrollers K3 and K4, including peripherals. The following values are substituted for the remaining components [D]: 45,662 years for the switching transistors K5 and K7, 228,310 years for the resistances R1 and R2, and 1,141 years for the measuring amplifiers K6 and K8. The $MTTF_d$ values of the channels are thus 329 years and 815 years. Following capping to 100 years, the resulting symmetrized $MTTF_d$ value is 100 years.
- $DC_{avg}$ of the logic control: the *DC* is 99% for K1 and K2 owing to cross-checking of the messages in the microcontrollers K3 and K4; the *DC* is 60% for K3 and K4 owing to cross-checking and self-tests of simple effectiveness achieved by software; and the *DC* is 90% for the remaining components owing to fault detection in K4 by means of the position measuring system 1S4. The averaging formula for $DC_{avg}$ produces a result of 74% (“low”).
- Adequate measures against common cause failure (65 points): separation (15), overvoltage protection (15) and environmental conditions (25 + 10)




- The logic control corresponds to Category 3 with a high $MTTF_d$ per channel (100 years) and low $DC_{avg}$ (74%). This results in an average probability of dangerous failure of $7.36 \times 10^{-8}$ per hour.
- $MTTF_d$ of the hydraulic part of the control system: an $MTTF_d$ of 150 years [S] is substituted for the proportional valve 1V4 and the directional control valve 1V3. Following capping, this results in a symmetrized $MTTF_d$ value of 100 years.
- $DC_{avg}$ of the hydraulic part of the control system: the DC for 1V4 and 1V3 is 99% owing to direct monitoring of the position in K4 via 1S4/1S3. The averaging formula for $DC_{avg}$ produces a result of 99% (“high”).
- Adequate measures against common cause failure (70 points): separation (15), the use of well-tried components (5), overpressure protection (15) and environmental conditions (25 + 10)
- The hydraulic part of the control system corresponds to Category 4 with a high $MTTF_d$ per channel (100 years) and a high $DC_{avg}$ (99%). This results in an average probability of dangerous failure of $2.47 \times 10^{-8}$ per hour.
- The average probability of dangerous failure of the safety function is produced by addition of the proportions for the MPC, the logic control and the hydraulic part. The total is $3.98 \times 10^{-7}$ per hour. This corresponds to PL d.

**More detailed references**

- ISO 15998: Earth-moving machinery – Machine control systems (MCS) using electronic components – Performance criteria and tests for functional safety (04.08)
- IEC 61784-3: Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions (12.07)
- Prüfgrundsätze Bussysteme für die Übertragung sicherheitsrelevanter Nachrichten GS-ET-26. Ed.: Fachausschuss Elektrotechnik, Cologne 2002. www.dguv.de, Webcode d14884