IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

The SISTEMA Cookbook 4

When the designated architectures don't match

Version 2.0 (EN)

Authors: Michael Hauke, Ralf Apfeld, Michael Huelke, Thomas Bömer, Christian Werner
Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA)
Alte Heerstraße 111
53757 Sankt Augustin, Germany
Tel.: +49 30 13001-0
Fax: +49 30 13001-38001
Internet: www.dguv.de/ifa

Published by: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV)
Mittelstraße 51
10117 Berlin

– March 2020 –

Contents

Contents 3

Introduction 5

1 Single-fault tolerance in single-channel structures 6

1.1 Description 6

1.2 Input in SISTEMA 6

1.3 Remarks 7

2 Encapsulated subsystem with parallel functional channel 8

2.1 Description 8

2.2 Input in SISTEMA 8

2.3 Tip 9

2.4 Remarks 9

3 More than two functional channels 11

3.1 Description 11

3.2 Input in SISTEMA 11

3.3 First step 12

3.4 Second step 13

3.5 Tip 14

3.6 Remarks 14

4 Test rate in Category 2 16

4.1 Description 16

4.2 Case 1: Demand rate to test rate higher than 1/100 17

4.3 Remarks for case 1 17

4.4 Case 2: Fault detection triggered by the demand upon the safety function 18

4.5 Remarks for case 2 18

5 Mission time higher than 20 years 19

Introduction

To determine the probability of a dangerous failure per hour in accordance with the simplified method described in EN ISO 13849 the control system that is implemented must correspond to one of the designated architectures for the Categories. If this is not the case, the simplified method cannot be used and a more involved method, such as Markov modelling, is generally required. On occasions however, a minor – conceptual – change is sufficient to enable the architecture to be modelled to a designated architecture. Examples of such cases are described below, see Figure 1. A SISTEMA file with associated model projects can be found on the website of the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA) in the download area at http://www.dguv.de/ifa/13849e, together with the SISTEMA cookbooks.

The present, second edition of SISTEMA Cookbook 4 contains a number of updates with respect to the first edition, which was published in 2012:

- Amendments have been made to Chapter 1: the current version of ISO 13849-1 does not make provision for emergency stop devices to be modelled with fault exclusion at subsystem level.
- Amendments to Chapter 2 are limited to editorial changes.
- Certain details have been revised in Chapter 3.
- Chapter 4 has been updated, since in accordance with the third edition of ISO 13849-1, published in 2016, the ratio of the demand rate of the safety function to the test rate may now exceed 1/100; it must however be at least 1/25.
- The section entitled "Mission time higher than 20 years" has been added to Chapter 5.

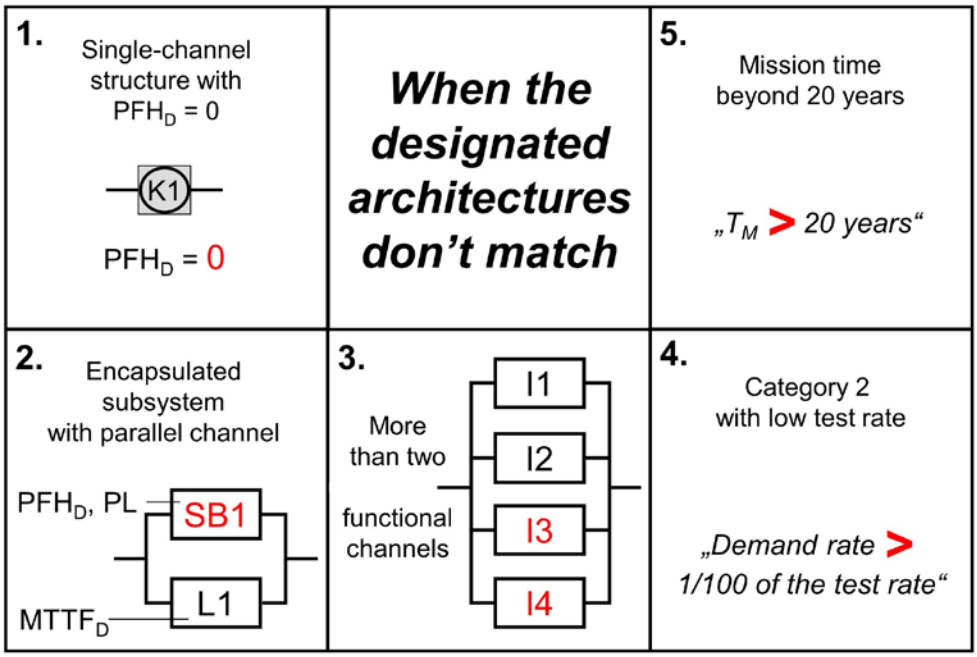

Figure 1:
Five special cases which deviate from the designated architectures (Categories) of the standard but which can nevertheless be analysed by SISTEMA

1 Single-fault tolerance in single-channel structures

1.1 Description

In certain cases, a single-channel subsystem may possess single-fault tolerance. One such case is when either **all** random component faults of a subsystem result in safe failure, or fault exclusions may be assumed. A PFH_D value of zero for a subsystem is justified only in exceptional cases, where permitted by specific applications. This assumption applies for example to position switches with personnel safety function for the monitoring of interlocking guards on printing and paper processing machines not requiring regular operational access to danger points and with a maximum PL_r of d (see EN 1010-1:2004+A1:2010, Section 5.2.11.2). The position switches must also be designed in accordance with EN 60947-5-1:1997 and fitted in accordance with EN 60204-1:2006. In this case, neither statement of a DC[1] nor analysis of the CCF[2] is necessary.

