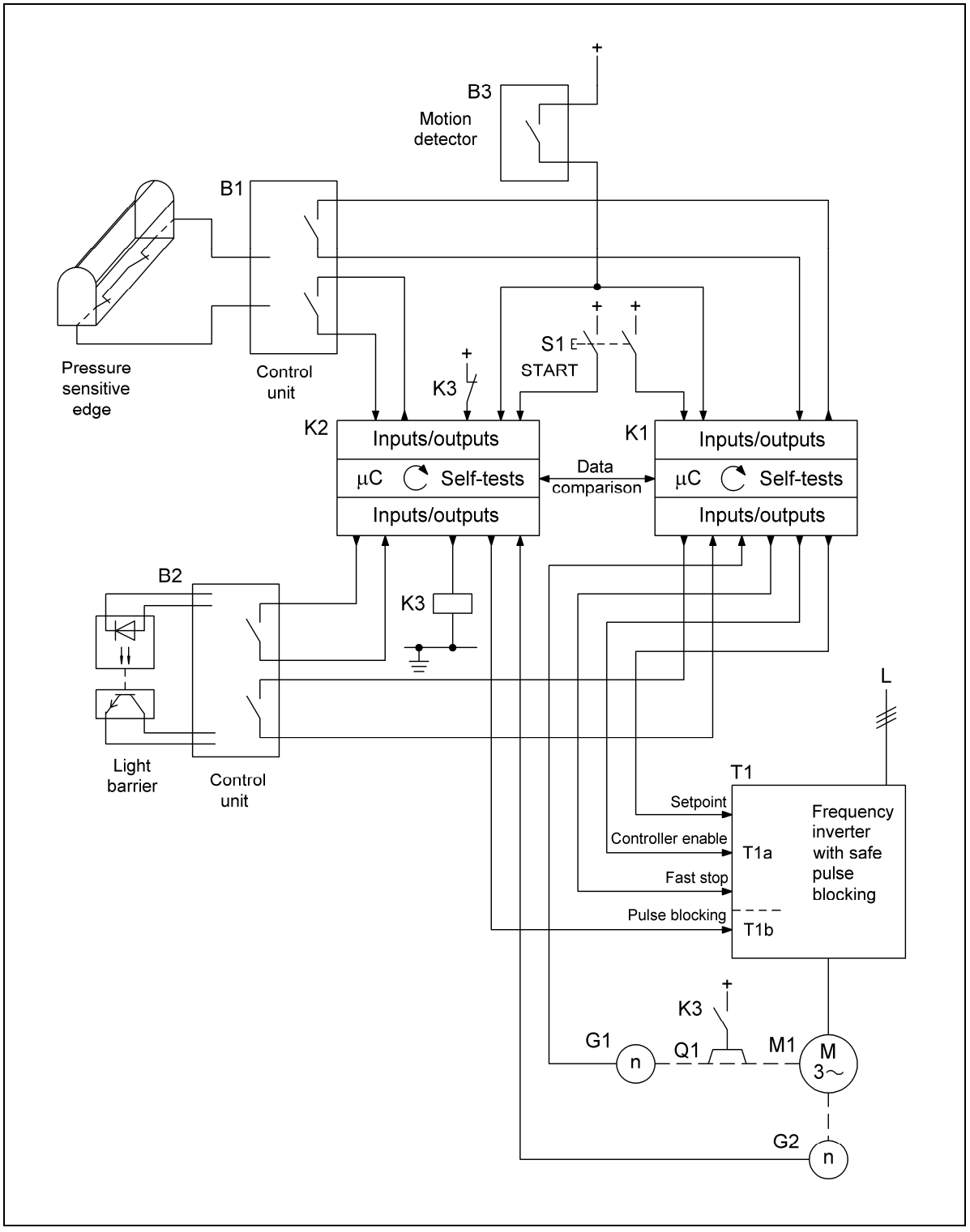
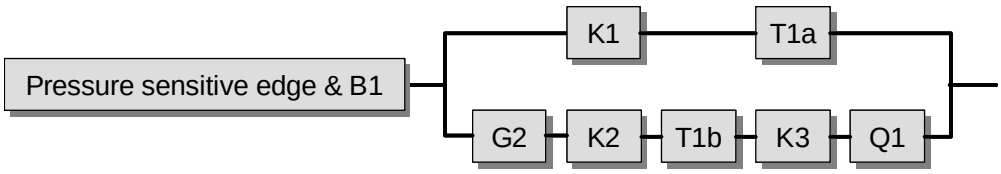
## 8.2.23 Revolving door control – Category 3 – PL d (Example 23)

