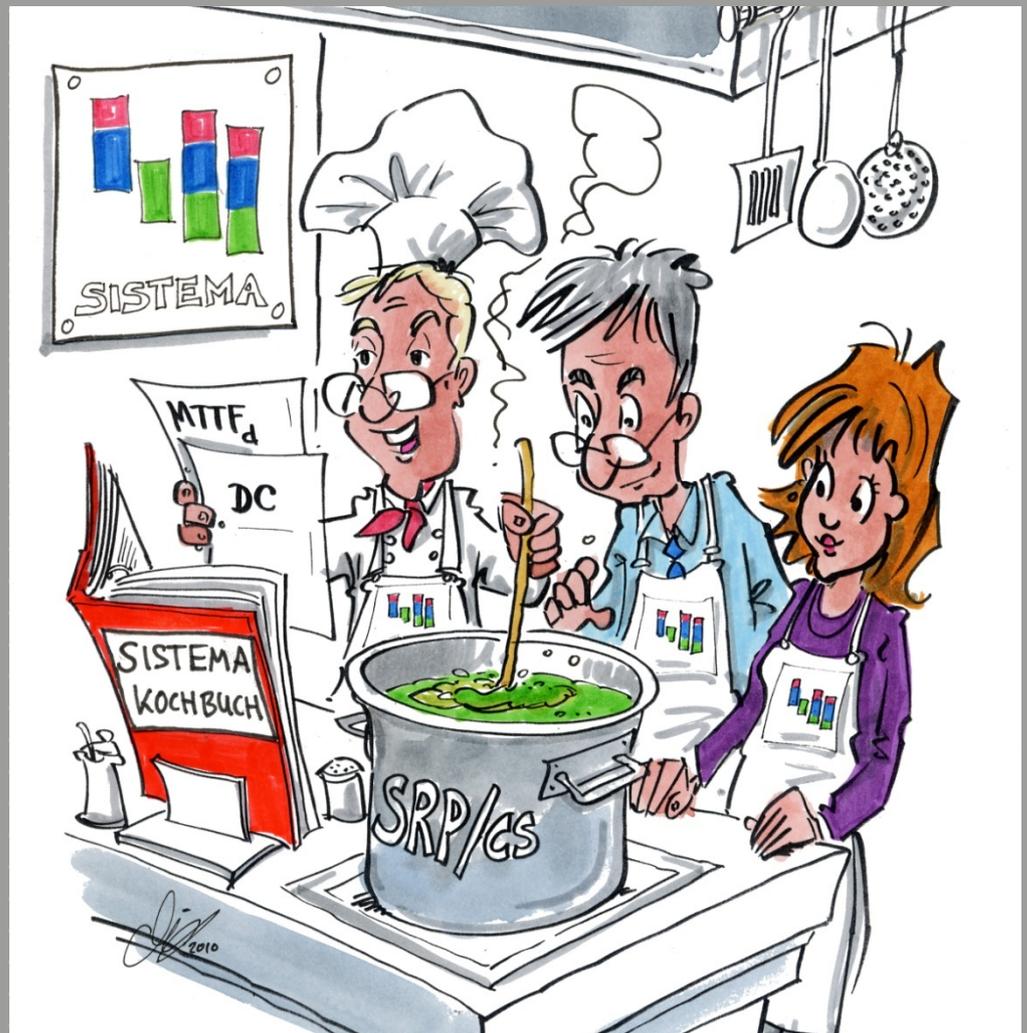


The SISTEMA Cookbook 1

From the schematic circuit diagram to the
Performance Level – quantification of safety
functions with SISTEMA

Version 1.0 (EN)



Verfasser: Ralf Apfeld, Michael Hauke, Michael Schaefer, Paul Rempel, Björn Ostermann
Institute for Occupational Safety and Health of DGUV (IFA),
Sankt Augustin

Herausgeber: Institut für Arbeitsschutz der Deutschen Gesetzlichen
Unfallversicherung (IFA)
Alte Heerstr. 111, 53757 Sankt Augustin, Germany
Phone: +49 2241 231-02
Fax: +49 2241 231-2234
Internet: www.dguv.de/ifa

– October 2010 –

Contents

| | | |
|-----------------|---|-----------|
| 1 | Introduction..... | 4 |
| 2 | Schematic circuit diagram showing functional and test channels..... | 6 |
| 2.1 | Creating the schematic circuit diagram | 6 |
| 2.2 | Entering the function and test channels | 7 |
| 3 | From the schematic circuit diagram to the safety-related block diagram | 9 |
| 3.1 | Categories to EN ISO 13849-1 | 9 |
| 3.2 | Structural analysis and explanations | 10 |
| 4 | Transfer to SISTEMA..... | 15 |
| 4.1 | Creating a project | 16 |
| 4.2 | Creating safety functions | 17 |
| 4.3 | Setting the PLr | 17 |
| 4.4 | Adding subsystems | 17 |
| 4.5 | Encapsulated subsystems | 18 |
| 4.6 | Subsystems as groups of blocks within a rigid structure (Category) | 18 |
| 4.6.1 | Entering blocks | 20 |
| 4.6.2 | Entering elements..... | 20 |
| 4.6.3 | Entering safety-related data | 21 |
| 4.6.3.1 | MTTF _d /B _{10d} | 21 |
| 4.6.3.2 | DC | 22 |
| 4.7 | Objective attained? | 23 |
| Annex A: | Concepts and abbreviations..... | 24 |
| Annex B: | Abbreviations from EN ISO 13849-1 | 25 |
| Annex C: | Model form for user's applications | 26 |
| Annex D: | Schematic table | 27 |
| Annex E: | Flow chart for structure analysis (without example)..... | 29 |

1 Introduction

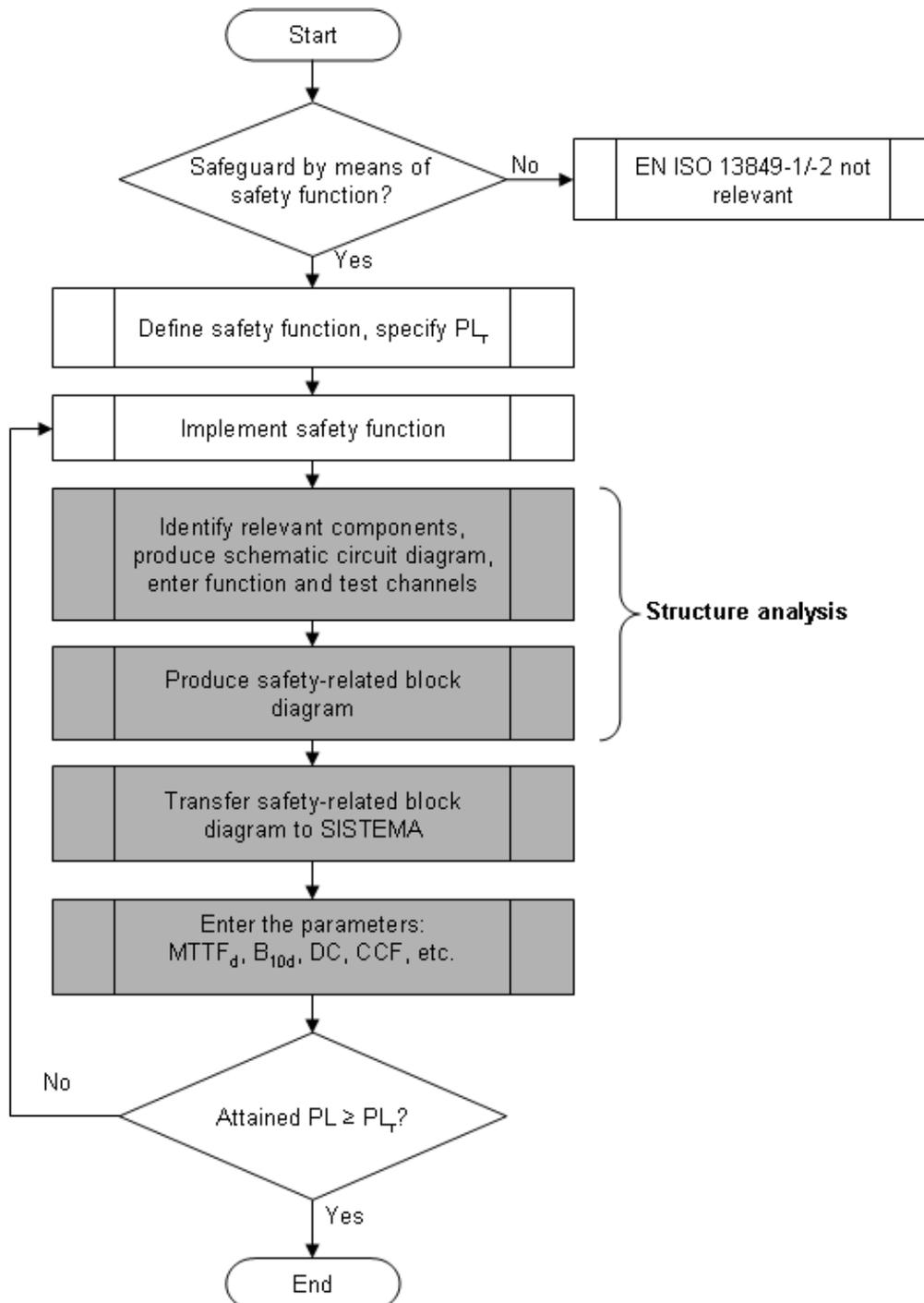
Control systems which perform safety functions are employed in order for machines to be designed safely and thereby to satisfy the requirements of the Machinery Directive, 2006/42/EC. For this purpose, the safety functions required for risk reduction are defined as part of the risk assessment conducted during design of the machine and then implemented by means of a suitable control system. The safety-related parts of machine controls can be implemented in accordance with EN ISO 13849-1. Included in the requirements of this standard is the necessity for the machine design engineer to calculate the probability of a dangerous failure per hour (**PFH**) in order to determine the Performance Level (**PL**). The Performance Level is dependent upon the control system's structure (Category), as well as the systematic requirements.