The first edition of this SISTEMA Cookbook, which was based upon ISO 13849-1:2008 (second edition of the standard), referred to emergency stop devices as an example of this special case. Emergency stop devices are however treated differently in the current, 2016 version of the standard, as a result of which fault exclusion for the emergency stop device subsystem is no longer recommended. Annex D.2.5.4 of IFA Report 2/2017e on the current version of the standard contains comprehensive information on the modelling of emergency stop devices and other electromechanical components.

Bus systems for the transmission of safety-related information may also be physically of single-channel design and nevertheless transmit data with single-fault tolerance. Section 6.2.18 of IFA Report 2/2017e also provides further information on this aspect.

1.2 Input in SISTEMA

Figure 2 illustrates the input in SISTEMA. Input is in the form of a subsystem in which the PL[3] and PFH_D[4] values are entered directly on the "PL" tab (1., 2.). The PFH_D value is "0" (3.). The input on the "Category" tab is for information only and is documented but not interpreted by SISTEMA.

[1] DC = Diagnostic Coverage

[2] CCF = Common Cause Failure

[3] PL = Performance Level

[4] PFH_D = Probability of a dangerous Failure per Hour

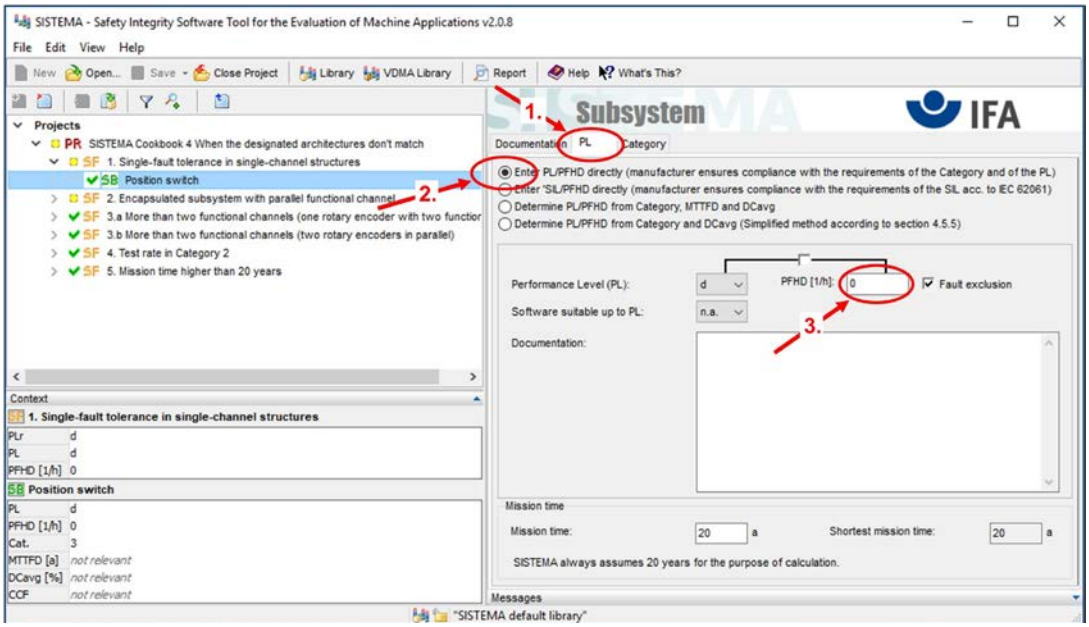

Figure 2:
Position switch with personnel safety function according to section 5.2.11.2 of EN 1010-1+A1:2010 with fault exclusion and PFH_D = 0 as a subsystem with fault exclusion and PFH_D = 0 in SISTEMA

1.3 Remarks

For internal processing reasons, if a PFH_D value of “0” is entered, SISTEMA ticks fault exclusion in this case. If the subsystem with fault exclusion is the only subsystem below the safety function, SISTEMA indicates with a yellow warning message that the safety function is implemented complete with fault exclusions. **For PL_r e, fault exclusion at subsystem level is not generally permissible.** The warning messages are intended to prompt careful review of the validity of the inputs made at this point. More information on fault exclusions can be found in EN ISO 13849-1:2015, Section 7.3 and in EN ISO 13849-2.

2 Encapsulated subsystem with parallel functional channel

2.1 Description

If encapsulated subsystems are employed in one channel of a two-channel structure[5], "only" the PFH_D and PL (or SIL[6]) are available, and not the $MTTF_D$[7] required for analysis of the two-channel system. In order for this subsystem still to be analysed, the corresponding $MTTF_D$ for one channel must instead be determined from the PFH_D and PL values stated by the manufacturer. The question is therefore how the encapsulated subsystem L1 with known PFH_D can be modelled approximately to a Block L1 with $MTTF_{D1}$ and DC_1.