Figure 8.40:
Revolving door control employing microcontrollers






**Safety functions**

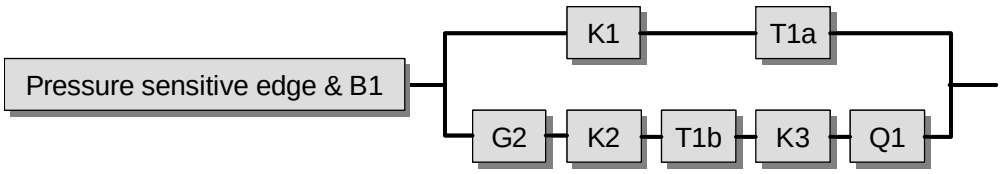
- Safety-related stop function: when the pressure sensitive edge is actuated, the revolving movement of the door is halted (SS1 – safe stop 1).
- Safely limited speed (SLS): when a person or object is detected by the light barrier, the speed of the revolving door is reduced and safely limited.

**Functional description**

- The revolving movement of the door is initiated only once the control system has been switched on by the pushbutton S1. In normal operation, the command for the revolving movement is issued by the motion detector B3 located on the door. The frequency inverter T1 is actuated jointly by the two microcontrollers K1 and K2. Each microcontroller (µC) contains a central processing unit (CPU) in the form of a microprocessor, and working memory (RAM) and read-only memory (ROM). K1 controls the functions of setpoint assignment, enabling of the controller, and fast stop. K2 actuates pulse blocking, and the holding brake Q1 can be released by means of the contactor relay K3. The rotary signal encoders G1 and G2 transmit the motor speed to K1 and K2 respectively.
- Faults in the pressure sensitive edge or light barrier are detected in the associated control units B1 and B2. The same applies to faults in B1 and B2 themselves, which are detected by internal monitoring. Faults in the components of the microcontrollers are detected by the performance of self-tests and by data comparison. Proper operation of the frequency inverter T1 is monitored by means of the rotary signal encoders G1 and G2 in K1 and K2 respectively. When detected, faults are controlled via K1 and/or K2, leading to the door's movement being halted by T1 and/or Q1. The wings of the door can be opened manually in order for trapped persons to be freed.
- Owing to redundant processing channels, a single fault does not result in loss of the safety function. The combination of undetected faults may lead to loss of the safety function.

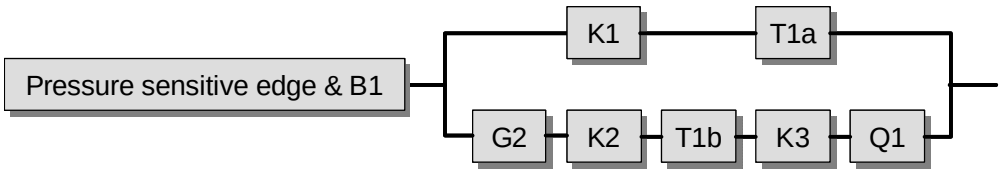
**Design features**

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- The pressure sensitive edge safeguards against crush, shear and entrapment points. It is connected to the control system via B1. The subsystem, comprising sensor and control unit, satisfies the requirements of EN 1760-2 in Category 3 and of EN ISO 13849-1 for PL d. Faults in the sensor of the pressure sensitive




edge or in the supply conductors must be excluded or be detected via the control unit (pressure sensitive edges operating on either the break-contact or make-contact principle may be employed). When a pressure sensitive edge is reset following actuation, the rotary movement begins again with a time delay. The pressure sensitive edge possesses an adequate deformation path and an adequate range of action.