For this purpose, the IFA provides the SISTEMA software tool (the German acronym stands for "safety of controls on machines"), which can be downloaded free of charge from www.dguv.de/ifa, Webcode [e34183](#).

Before beginning the calculations, the machine design engineer must produce a safety-related block diagram for each safety function from the circuit diagram. The safety-related block diagram must show the implementation of the safety function in functional channels (including redundant channels, where present) and testing components, also where present.

The SISTEMA Cookbook 1 addresses this unfamiliar and difficult abstraction step (Figure 1) and the subsequent step, that of transferring the blocks to SISTEMA and entering their parameters.

Figure 1:
Flow chart, from the safety function to the Performance Level; the four steps with grey background are described in detail in these instructions.



2 Schematic circuit diagram showing functional and test channels

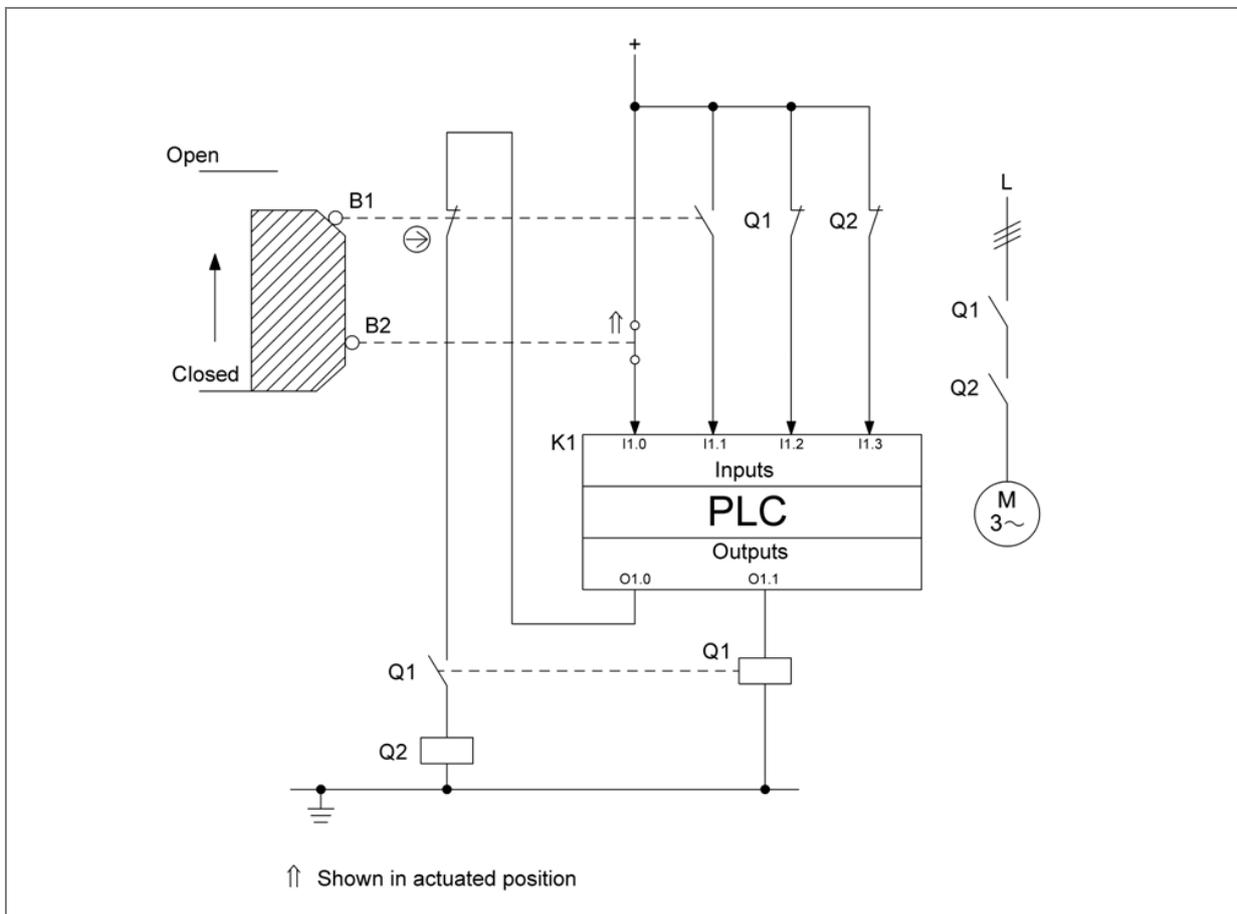
2.1 Creating the schematic circuit diagram

In order for the probability of failure of a safety function to be calculated at a later stage, it must be known which components are employed in the safety function and which are not. A precise definition of the safety function (see BGIA Report 2/2008, Chapter 5) is therefore indispensable for the subsequent steps. The schematic circuit diagram showing the relevant components is produced for each safety function. The relevant components include all those of which the failure may impair execution of the safety function in a functional channel (redundant structures possess two functional channels). They also include all test facilities responsible for detecting such dangerous failures and bringing about a safe state. A schematic circuit diagram shows for example the electrical circuitry of position switches, programmable logic controllers (PLCs) and contactors, and the flow of current from the sensor, via signal processing, to the actuator.



Example 1 (Figure 2) shows an implementation of the safety function for "opening of the movable guard initiates the safe torque off (STO) safety function". All other components which are purely functional and have no influence upon the safety function have already been omitted.

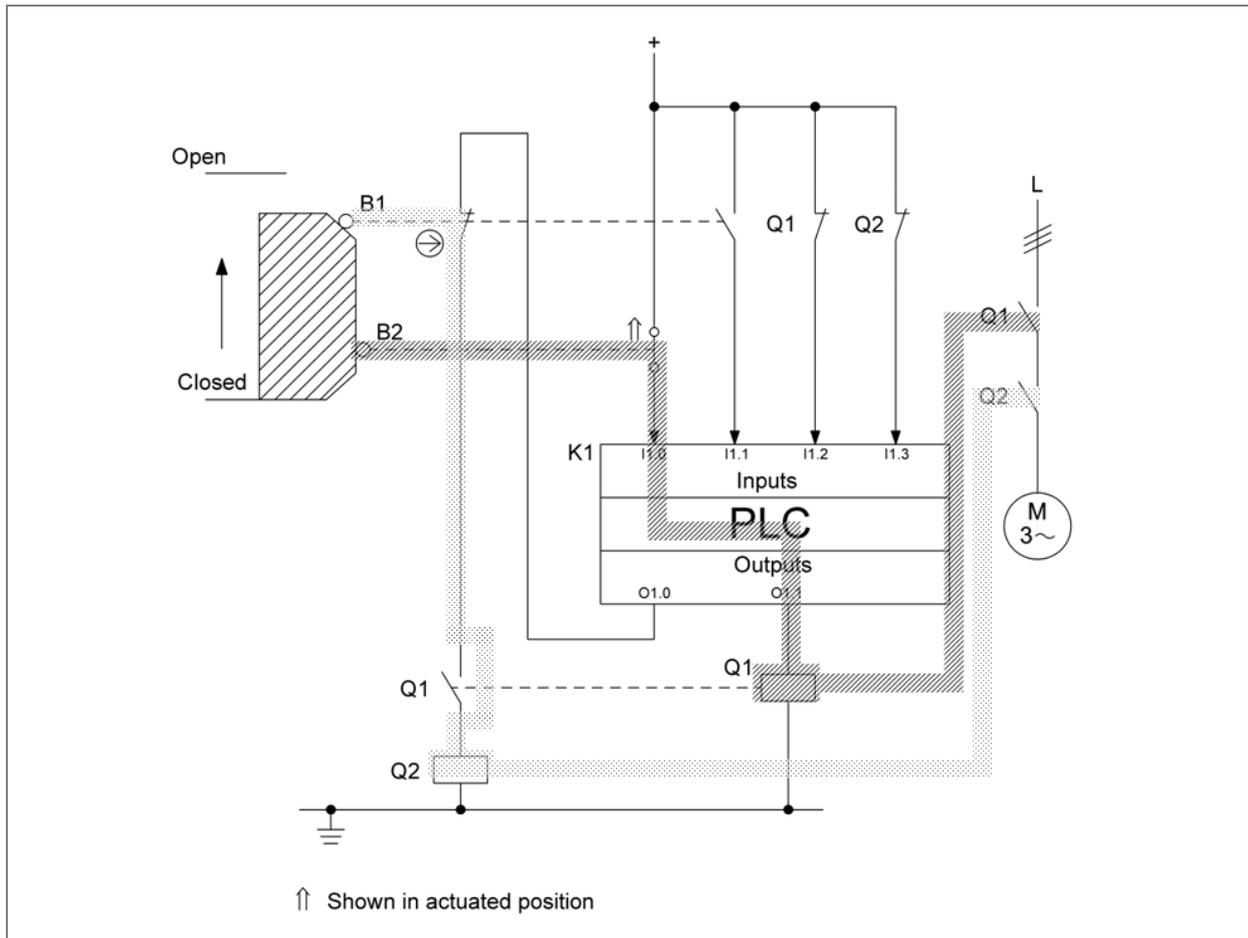
Figure 2:
Schematic circuit diagram showing relevant components (Example 1); see BGIA Report 2/2008e, Chapter 8.2.18