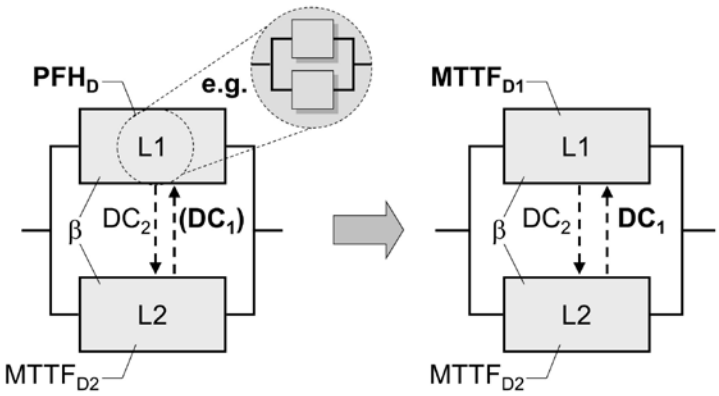

Figure 3:
Modelling of an encapsulated subsystem L1 to a block

Several dependencies, which make it difficult to formulate a simple recipe, are relevant to modelling. The approach presented below is not always successful, particularly if Category 4 is to be attained. The only remaining option is then a detailed analysis, for example involving a Markov model deviating from the standard structures.

2.2 Input in SISTEMA

If no information is available on the effective detection of faults in L1, the following applies by approximation:

$$MTTF_{D1} = \frac{1}{PFH_D} \quad \text{and} \quad DC_1 = 0\%$$

Only if faults in the encapsulated subsystem L1 are detected from outside, for example by L2, can a correspondingly higher value be applied for DC_1. In this case:

[5] Use of an encapsulated subsystem in Category 2, 3 or 4 in a single channel only is in fact not cost-effective. Such circuits are however encountered in practice.

[6] SIL = Safety Integrity Level

[7] $MTTF_D$ = Mean Time To dangerous Failure

$$DC_1 = \frac{\text{Failure rate of dangerous faults in L1 } \mathbf{\text{detected externally which cannot be detected by internal diagnostics measures in L1}}{\text{Failure rate of all dangerous faults in L1 } \mathbf{\text{which cannot be detected by internal diagnostics measures in L1}}}$$

Figure 4 shows application of the approach in SISTEMA. The subsystem shown consists of a safety module in the form of an encapsulated subsystem (with PL d and $PFH_D = 3.0 \cdot 10^{-7}$/h when the maximum number of switching cycles specified by the manufacturer is observed) in the first channel, and parallel to it a contactor with mirror contacts in the second channel.

Chapter 3 shows application with $DC_1 > 0$ with reference to a further example.

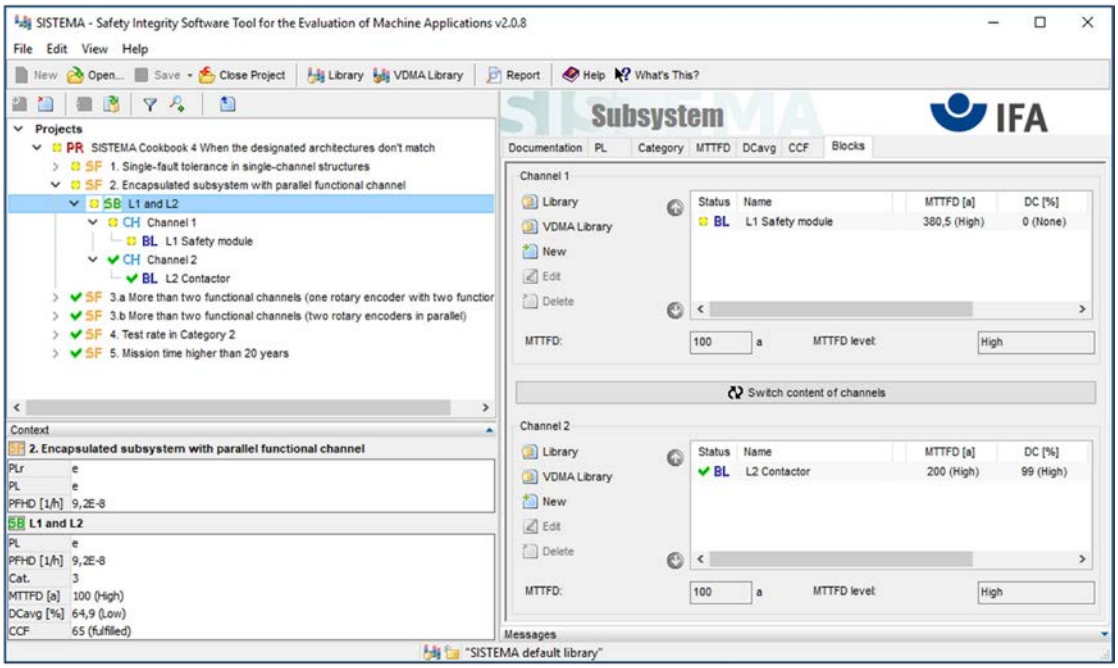

Figure 4:
SISTEMA screenshot of a subsystem addressed by the approach described above

2.3 Tip

The reciprocal is formed automatically by SISTEMA when the PFH_D value is entered in the "Dangerous failure rate" field on the $MTTF_D$ tab. For example, $PFH_D = 3.0 \cdot 10^{-7}$/h corresponds to an input of 300 FIT (1 FIT = $1.0 \cdot 10^{-9}$/h) and an $MTTF_D$ value of 380.5 years.

2.4 Remarks

When the $MTTF_D$ is calculated as the reciprocal of the PFH_D, attention must be paid to **correct conversion of the units** (1 year = 8760 hours).

A **correct "two-channel" circuit arrangement** for L1 is a requirement in this case, as is satisfaction of all boundary conditions specified for L1 for the PFH_D stated, for example with regard to fault detection.