- The light barrier has the function of leading, non-contact safeguarding of hazardous zones. Together with B2, it satisfies at least the requirements for Type 2 to EN 61496-1 and IEC 61496-2, and to EN ISO 13849-1 for PL d. The revolving speed, which is safely reduced following detection of a person or an object by the light barrier, is increased again to the normal speed following a present timeout. The supply conductors to the transmitter and receiver are laid separately or with protection.
- During the first start-up of the door's revolving movement, start-up tests are performed. The tests include, for example, tests of the microcontroller blocks (microprocessor, random-access and read-only memory), input and output tests, and checking of driving of the motor by the frequency inverter (including testing of controller enabling, the fast-stop functionality and pulse blocking). A brake test is also performed, in which the frequency inverter is required to act against the operating holding brake.
- During comparison of data between the two controllers, desired values and intermediate results are exchanged, with inclusion of the cyclical self-tests.
- Since the frequency inverter employs safe pulse blocking, a contactor is no longer required for de-energization of the supply voltage. The frequency inverter is suitable for driving and braking.
- K3 possesses mechanically linked contact elements to IEC 60947-5-1, Annex L. The switching position of the break contact is monitored by the microcontroller K2 for the purpose of fault detection.
- It is assumed in the example that closed-loop control provided by the frequency inverter T1 is sufficient for braking of the revolving door. Once the drive has come to a halt, pulse blocking is activated and controller enabling cancelled in order to prevent unexpected start-up. The braking time and braking distance are monitored by the controller. The brake Q1 is required in the event of a fault so that, should T1 for example no longer be able to execute the specified function, no danger may arise owing to an undesired movement. Q1 operates on the closed-circuit current principle.
- The software (SRESW) in K1 and K2 is programmed in accordance with the requirements for PL d as per Section 6.3.




- The standard components G1 and G2 (where relevant for the rotary signal encoders) and T1 are employed in accordance with the instructions in Section 6.3.10.
- For the safety function “safely limited speed”, a fault exclusion is assumed for the fault condition of encoder shaft breakage (G1/G2). For details of the possibility of a fault exclusion, refer for example to IEC 61800-5-2, Table D.16.

**Remarks**

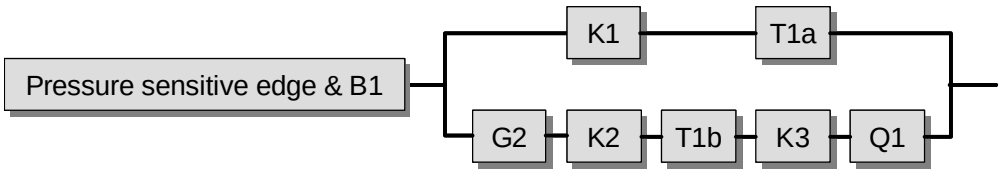
- The circuit example can be employed for implementation of the safety functions “safety-related stop function” and “safely limited speed” in a control system for three-wing and four-wing revolving doors with break-out function (the wings can be folded manually in an emergency) for use in public and commercial buildings.
- Regular manual inspection of the pressure sensitive edge is required. Firstly, the functionality must be checked; secondly, the pressure sensitive edge must be inspected visually in order for any damage to be detected in good time.

**Calculation of the probability of failure**

- For calculation of the probability of failure, the frequency inverter T1 is broken down into the blocks T1a and T1b. The block T1a contains the functions set-point assignment, enabling of the controller and fast stop, and their implementation in the control system. The block T1b contains the safe pulse blocking function, which is achieved by a small number of components.