2.2 Entering the function and test channels

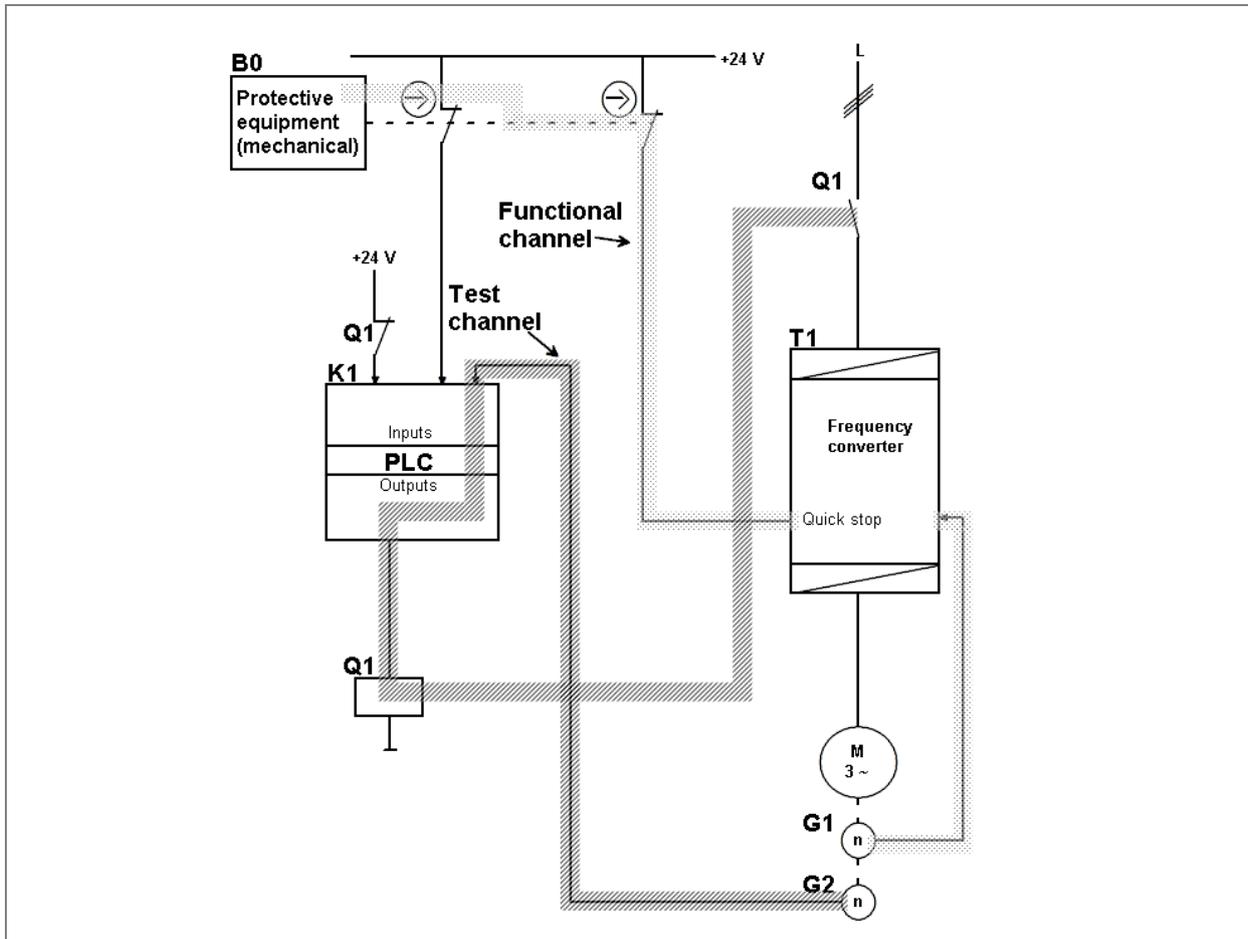
The functional channels are first marked on the schematic circuit diagram. It has been found effective in practice to "work backwards", i.e. to begin at the actuator end and follow the channel back to the sensor. This yields the signal paths from the triggering event to the response of the safety function (Figure 3).

Figure 3:
Schematic circuit diagram with two redundant functional channels, B1-Q2 and B2-K1-Q1 (Example 1)



Where circuits employ a test channel with a dedicated disconnecting device (Category 2), this test channel is also marked on the schematic circuit diagram. Figure 4 shows the example of a protective device fitted at the intake of a roller; when the device is tripped, the motor is stopped within 1/3 of a rotation. In this example, the angle of rotation required for the motor to come to a stop is tested regularly by manual actuation of the protective device.

Figure 4:
 Example 2 with marked functional channel B0 – T1 – G1 and test channel with dedicated disconnecting device G2 – K1 – Q1



Chapter 3 explains how the schematic circuit diagram is transformed into a safety-related block diagram.

3 From the schematic circuit diagram to the safety-related block diagram

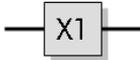
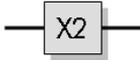
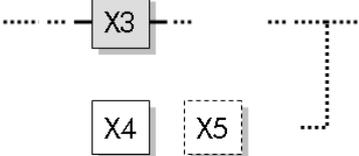
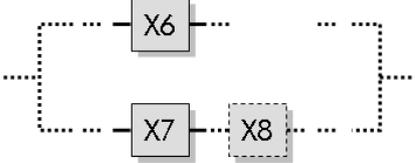
In the next step, the schematic circuit diagram is transformed for each safety function into the logical representation of the safety-related block diagram. In the course of the transformation, the components of the schematic circuit diagram are assigned to "subsystems" with which the safety function is modelled in SISTEMA.

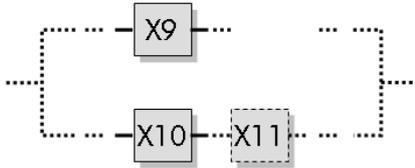
In the presentation as a safety-related block diagram **the logical interrelationships are relevant rather than the physical connections between the components.** Each component within a safety function is a constituent part of a certain structure. This structure is termed a "Category" in EN ISO 13849-1, and grouped within SISTEMA as a subsystem. The sequences of subsystems with their corresponding Categories are represented by a safety function in the form of a safety-related block diagram. The sequence of the subsystems has no bearing upon subsequent calculation of the probability of failure.

3.1 Categories to EN ISO 13849-1

The Categories to EN ISO 13849-1, their characterizing features and their typical representation are shown in Table 1.

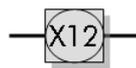
Table 1: Features and representation of the Categories

| Structure | Category to EN ISO 13849-1 and particular features | Typical representation in the safety-related block diagram |
|-----------------------------------|---|--|
| Single-channel | Category B (basic category) |  |
| Single-channel | Category 1 (use of well-tried components) |  |
| Single-channel, tested | Category 2 (component faults in the functional channel (X3) are detected by fault detection via the test channel (X4, X5); the safe state is brought about) Note: the functional and test channel may comprise one or more component(s). |  |
| Two-channel, with fault detection | Category 3 (single-fault tolerance by redundancy, testing) Note: Each channel may comprise one or more component(s). |  |

| Structure | Category to EN ISO 13849-1 and particular features | Typical representation in the safety-related block diagram |
|-----------------------------------|--|--|
| Two-channel, with fault detection | Category 4 (as for Category 3, but also robust against the accumulation of two undetected faults) Note: Each channel may comprise one or more component(s). |  |

Encapsulated subsystems constitute a particular case. Encapsulated subsystems are components for which the manufacturer himself states the PL, PFH and Category (e.g. safety PLC, safety modules); see Table 2.

Table 2: Encapsulated subsystems

| Structure | Category to EN ISO 13849-1 and particular features | Typical representation in the safety-related block diagram |
|--|---|---|
| Different internal structures possible | PL, PFH and Category are stated by the manufacturer |  |



Note: Component arrangements other than these do not comply with the designated architectures of EN ISO 13849-1 and cannot be analysed by SISTEMA.

3.2 Structural analysis and explanations

In the structural analysis, the components in the schematic circuit diagram are transferred to a safety-related block diagram, and the Category is determined by means of the characteristics of redundancy, testing, and the use of well-tried components.

Note: This section is only concerned with determining the structure. Additional requirements beyond this apply to all Categories: for example, components must be designed, fabricated, selected, assembled and combined in compliance with the relevant standards in such a way that they are able to withstand the anticipated ambient conditions. Essential safety principles must be applied. In Categories 1, 2, 3 and 4, safety principles which are well-tried must also be applied. Information on these aspects can be found in EN ISO 13849-2. Quantitative requirements the observance of which is checked by SISTEMA also apply to the Categories.

The procedure described here is geared to the application of EN ISO 13849-1 and its "designated architectures" for the Categories. If modelling to one of the categories is not possible, even when additional components or channels are omitted, the simplified method described in the standard cannot be applied. In this case, the probability of failure must be verified with recourse to other methods, such as Markov modelling, as described in EN 61508-6, Annex B.

Procedure for structural analysis:

The starting-point for the structural analysis is the schematic circuit diagram on which the function and test channels are marked. The procedure is shown schematically in Annex E. Figure 5 contains the same procedure, together with its application to Examples 1 and 2 shown in Chapter 2.

Step 1: Formation of a sequence of the components in a functional channel

All components along the first functional channel (that with the fewest components) are written as blocks from left to right (from the sensor to the actuator).

Step 2: Considering the first block

Each individual block of the first functional channel is now assigned in turn to subsystems of the relevant Category, according to the characteristic features of the Categories.

Step 3: Does the component manufacturer state the PL and PFH (and Category)?

An encapsulated subsystem can be recognized as such by the fact that it is already characterized by the manufacturer by a PL (or SIL in accordance with IEC standards), PFH and Category (internal structure). The internal structure of the encapsulated subsystem need not be deconstructed further.

Note: If a Category 3 or 4 encapsulated subsystem occupies in both redundant functional channels, both functional channels pass through it.

Step 4: Can all component faults be excluded?