This method applies both when the encapsulated subsystem as shown in Figure 3 forms a channel on its own, and when **further blocks** are present with it in this channel. This procedure can also be applied when (identical or different) encapsulated subsystems are employed **in both channels** of a two-channel structure. Refer also to Chapter 3 in this context.

All internal measures which reduce the probability of failure of L1, such as multichannel structure and fault detection, are taken into account in the $MTTF_{D1}$ via the PFH_D. No further use may therefore be made of the internal diagnostics measures within L1, since they have already been "used up" for determination of the PFH_D. Under these circumstances, $DC_1 = 0$ must first be assumed. This results in SISTEMA displaying the warning: "Please check whether for the required PL a component with a DC of 0% is in accordance with the requirements of the category 3 in terms of failure detection." For encapsulated category 2, 3 or 4 subsystems, this warning can be ignored, since these subsystems possess internal fault-detection measures.

If Category 4 is desired for the entire subsystem containing L1 and L2, the condition DC_{avg} of at least 99% (with tolerance[8], 94% is sufficient) may result in failure of this approach unless a satisfactory DC can be attained by means of external testing.

[8] With use of the 5% tolerance in accordance with Table 6 of the standard

3 More than two functional channels

3.1 Description

Since the simplified method described in EN ISO 13849-1 (and therefore also applicable in SISTEMA) can be used only for analysis of single-channel and two-channel structures, the number of channels present must be reduced to two. The simplest way of achieving this is simply to ignore surplus channels (ideally those with lower reliability) during the analysis. This solution is effective however only if the PFH_D calculated in this way is adequate. Alternatively, two channels can first be grouped in an interim step and presented as a single block in a channel (refer also to Chapter 2). Figure 5 summarizes this procedure.

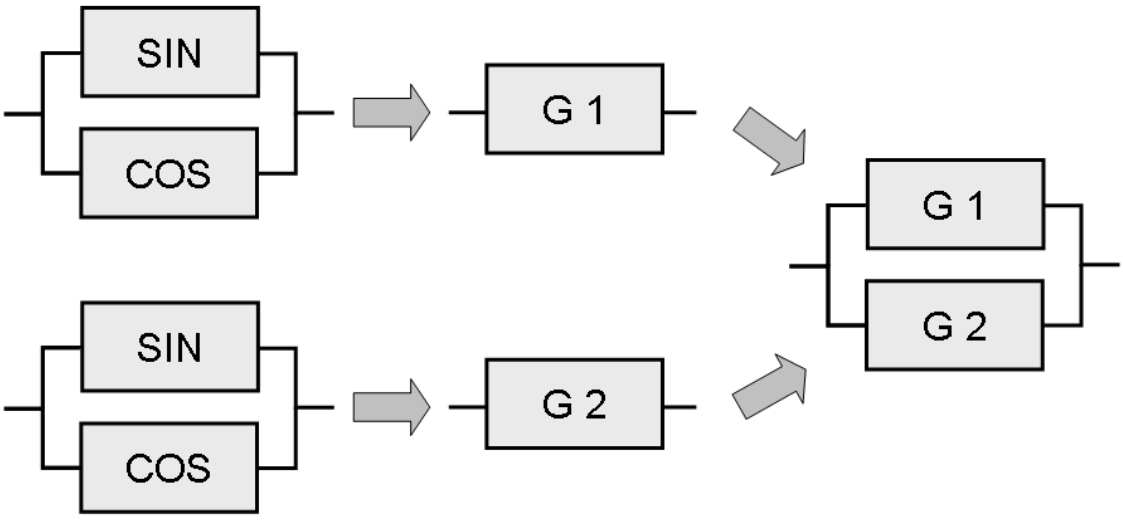

Figure 5:
Method for modelling a four-channel encoder system to a two-channel structure

In this example, it is assumed that the safety function evaluates only the speed value, such as the "safely limited speed" function (SLS to EN 61800-5-2).

3.2 Input in SISTEMA

The step-by-step grouping method is illustrated by an example with a four-channel structure, as shown in Figure 6:

Two identical rotary encoders G1 and G2 measure the speed on the same shaft and supply the corresponding sine and cosine output signals[9]. The two output signals are assumed to be independent of each other and thus to constitute separate channels (see Section 3.6). The use of multiple redundancy in this case serves to reduce the contribution of the encoders' PFH_D to the safety function.

[9] For position-based safety functions and certain other safety functions, a single sin/cos rotary encoder must be treated as a single-channel system, since the information (e.g. "direction of rotation") can be obtained only from the sine **and** cosine signals in combination..