The detailed calculation of the probability of failure is performed for the “safety-related stop function (SS1)”, which is also shown in the block diagram:

- Since the pressure sensitive edge with the associated control unit B1 is available commercially as a safety component, its probability of failure is added at the end of the calculation ($3.00 \times 10^{-7}$ per hour [E]).
- $MTTF_d$: the safety-related components of K1 and K2 and their peripherals are considered, following application of the parts count method, by a value of 878 years [E]. A value of 75 years [E] is substituted in the formula for G2. Values of 100 years [E] for T1a and of 1,000 years [E] for T1b are substituted in the formula. A $B_{10d}$ value of 400,000 cycles [S] is substituted for K3. At one operation per day, $n_{op}$ is 365 cycles per year, and the $MTTF_d$ is 10,959 years. Q1 is considered with an $MTTF_d$ of 50 years [E]. The holding brake Q1 is required only in the event of a fault, and is not subject to operational wear. Overall, the symmetrized $MTTF_d$ value per channel is 64.3 years (“high”).



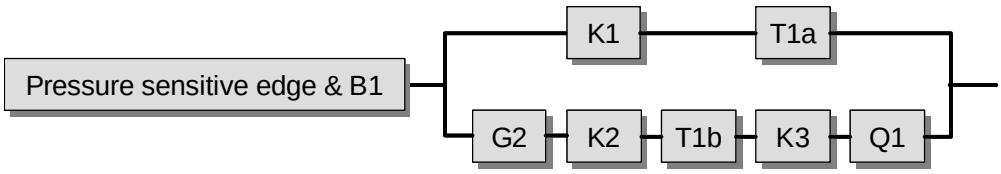

- $DC_{avg}$: owing to the selection of suitable test measures, the *DC* value for K1 and K2 is 60%. Internal self-tests are performed on the microcontroller components. A *DC* of 90% is substituted for the block T1a, since fault detection occurs via the process. G2 is rated with a *DC* of 90%; here too, fault detection is provided by the process and by the comparison with G1 via K1 and K2. K3 is rated with a *DC* of 99% owing to direct monitoring of readback of a mechanically linked contact. Owing to performance of the static start-up test, a *DC* of 60% is substituted for T1b and a *DC* of 30% for Q1. Averaging thus produces a $DC_{avg}$ of 62% (“low”).
- Adequate measures against common cause failure (70 points): separation (15), FMEA (5), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the control elements corresponds to Category 3 with a high $MTTF_d$ (64.3 years) and low $DC_{avg}$ (62%). For the combination of the components K1 and T1a in the first channel and G2, K2, T1b, K3 and Q1 in the second channel, the average probability of dangerous failure is $1.94 \times 10^{-7}$ per hour. Together with the sensor unit consisting of pressure sensitive edge and control unit B1, the overall average probability of dangerous failure of the control for this safety function is $4.94 \times 10^{-7}$ per hour. This corresponds to PL d.

**Calculation of the probability of failure for the safety function “safely limited speed (SLS)”:**

- G1 must also be considered in the first channel for this calculation. An $MTTF_d$ of 75 years [E] is substituted for this purpose. The *DC* of 99% is derived from fault detection via the process and the comparison with G2 via K2 and K1. Adequate measures against common cause failure were selected in the same way as for the first example analysis. With an $MTTF_d$ of 34.9 years and a $DC_{avg}$ of 70%, the average probability of dangerous failure is $4.46 \times 10^{-7}$ per hour. Following addition of the sensor unit, in this case consisting of the light barrier and control unit B2 with a value of $2.00 \times 10^{-7}$ per hour [E], the overall average probability of dangerous failure of the control system for this safety function is $6.46 \times 10^{-7}$ per hour. This also corresponds to PL d.

**More detailed references**

- EN 1760-2: Safety of machinery – Pressure sensitive protective devices – Part 2: General principles for the design and testing of pressure sensitive edges and pressure sensitive bars (03.01)
- DIN 18650-1: Schlösser und Baubeschläge – Automatische Türsysteme (12.05). Beuth, Berlin 2005




- IEC 60947-5-1: Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices (11.03)
- EN 61496-1: Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests (05.04)
- IEC 61496-2: Safety of machinery – Electro-sensitive protective equipment – Part 2: Particular requirements for equipment using active opto-electronic protective devices (AOPDs) (04.06)
- IEC 61800-5-2: Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional (07.07)

Figure 8.41:
Determining of the PL by means of SISTEMA