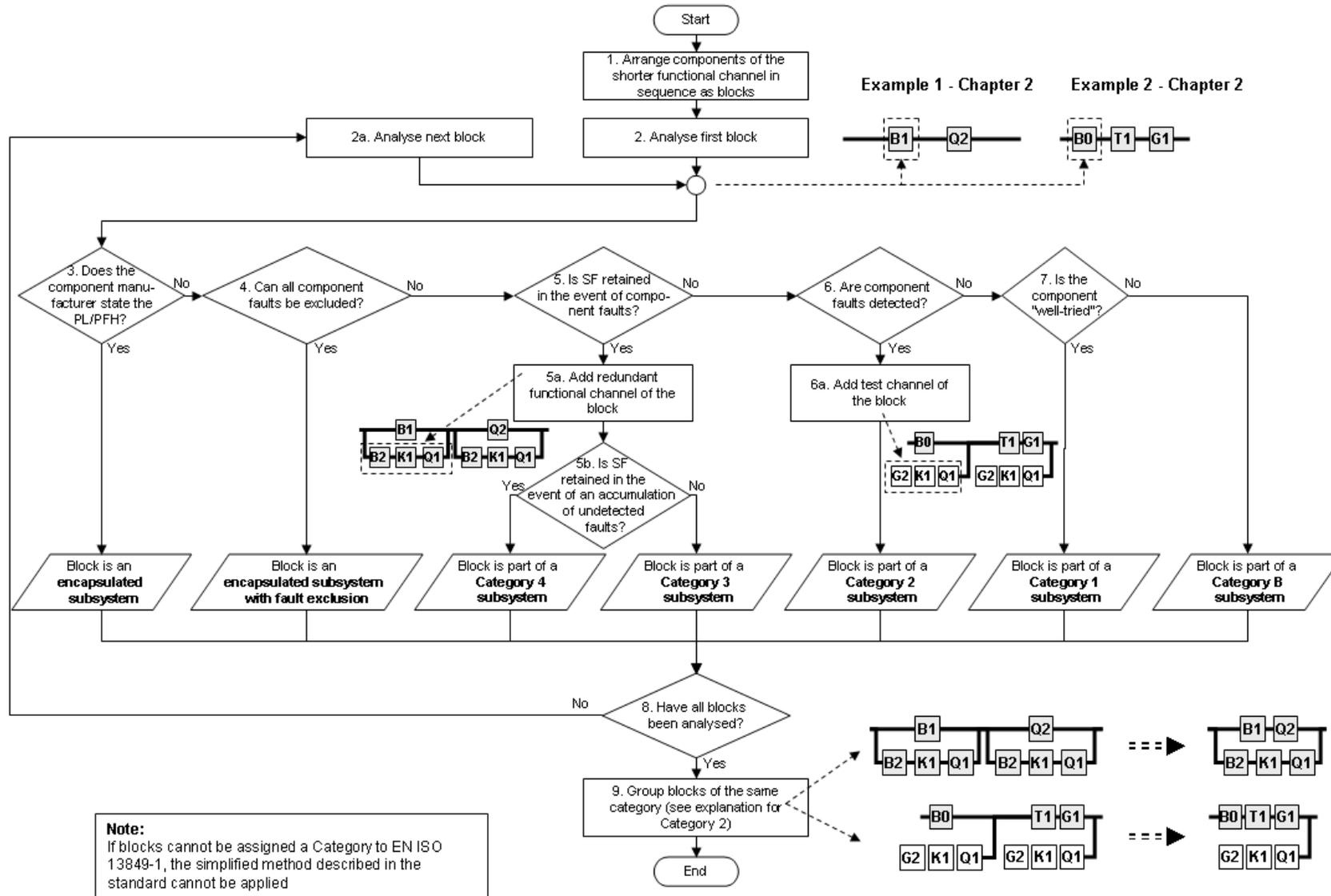
All assumed faults for the component in the block under analysis are considered in turn. For this purpose, the annex of EN ISO 13849-2 contains the fault models of a number of components used in machine controls. Owing to justified fault exclusions, certain component faults can be discounted. For each fault case, it must be considered whether the intended safety-related functionality of the component is retained (harmless fault) or fails (dangerous fault). A dangerous fault exists for example for contactor Q2 in Example 1 (Figure 3) when the safety door is opened but Q2 fails to drop out because its contacts have welded.

Should no dangerous faults whatsoever need to be assumed for the component, no value exists for calculation of the PFH of the safety function. It need not be considered in the safety-related block diagram. Further presentation of the safety function can however be constructive, since it may be conducive to an understanding of it. In this case, the block is treated as an encapsulated subsystem ("fault exclusion" is then subsequently ticked in SISTEMA, and further entries are not required).

**Step 5: Is the safety function retained in the event of component faults?**

The dangerous faults to be assumed for the component in the block under analysis are determined in Step 4. Their effects upon the safety function are now considered.

Figure 5: Flow chart of structural analysis with reference to the examples from Chapter 2: SF = safety function



Step 5a: Adding the redundant functional channel of the block(s)

If the safety function is maintained by one or more redundant components in the event of a fault in the block under analysis (i.e. a second functional channel is present), these components are presented as blocks in a second functional channel (refer to the example in Table 1: Categories 3 and 4).

In Example 1 (Figure 3), this applies to both B1 and Q2. The redundant functional channel B2-K1-Q1 is therefore added to both blocks.

Note: The components of the redundant functional channel are thus used several times. This is a result of the phased procedure and should not be a hindrance at this stage. Blocks of which multiple instances exist are grouped together again in Step 8.



If redundant components have been entered, a major basic criterion for Categories 3 and 4 has been met. A single fault in a component of the first or second functional channel must not result in loss of the safety function (single-fault tolerance).

Note: In addition, Category 3 requires that, wherever reasonably possible, individual faults in components within the two functional channels should be detected.

Step 5b: Is the safety function retained in the event of an accumulation of undetected faults?

For the block under analysis here and its redundant functional channel, single-fault tolerance has been identified up to this point and Category 3 is satisfied. Are the criteria for Category 4 also met? For this purpose, the behaviour in the event of undetected faults occurring must be studied. If the safety function is retained in the event of an accumulation of two undetected faults, the subsystem satisfies Category 4. If the safety function is not retained at the second undetected fault, the subsystem satisfies Category 3.

In Example 1 (Figure 3), PLC K1 could actuate outputs O1.0 and O1.1 continuously in the event of a fault. Q1 would be continually energized in this case. Even if the PLC were able to detect this fault by reading back of the monitoring contacts, it would not be able to bring about the safe state. Should a second fault then cause the contacts of Q2 to weld, the motor would continue to run even with the protective equipment open; the safety function has failed, and Category 4 is not met.

Note: In Category 4, single-fault tolerance must be satisfied and the discrete fault in a component in the first or second functional channel must be detected at or before the next demand upon the safety function. If detection in this way is not possible, an accumulation of two undetected faults must not lead to loss of the safety function.

Step 6: Are component faults detected?

At this point, it is clear that there is no redundancy and that consequently neither Category 3 nor Category 4 is met. If failure of a block in a test channel is detected by a test channel and the safe state is brought about, the subsystem satisfies Category 2.

In Example 2 (Figure 4), tripping of B0 causes controlled stopping of the motor by T1/G1 within 1/3 of a rotation. Testing is in response to a demand by K1 prompted by manual actuation of B0 and measurement of the stopping angle by K1/G2. In the event of a fault, the safe state is brought about via Q1. The test detects faults in B0 and T1/G1. The test channel G2-K1-Q1 thus detects faults in B0 and T1/G1 and brings about the safe state; Category 2 is thus met.

Note: Reasonable fault detection is also a requirement for Categories 3 and 4. Conversely, Category 2 subsystems lack a redundant functional channel.

Step 6a: Adding the test channel of the block

The components of the test channel which detect failure of the block and bring about the safe state are presented in the safety-related block diagram as test blocks as shown in Table 1 (Category 2)

If components are entered in the test channel, a major basic criterion for Category 2 is met: the safety function must be tested at suitable intervals. This causes the loss of the safety function to be detected and a safe state to be brought about by an independent disconnecting device. A further important requirement for Category 2 is the test frequency (see BGIA Report 2/2008e, Section 6.25). However this is not relevant to the structural analysis.

Step 7: Is the component "well-trying"?

Redundancy or testing was not found in the example. Only Category 1 or Category B are therefore possible. Should the component in the block under analysis be a "well-trying" component to EN ISO 13849, the block is presented as part of a Category 1 subsystem. A list of well-trying components can be found in EN ISO 13849-2. If not, the block is part of a Category B subsystem.

Step 8: Have all blocks been analysed?

If further blocks still await analysis following assignment of the block to a subsystem, the procedure on the diagram is repeated with the next block, beginning at Step 2a. The procedure otherwise continues at Step 9.

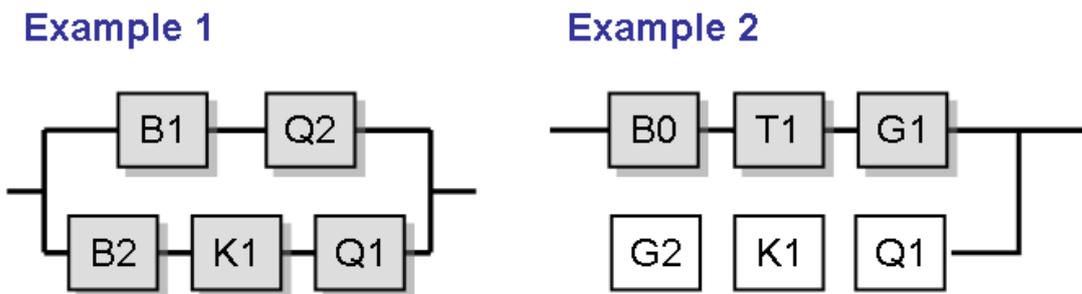
Step 9: Grouping blocks of the same category

Subsystems of the same category can be merged by the grouping of components of identical channels (see BGIA Report 2/2008, Figure 6.14). Each component occurs only once within a channel; duplicates can be removed. The same component clearly cannot be used simultaneously in two redundant functional channels. In Category 2, only components which share the same test channel can be grouped in a functional channel.

Since SISTEMA limits $MTTF_d$ values of each channel within the subsystems (capping), grouping may result in a lower probability of a dangerous failure per hour being calculated. The lower probability of failure (PFH) is an advantage. A disadvantage however is that the grouped representation often makes it more difficult to follow the logical sequence of signal processing.

The examples in Chapter 2 yield the safety-related block diagrams in Figure 5a:

Figure 5a: Result of the structural analysis for the examples from Chapter 2



The safety function is now presented logically on the safety-related block diagram. In the next chapter, the probability of failure (PFH) is calculated with the aid of SISTEMA.

4 Transfer to SISTEMA

The SISTEMA software tool employs multiple hierarchical levels (Figure 6). The individual levels are explained in Table 3.