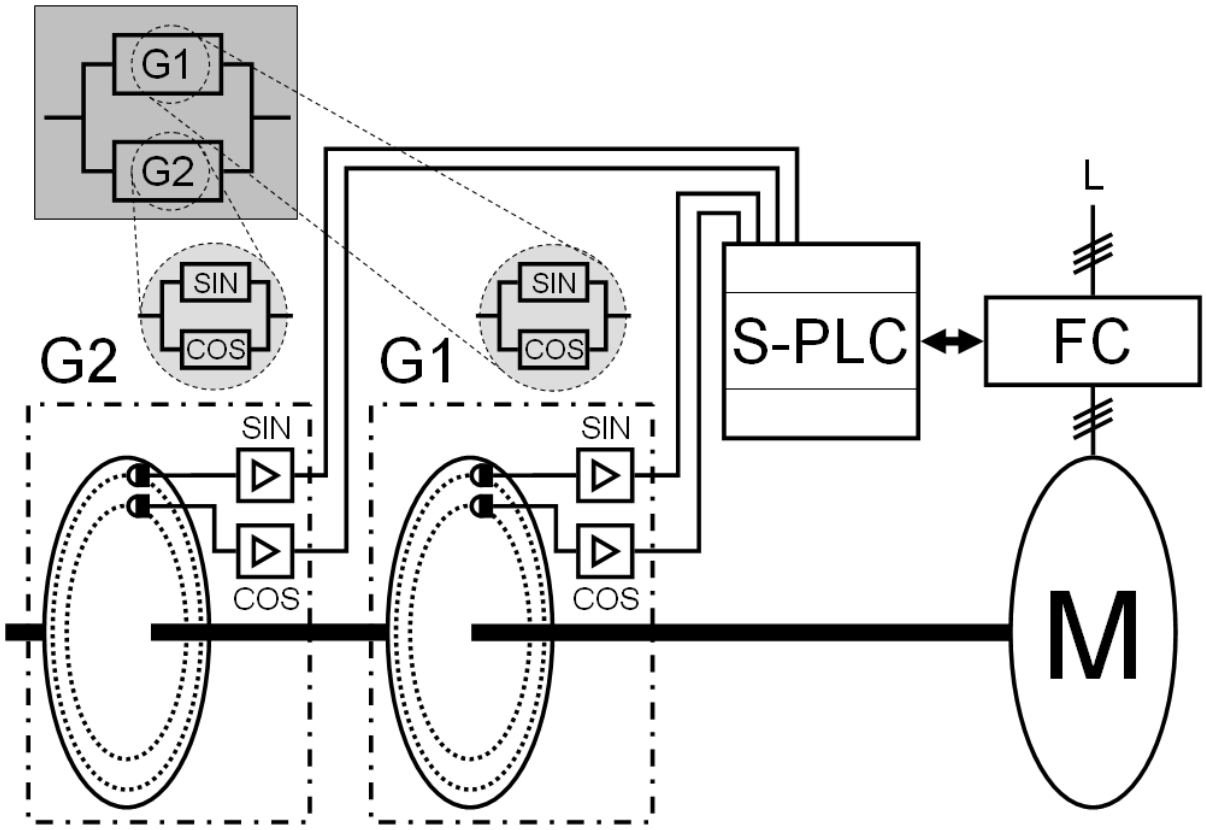

Figure 6:
Example of a four-channel structure for detection of the speed

3.3 First step

In this special example, the hardware for the sine and cosine signal from each encoder would be modelled as a functional channel in its own right. This is possible on encoders on which no component faults are able to occur which falsify the sine and cosine signals in a mutually complementary manner ($\sin^2\alpha + \cos^2\alpha = 1$, see Section 3.6). In order for all four channels to be considered, each of the two encoders G1 and G2 is first modelled separately as a two-channel subsystem. The PFH_D of an encoder is calculated in the usual way in that the hardware of the sine and cosine signals each form a channel of a Category 3 or 4 subsystem. Category 4 and an $MTTF_D$ of 100 years for each channel are assumed in this example. As a DC measure, a separate check can for example be performed by the control system for $\sin^2\alpha + \cos^2\alpha = 1$ for each encoder. 99% DC is employed for this purpose. The PFH_D values determined for each of the two encoders are $2.5 \cdot 10^{-8}$/h and form the result of the first step (see Figure 7).

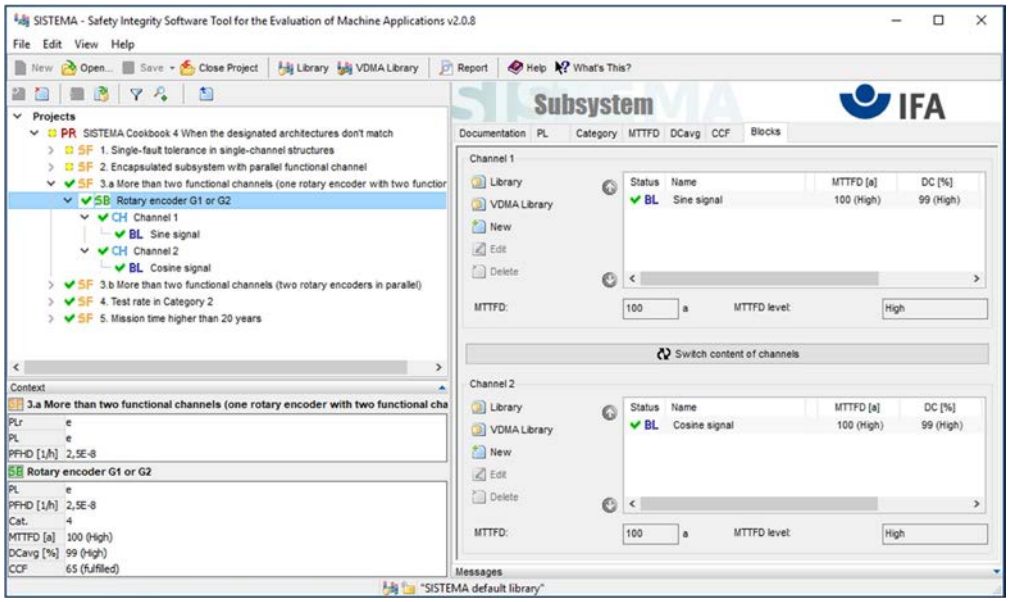

Figure 7:
SISTEMA screenshot of an encoder G1 or G2 forming a two-channel subsystem

3.4 Second step

A new Category 3 or Category 4 two-channel subsystem in which each individual encoder is modelled as a block in a channel can be created for the overall system from two encoders, as described in Chapter 2.

The reciprocal of the PFH_D for an individual encoder is employed as the $MTTF_D$ of the blocks ($MTTF_D = 1/PFH_D$). In this case, the resulting $MTTF_D$ values for each of the two encoders are 4621.7 years, i.e. the reciprocal of $2.5 \cdot 10^{-8}$/h or an input of 24.7 FIT for the dangerous failure rate. In SISTEMA, the expert option of "$MTTF_D$ capping for Category 4 lower from 2500 to 100 years" must also be deactivated.

The DC for the blocks is determined by the evaluation of additional "external" fault-detection measures which detect a dangerous failure of an individual encoder and place the entire system in a safe state. Any existing detection of dangerous failures by the internal DC measures within an individual encoder is not therefore considered in this method (see Section 2.4). The DC requirements of the Category (at least "low" for Category 3 and at least "high" for Category 4) must be satisfied by the "external" DC alone when this method is used. A DC value of 95% was estimated conservatively in this case for comparison of the two encoder signals in a downstream control system (see Section 3.6). This also satisfies the requirements of Category 4 assumed in the example (see Figure 8).

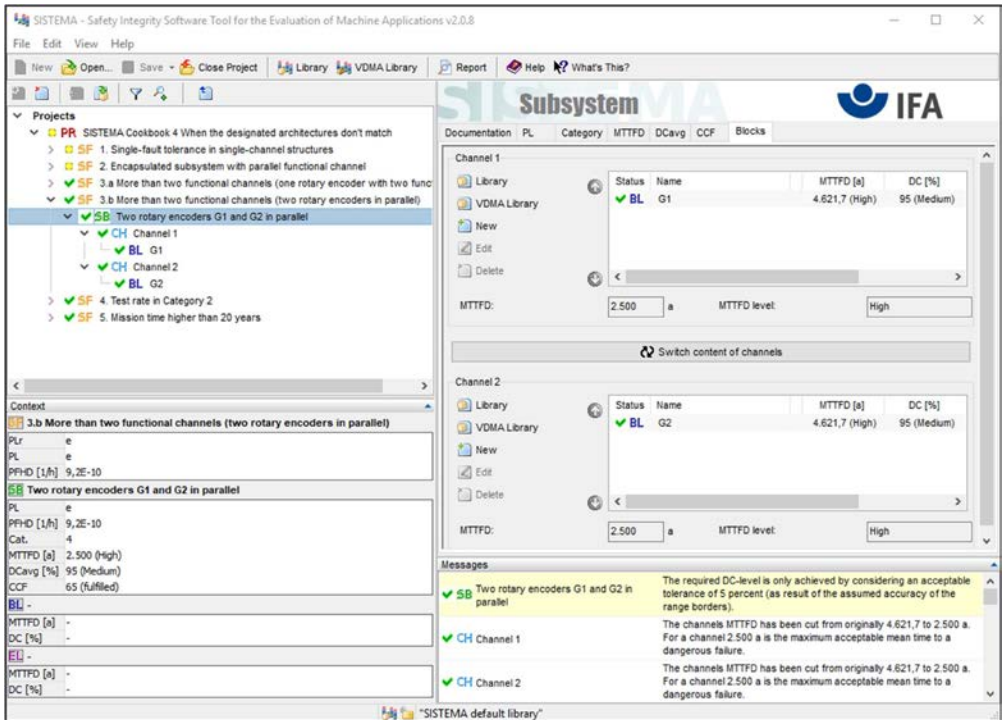

Figure 8:
SISTEMA screenshot of the two encoders G1 and G2 constituting a two-channel subsystem

3.5 Tip

The manufacturer often states a PFH_D for encoders for safety-related applications. Where this is the case, the first step can be skipped and it can be directly started with the second step.

3.6 Remarks

Sine/cosine rotary encoders generally scan a barcode disk optically and generate the desired signal form from it. The form of the signal is determined by the configuration of the optical path in the sensor. The analogue signals are then processed. In principle, the signals from the two channels may to some degree be processed within the same circuit. Single-fault tolerance of the electronics can nevertheless be assured, since a component fault that could lead at the same time to undetectable falsification of sine **and** cosine signals is not conceivable. No components exist for storage of the analogue signals; the output signals cannot therefore be "frozen".

Breakage of the mechanical link between the drive shaft and the encoder shaft cannot be detected by $\sin^2\alpha + \cos^2\alpha = 1$, and therefore contributes to the PFH_D of the individual encoder. If the two encoders are coupled to the drive shaft independently of each other, downstream control logic could however detect such a dangerous failure with a high "external" DC by comparison of the information from the two encoders.

Alternatively, fault exclusion may be assumed for the mechanical coupling of the encoder to the shaft, in which case the coupling is not considered in the safety-related block diagram.

The fault exclusion is performed by the encoder manufacturer, subject to suitable design of the encoder's mechanical components and over-dimensioning. Particular attention must be paid to this fault exclusion in Category 4 systems. For further information, see EN IEC 61800-5-2: 2016, Table D.8.

As is usual in SISTEMA, common-cause faults in the two-channel subsystem comprising two encoders are automatically recorded on a dedicated tab and taken into account during determining of the PFH_D.