Figure 6: Hierarchical levels in SISTEMA

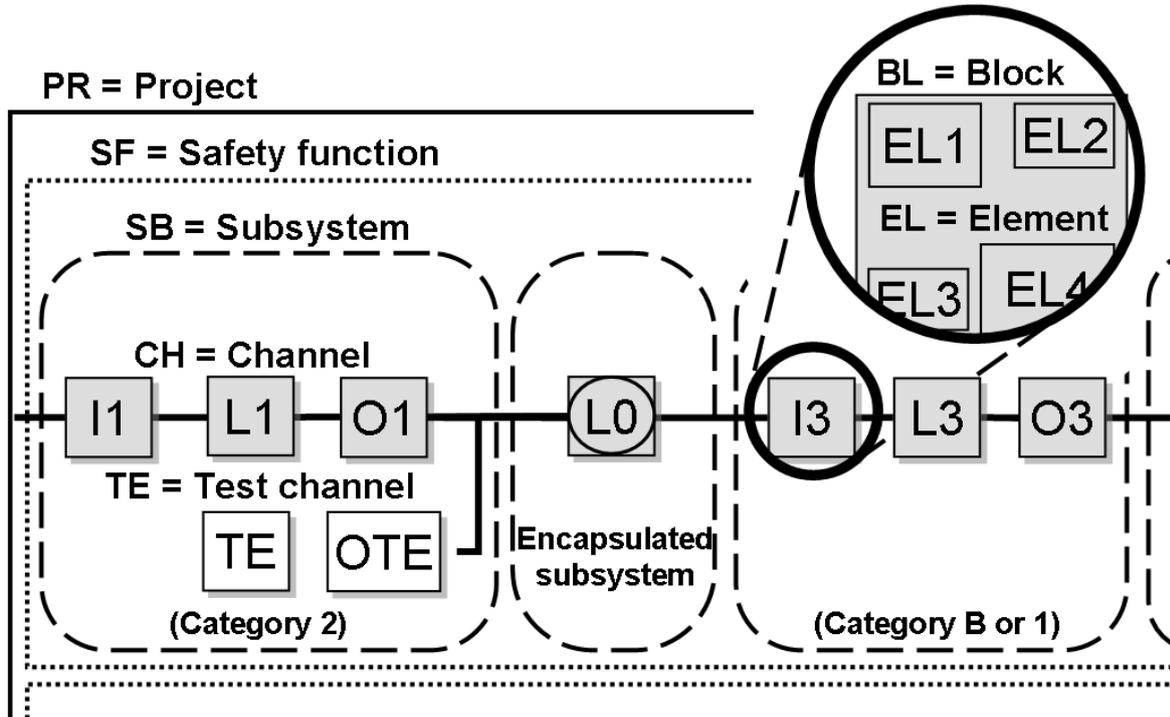
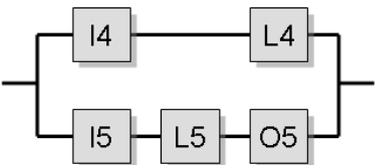
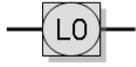
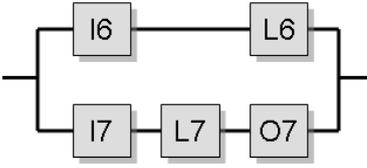
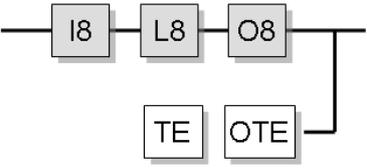
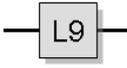


Table 3: Description of the hierarchical levels in SISTEMA

| Name | Description | Examples |
|------------------------|--|---|
| Project | Summary of safety functions, for example on a machine or part of a machine, or at a hazard point | Door to the working area on lathe XY |
| Safety function | Safety-oriented response to a triggering event | Safe operating stop when a safety door is opened |
| Subsystem | <p>a) Group of blocks within a rigid structure (Category)</p> <p>b) Safety component with statement by the manufacturer of the PL, PFH and Category (encapsulated subsystem)</p> | <p>a) Category 3 subsystem</p>  <p>b) Safety PLC</p>  |

| Name | Description | Examples |
|---------------------|--|---|
| Channel | Connection of blocks in series; SISTEMA creates either one or two functional channels, depending upon the selected Category. | <p>Functional channel 1</p>  <p>Functional channel 2</p> |
| Test channel | Connection of blocks in series for the test function; SISTEMA only creates a test channel for Category 2. | <p>Functional channel 1</p>  <p>Test channel</p> |
| Block | Component in the function or test channel |  <p>Safety PLC</p> |
| Element | A block contains one or more elements. A B _{10d} value (see Annex B) can only be entered for elements. | <p>Contactors, position switches, electromechanical components, all components with a manufacturer's B_{10d}-value</p> |

All steps required for creation of a SISTEMA project and for analysis are explained below. The entries relating to documentation have no influence upon the analysis. This aspect will not be considered further.

Note: It is advisable to select the order of entries such that the tabs in the working area are worked through from left to right, and the hierarchy levels (tree view in the navigation window) from top to bottom.

4.1 Creating a project

All safety functions of a machine or sub-machine can be grouped within a project (Figure 7). After creating a new project with "New" (1.), enter a name in the "Project name" dialog (3.). The name then also appears in the navigation window after the abbreviation PR (2.).

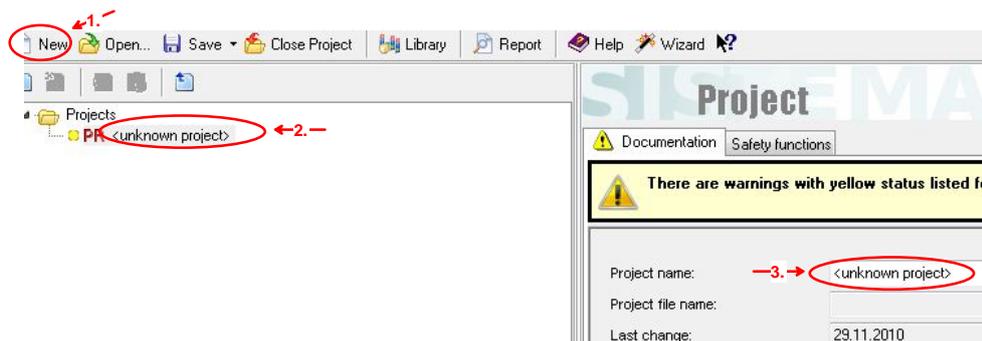


Figure 7

4.2 Creating safety functions

Create the required safety functions with "New" (3.) on the "Safety function" tab (2.) (Figure 8). The "Name of safety function" also appears in the navigation window, after the abbreviation **SF** (see Figure 9; 1.).

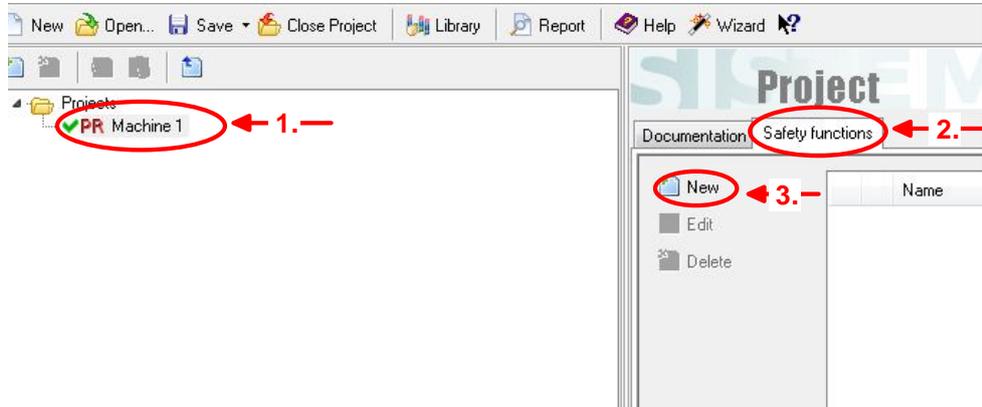


Figure 8

4.3 Setting the PLr

The required Performance Level PL_r is determined individually for each safety function (1.) (Figure 9). For this purpose, use the risk graph (3.) under "Safety function – PLr" (2.), or enter the PL_r is directly, for instance when it is specified by a machine-specific standard.

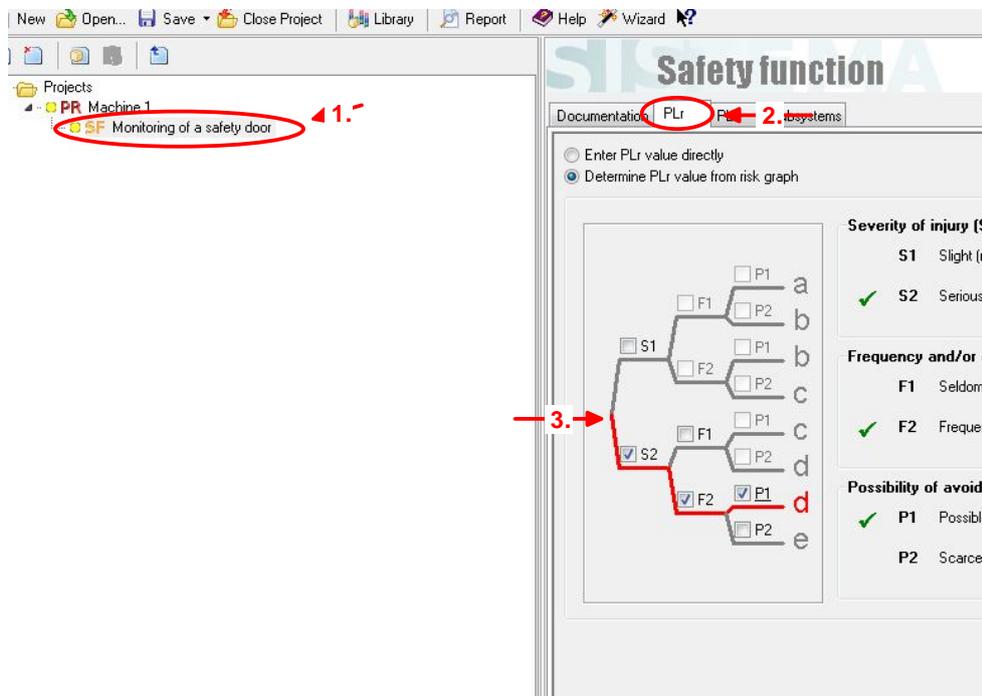


Figure 9

4.4 Adding subsystems

The subsystems determined in the safety-related block diagram are created. Add a subsystem with "New" (3.) under the safety function (1.) on the "Subsystems" tab (2.) (Figure 10).