4 Test rate in Category 2

4.1 Description

The reliability of a single-channel tested architecture, as provided for by Category 2, depends strongly upon the test rate. If a test is performed too infrequently, the safety it provides is deceptive: as the test interval increases, so does the probability of a dangerous failure of the safety function being followed by a demand upon the safety function before the next test is performed (see Figure 9, above). In a single-channel tested architecture, the test rate thus competes with the frequency of the demand upon the safety function. In the simplified method for estimation of a PL for Category 2, a pre-condition of EN ISO 13849-1 is that the ratio of the test rate to the mean demand rate upon the safety function must exceed 100.

Derogation from this rule is permissible since the third edition of EN ISO 13849-1 published in 2015 in the following two cases:

Case 1 The ratio of the demand rate to the test rate upon the safety function is higher than 1/100 but not exceeding 1/25. Calculation is then possible with use of a PFH_D allowance of 10% (see note 1 in annex K of the standard).

Case 2 Fault detection and fault response are triggered by the demand upon the safety function and are faster than the occurrence of the hazardous situation (see below, Figure 9).

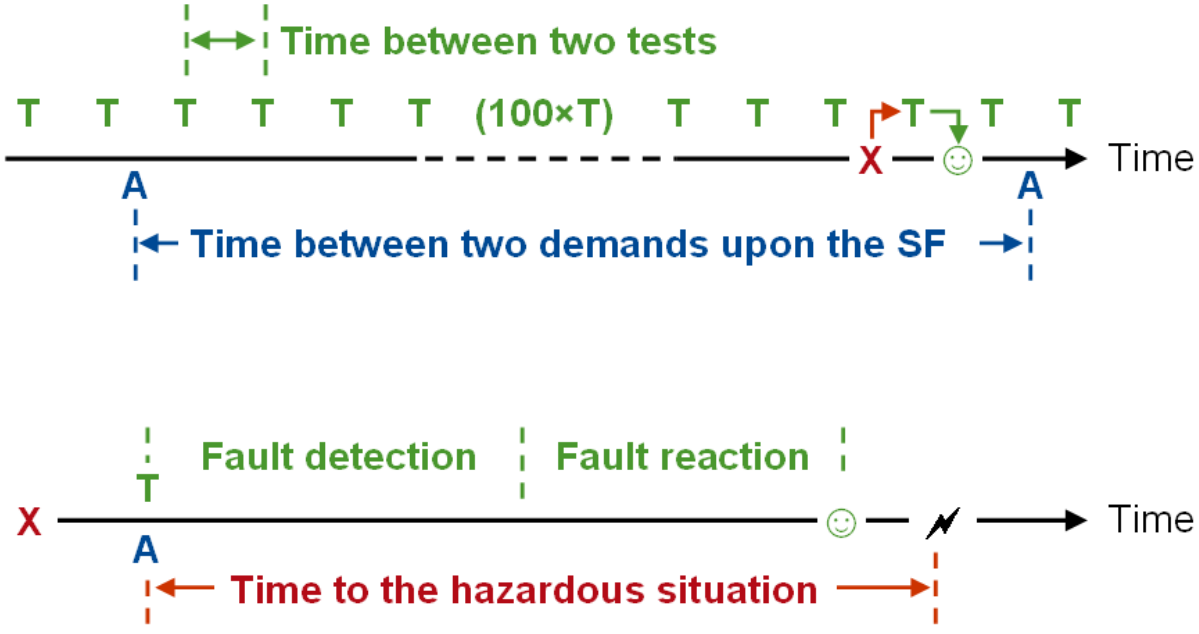

Figure 9:
Two alternative implementations for effective testing in Category 2.
T: points in time of the tests; X: dangerous failure of the functional channel; A: demand upon the safety function; ☺: safe state following fault detection; ↯: incidence of a hazardous situation

4.2 Case 1: Demand rate to test rate higher than 1/100

This section describes the case when the ratio of the demand rate to the test rate upon the safety function is higher than 1/100 but not exceeding 1/25.
For this purpose, Category 2 must be selected on the "Category" tab in the subsystem, and the condition "The requirements for the test frequency are satisfied." be confirmed under "Requirements of the Category". The "Reduced test frequency (1/25)" condition must also be selected. This causes SISTEMA to include the addition of 10% to the PFH_D automatically in the calculation.

Figure 10 shows the example of a Category 2 subsystem with $MTTF_D$ = 100 years, DC = 90%, and a value of 1/25 for the ratio of the demand rate upon the safety function to the test rate. SISTEMA calculates a PFH_D value of $2.5 \cdot 10^{-7}$/h (PL d). Subject to a ratio between the rates being 1/100 the calculated PFH_D value without allowance would be $2.3 \cdot 10^{-7}$/h.