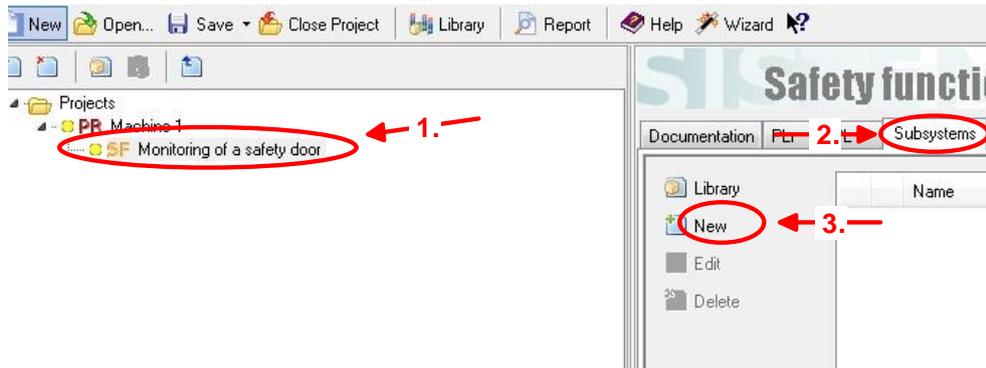


Figure 10

4.5 Encapsulated subsystems

Manufacturers' data on the PL, PFH and Category are available for encapsulated systems. Enter them (4.) directly below the subsystem (1.) in the "PL" tab (2.) after selecting "Enter PL / PFH directly" (3.) (Figure 11). The Category can be entered in the next tab, "Category". Since the PL and PFH are available for this subsystem, it is not necessary to enter the Category for calculation of the PFH of the safety function as a whole.

Note: If the box (4.) is checked, the PL and PFH are calculated from each other by means of mean values.

Fault exclusion:

In encapsulated systems in which all hazardous component faults are excluded, check the "Failure exclusion" box (→ PFH=0).

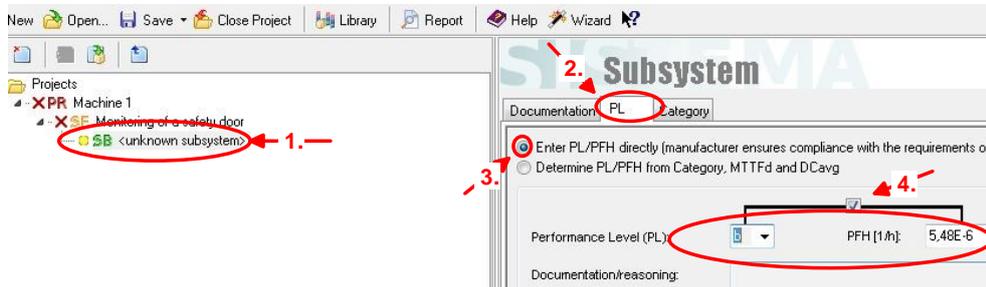


Figure 11

4.6 Subsystems as groups of blocks within a rigid structure (Category)

In the subsystem (1.), select "Determine PL / PFH from Category, MTTFd and DCavg" under "PL" (2.) (Figure 12).

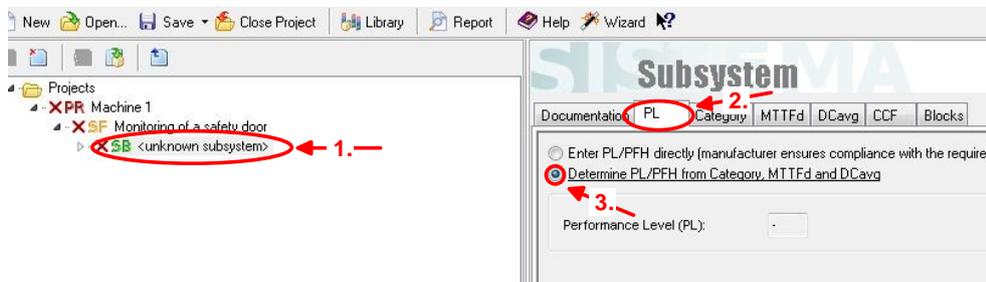


Figure 12

Then:

- a) In the subsystem (1.) under "Category" (2.) (Figure 13), select the relevant Category and evaluate the "Requirements of the Category".

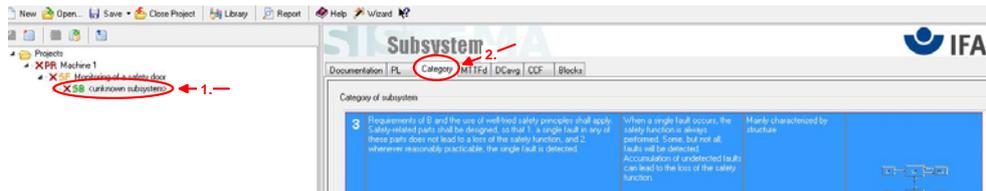


Figure 13

b) Enter the $MTTF_d$ value directly in the subsystem (1.) under "MTTF_d" (2.), or select "Determine $MTTF_d$ -value from blocks" (3.) (Figure 14).

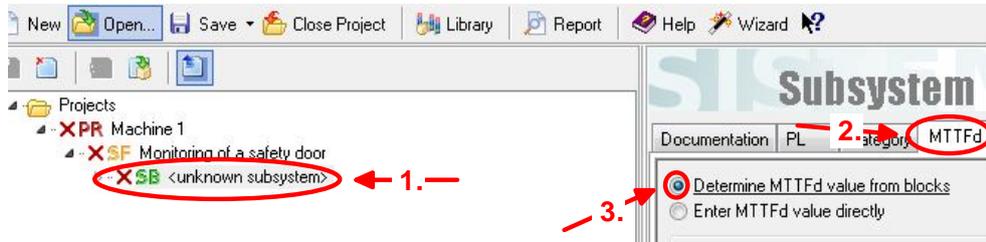


Figure 14

c) Enter the DC_{avg} value directly in the subsystem (1.) under "DC_{avg}" (2.), or select "Determine DC_{avg} -value from blocks" (3.) (Figure 15).

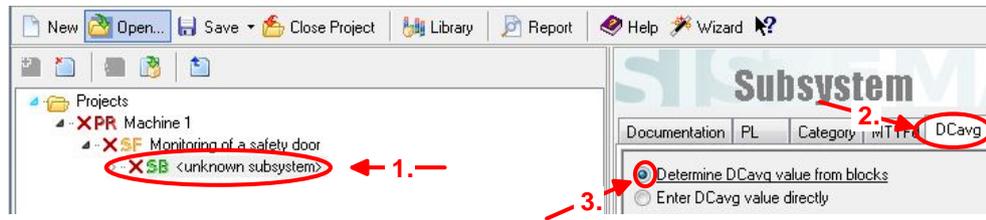


Figure 15

d) For each two-channel subsystem, faults must be considered which would cause both channels to fail for the same reason (CCF). Of these, Category 2 (functional channel and test channel) and Categories 3 and 4 (two functional channels in each case) are affected. Entry is made in the subsystem (1.) under "CCF" (2.) by selection of the measures to be taken (Figure 16). At least 65 points must be reached. The number of points reached can be entered directly or compiled by a library of measures (3. and 4.).

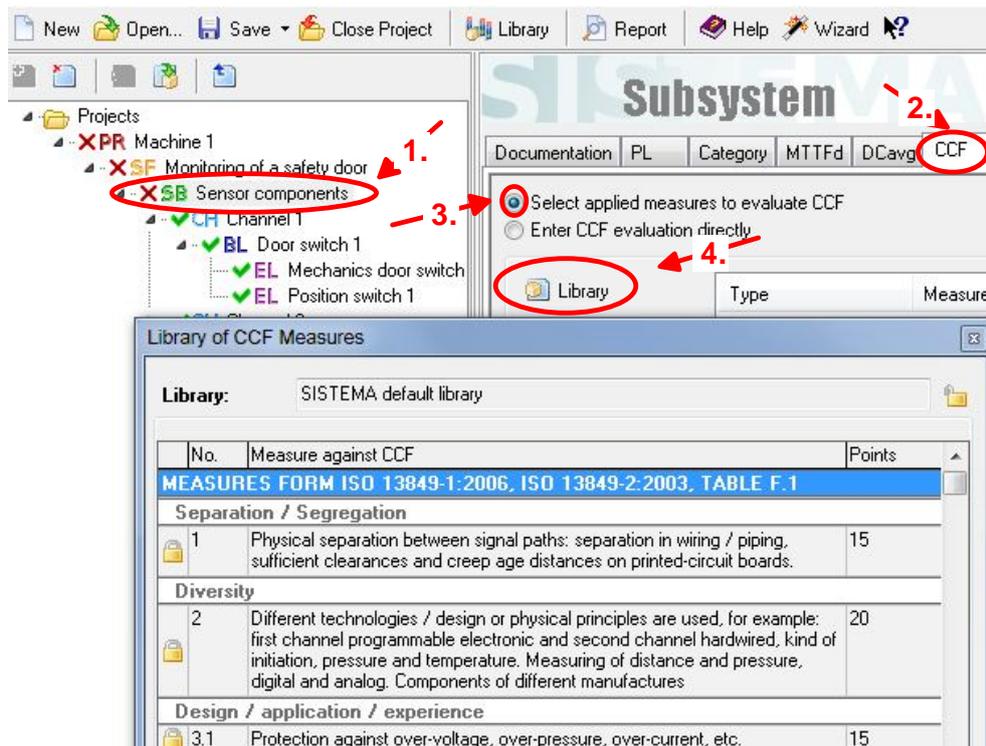


Figure 16

4.6.1 Entering blocks

Once the subsystems have been formed, further specification is necessary (exception: 4.5 Encapsulated subsystems). When the Category of a subsystem is selected, SISTEMA creates the relevant channels (**CH**). Under "Channel", the blocks (**BL**) are added corresponding to the individual components of a channel. If no further subdivision of the blocks is required, the procedure can continue with 4.6.3. If a block is to be further subdivided into elements (always necessary with components for which the B_{10d} is stated), the following settings are required:

- a) In block (1.) under "MTTF_d" (2.), select "Determine MTTF_d-value from elements" (3.) (Figure 17).

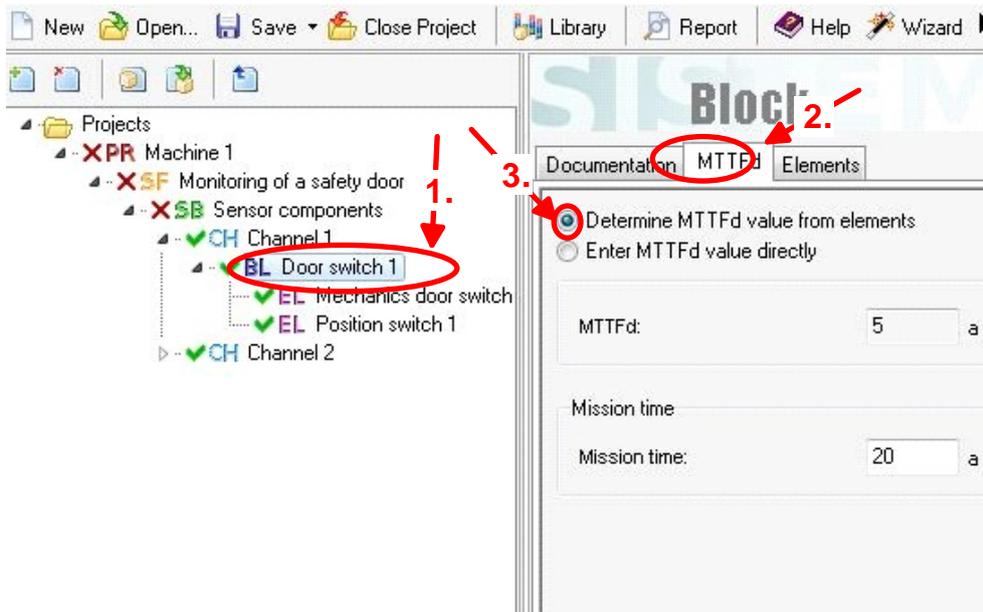


Figure 17

- b) In block (1.) under "DC" (2.), select "Determine DC-value from elements" (3.) (Figure 18).

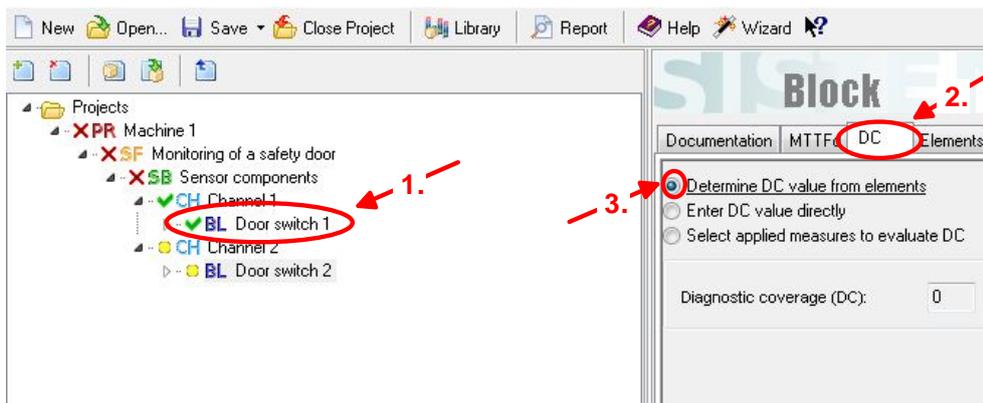


Figure 18

4.6.2 Entering elements

If a block is to be divided into elements (**EL**), create elements in the block (1.) under "Elements" (2.) with "New" (3.) (Figure 19).

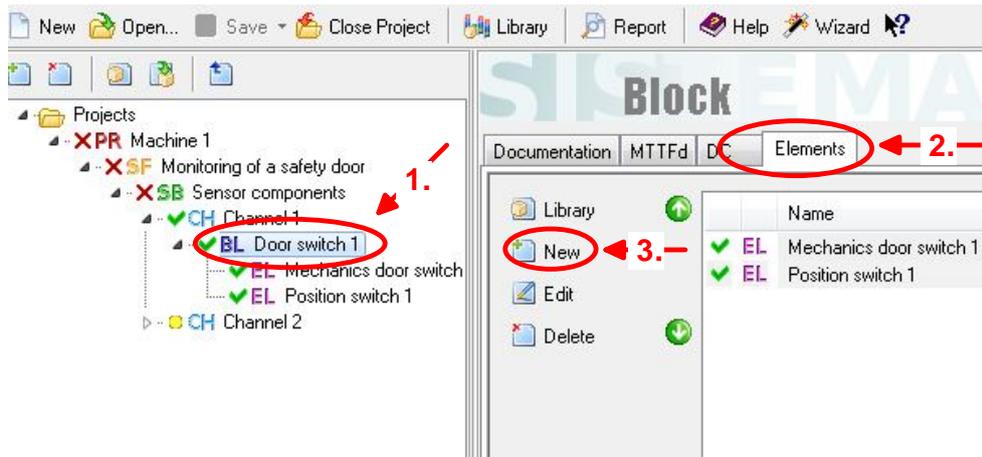


Figure 19

At element level (1.), calculation is necessary with consideration for the B_{10d} value and the number of operations n_{op} , for example in order to determine the $MTTF_d$ (2.) of electromechanical and pneumatic components (Figure 20). Select "Determine $MTTF_d$ -value from B_{10d} -Value" (3.) and "Calculate n_{op} " (4.) in order to enter the required values (5.).

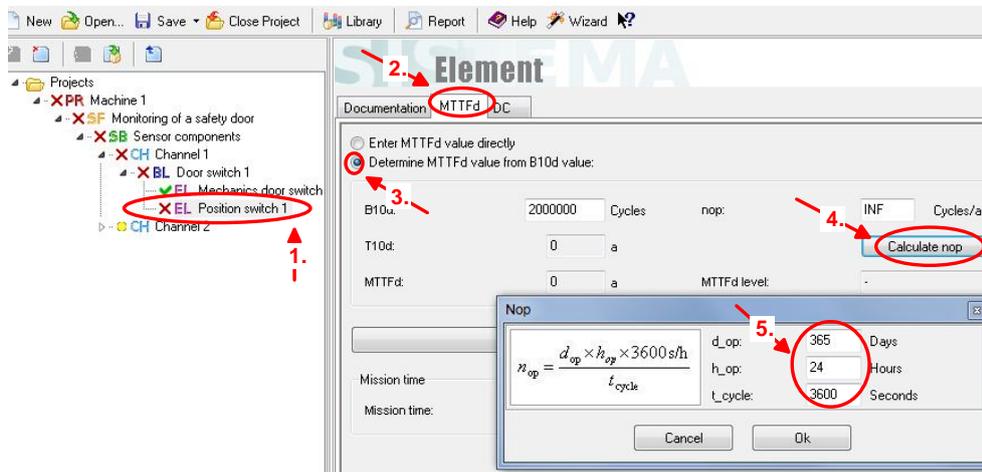


Figure 20

4.6.3 Entering safety-related data

The safety-related data required for calculation of the PFH include the applicable component quality ($MTTF_d$, B_{10d}), the number of operations of electromechanical and pneumatic components (n_{op}) and the diagnostic coverage (DC).

4.6.3.1 $MTTF_d/B_{10d}$

Enter at block or element level (1.) on the " $MTTF_d$ " tab (2.) (Figure 21).

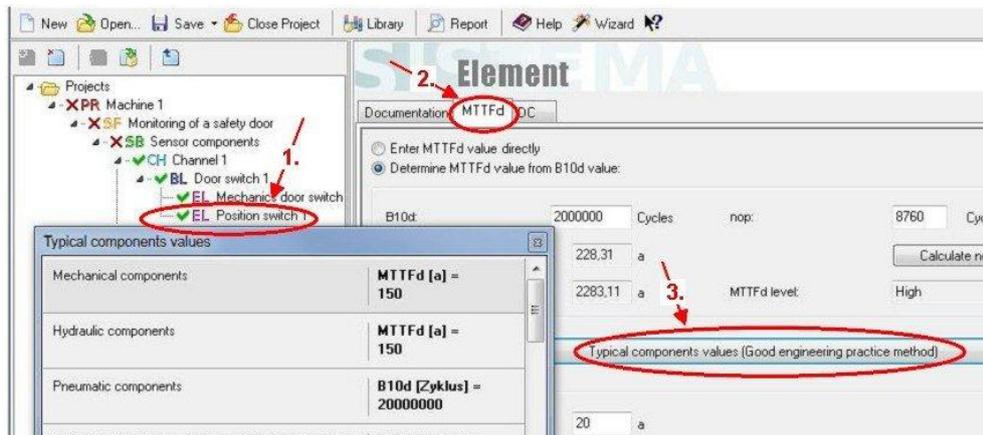


Figure 21

The safety-related parameters of the components can be determined from any of the following:

- a) Manufacturers' data
- b) Established collections of data (for sources, see EN ISO 13849-1, Annex D)
- c) EN ISO 13849-1, Annex C; stored in SISTEMA under "Typical component values" (3).

If all dangerous component faults can be excluded, a fault exclusion can also be selected when "Enter MTTF_d-value directly" is selected.

4.6.3.2 DC

For Category 2 and higher, fault-detection measures for the components are required. In the block or element (1.), a percentage is entered on the "DC" tab (2.) for each component to describe the diagnostic coverage of fault detection. Selection of "DC-rating by choosing measures" enables the DC tables in EN ISO 13849-1, Annex E to be accessed via "Library" (3.). The values can be accepted as-is or used for guidance. Where the standard proposes a band of possible DC values, a concrete value within this band can be selected (Figure 22).

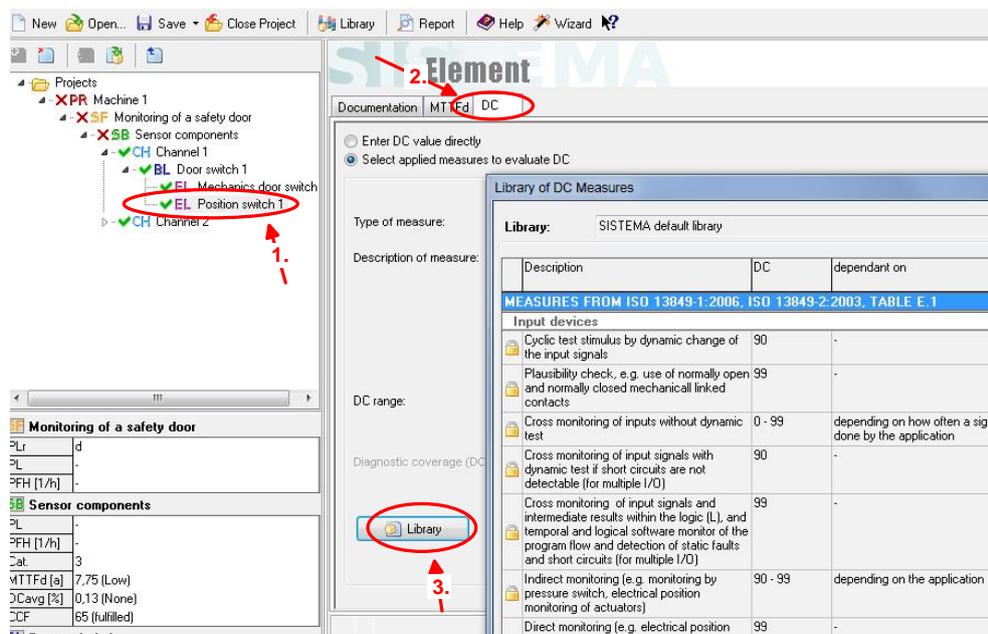


Figure 22

4.7 Objective attained?

Check for error messages (red cross) in the message window (centre, below). If none are present, the PFH can be calculated (Figure 23).

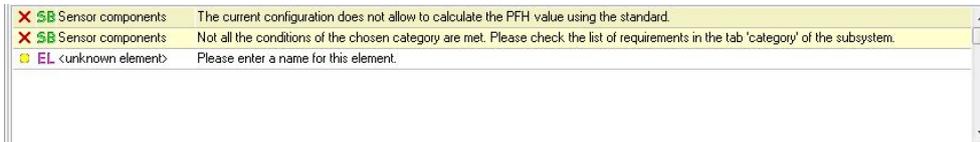


Figure 23

The result of the calculation is indicated at the bottom left for the selected safety function and the corresponding subsystems, blocks and elements (Figure 24). The (attained) PL of the safety function must at least equal the (required) PL_r. If the attained PL is insufficient, components with a higher MTTF_d or a higher B_{10d} value must be employed, the fault detection (DC) must be improved, or subsystems of other Categories must be implemented.

| | |
|------------------------------------|---------------------|
| Monitoring of a safety door | |
| PL _r | d |
| PL | d |
| PFH [1/h] | 3,56E-7 |
| Sensor components | |
| PL | d |
| PFH [1/h] | 3,56E-7 |
| Cat. | 3 |
| MTTF _d [a] | 9,96 (Low) |
| DC _{avg} [%] | 99 (High) |
| CCF | 65 (fulfilled) |
| Door switch 1 | |
| MTTF _d [a] | 9,96 (Low) |
| DC [%] | <i>not relevant</i> |
| Position switch 1 | |
| MTTF _d [a] | 2283,11 (High) |
| DC [a] | <i>not relevant</i> |

Figure 24

Annex A: Concepts and abbreviations

Definition of key concepts referred to in a similar way in Annex B of EN ISO 13849-1:

| Concepts | Definition |
|---|---|
| Safety function (SF) | Safety-oriented response to a triggering event (demand upon the safety function). In redundant systems, the safety function is executed in multiple and independent ways. The PL describes the reliability of its execution. |
| Schematic circuit diagram | Excerpt from the wiring diagram or function circuit diagram which indicates the technical (hardware) interconnections between the safety-related parts of the control system. |
| Safety-related block diagram | Presentation of the logical connections between the components from which the functional and test channels can be seen. |
| Components | Safety-related hardware units, parts of the control system |
| Subsystem (SB) | Largest unit of components which executes the safety function fully or in sections. A subsystem possesses a continuous structure and is described by a Category. |
| Encapsulated subsystem | Safety component for which the manufacturer already states the PL, PFH and Category. The internal structure need not therefore be considered more closely. |
| Functional channel | Hardware units connected in series; chains of components which execute the entire safety function from the sensor to the actuator. Redundant subsystems possess (at least) two independent functional channels. |
| Function signal | Signal that passes the demand for the safety function on along a functional channel from the sensor to the actuator, where for example it leads to disconnection. |
| Redundant function block | Hardware unit connected in parallel; component in a section of a redundant functional channel; part of a functional channel in Category 3 or 4 subsystems. |
| Non-redundant function block | Component in a section of a non-redundant functional channel; part of a functional channel in Category B, 1 or 2 subsystems. |
| Test channel | Chain of components which transmits a "Testing" disconnection signal (not to be confused with the signal path over which test signals are exchanged between the testing and tested blocks for the detection of a dangerous failure). |
| Testing disconnection signal | Transmits the result of a test which has detected a dangerous failure of a function block, from a test block to a function block further on or to an additional disconnecting block, with the result that the safety function is successfully completed or a safe state is brought about. |
| Test block | Hardware unit for diagnostics: Component that tests one or more function blocks and generates a "Testing" disconnection signal when it detects a dangerous failure in them; or a transmitting or disabling block in the test channel |
| Closed-circuit current principle | Interruption of a circuit leads to the safe state. |

Annex B: Abbreviations from EN ISO 13849-1

| Abbreviation | Unit | Name | Comment |
|-------------------|----------|---|--|
| SRP/CS | - | S afety-Related P art of a Control S ystem | |
| MTTF _d | Year, a | M ean T ime T o d angerous F ailure | Component quality |
| DC | % | D iagnostic C overage | Test quality (block, element) |
| DC _{avg} | % | A verage D iagnostic C overage | Test quality (subsystem) |
| CCF | - | C ommon C ause F ailure | Simultaneous failure of redundant channels |
| PFH | 1/h | P robability of a dangerous F ailure per H our | Probability of failure |
| PL | - | P erformance L evel | Actual value of the functional safety |
| PL _r | - | R equired P erformance L evel | Specified value of the functional safety |
| Cat. | - | C ategory | |
| T _M | Year, a | M ission T ime | Service life |
| B _{10d} | Cycles | Number of cycles until 10% of the components fail d angerously | Component quality (wearing component) |
| T _{10d} | Year, a | M ean T ime until 10% of the components fail d angerously | Permissible operating time (wearing component) |
| n _{op} | Cycles/a | n umber of o perations (average, per year) | Operating frequency |

Annex C: Model form for user's applications

Definition of the safety function:

Triggering event:

Response:

Safe state:

Schematic circuit diagram with entries for functional and test channels:
In the annex

Safety-related block diagram of the first functional channel, where applicable with the addition of components in the second functional channel or in the test channel:

Final safety-related block diagram, where applicable following the grouping of subsystems of the same Category:

Annex D: Schematic table

The schematic table is an alternative method of structure analysis in accordance with Figure 5. All components shown on the schematic circuit diagram are entered in a table in accordance with the method described in Section 3. Table 4 shows the possible combinations and the resulting structure (possible Category) and presentation in the safety-related block diagram; Table 5 has been completed for the example in Section 3, and Table 6 provides an empty form for the user's examples.

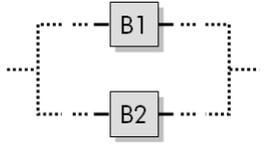
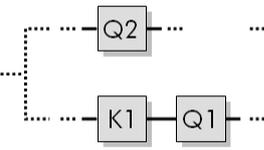
Table 4: Formalized schematic table for structure analysis in accordance with Section 3 (the steps stated in Section 3 are entered in red)

| Components in the first functional channel | (1) X1 (2) | X2(2a) | X3 (2a) | X4 (2a) |
|--|----------------------------------|------------|----------------|----------------|
| Is the Category stated by the component manufacturer (3)? | Yes | | | |
| Redundant component(s) (4) | | | X5 (, X6) (4a) | |
| Component(s) in the test channel (fault detection and disconnection) (5) | | | | X7 (, X8) (5a) |
| Possible Category | B to 4 Encapsulated subsystem | B or 1 (6) | 3 or 4 (4b) | 2 |
| Block presentation | | | | |

It can be helpful during the structure analysis to imagine Steps 3, 4 and 5 as follows: what happens when the component is hit with a "test hammer", i.e. a component fault is induced?

- (3) Does the internal structure maintain the (safety) function?
- (4) Is the SF retained owing to redundant design of the SF involving other components?
- (5) Is the component fault detected in time and a safe state brought about?

Table 5: Table completed for the example in Section 3

| | | |
|--|--|---|
| Components in the first functional channel | B1 | Q2 |
| Is the Category stated by the component manufacturer? | | |
| Redundant component(s) | B2 | K1, Q1 |
| Component(s) in the test channel (fault detection and disconnection) | | |
| Possible Category | 3 or 4 | 3 or 4 |
| Block presentation |  |  |

Block diagram (summary): (8)

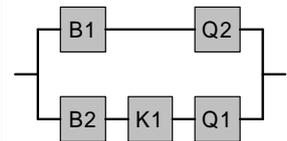


Table 6: Form for user's examples

| | | | | | | | | |
|--|--|--|--|--|--|--|--|--|
| Components in the first functional channel | | | | | | | | |
| Is the Category stated by the component manufacturer (3)? | | | | | | | | |
| Redundant component(s) (4) | | | | | | | | |
| Component(s) in the test channel (fault detection and disconnection) (5) | | | | | | | | |
| Possible Category | | | | | | | | |
| Block presentation | | | | | | | | |

Annex E: Flow chart for structure analysis (without example)