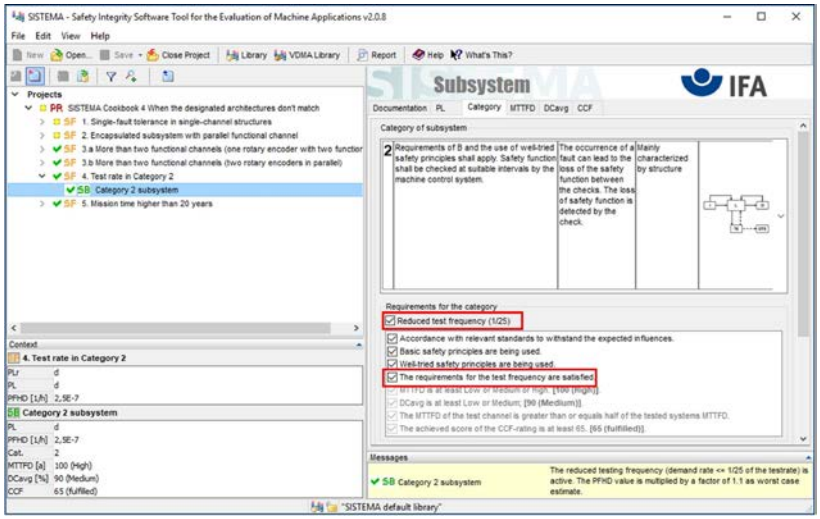

Figure 10:
Example of a Category 2 subsystem with a demand rate/test rate ratio of 1/25

4.3 Remarks for case 1

The increase in the probability of failure as a function of the ratio of the demand rate to the test rate can be determined by Markov modelling. At a ratio not exceeding 1/25, the maximum relative PFH_D allowance applicable under worst-case conditions is approximately 10%. The relative allowance refers to the PFH_D value of the Category 2 subsystem determinable by SISTEMA with an optimum ratio of the demand rate to the test rate of 1/100 or lower.

4.4 Case 2: Fault detection triggered by the demand upon the safety function

This section describes the case when fault detection and fault response are triggered by the demand upon the safety function and both occur more quickly than does the hazardous situation itself.

Under "Requirements of the category" on the "Category" tab of a Category 2 subsystem in SISTEMA, the condition "The requirements for the test frequency are satisfied." can also be marked when the efficacy of the test is assured in this alternative way. The reasoning for this is to be stated in the documentation field for the subsystem, for example: "The requirements for Category 2 upon the test rate are satisfied, since tests and the demand upon the safety function are synchronized such that testing takes place when the demand is made upon the safety function and testing is performed sufficiently fast for the safe state to be reached before a hazard occurs (see SISTEMA Cookbook 4, "When the designated architectures do not fit", Chapter 4)".

4.5 Remarks for case 2

Figure 9 on Page 15 illustrates that a Category 2 structure is also effective when testing occurs simultaneously with the demand upon the safety function and for example with associated signal exchanges. The safe state can be attained however only if fault detection (such as evaluation of the sensor signals in the logic) and the safe fault reaction (such as relaying of the signal from the logic to the actuators and stopping of a hazardous movement) occur more quickly than does the hazardous situation itself. This timeframe is determined for example by adequate safety clearances between safeguard or electro-sensitive protective equipment and the hazardous zone. This alternative by which effective testing can be achieved is stated in section 4.5.4 of EN ISO 13849-1:2015. Suitable model circuits are shown in IFA Report 2/2017e, Sections 8.2.11 and 8.2.12: the failure of a single-channel shut-off valve is detected at the demand upon the safety function, and alternative stopping of the hazardous movement initiated by de-energization of the exhaust valve or of the hydraulic pump. The longer overrun is included in this case in the fault-reaction time. The duration before incidence of the hazardous situation must therefore be correspondingly long.

If a safety function must be executed continually, the test rate cannot be sufficiently high. In this case, implementation of Category 2 is possible only by this alternative method through which fault detection and fault reaction always occur in time before a hazard occurs.

5 Mission time higher than 20 years

5.1 Description

Should the mission time of an SRP/CS exceed 20 years, the PFH_D values determined by means of the simplified method (Annex K of the standard) for Category 2, 3 and 4 are generally no longer valid. Under certain circumstances, this situation can however be addressed within the simplified procedure with a few improvements. There is however no benefit in extending the mission time beyond 30 years. Two possible cases exist.

5.2 Case 1: Mission time is specified from the outset exceeding 20 years

In the first scenario, the SRP/CS is specified from the outset for a mission time exceeding 20 years. The influence of the longer mission time can then be estimated erring on the safe side from the Markov models upon which Annex K of the standard is based, as follows: for every five years' extension of the mission time beyond 20 years, a further 15% is added to the PFH_D for Categories 2, 3 and 4 (Categories B and 1 require no adjustment of the PFH_D). The simplified method and SISTEMA can therefore still be used. This is conditional upon constant failure rates, irrespective of the mission time. For parts subject to wear, this means that the parts must be designed for the specified longer mission time T_M ($T_{10D} \geq T_M$), or each part must be replaced preventively upon expiration of T_{10D}.

5.3 Case 2: Later extension of the mission time

In the second case, the SRP/CS was originally designed for a mission time of 20 years, but is now to be used beyond this duration. The deterioration in the PFH_D anticipated from the Markov modelling can then be estimated as described in the first case with addition of an allowance. The situation is critical where the SRP/CS contains wearing parts or components that deteriorate over age; these typically include “chemical” components (e.g. “wet” electrolytic capacitors, batteries, electrochemical sensors), mechanical components (such as brakes, clutches), electromechanical components (such as switches, relays, contactors), fluid power components (such as valves), and certain optical components (such as optocouplers). In this case, the user of the machine (operating party) is generally unable to assess whether all its components are also designed for an extended mission time, or what measures, such as preventive replacement of individual parts, proof testing, etc., must be performed. Extension of the mission time – with addition of the allowance stated above to the PFH_D – is possible only when manufacturer's information is available on the measures to be taken when the mission time is extended, and only conditional upon these measures being implemented by the user (operating party).

5.4 Input in SISTEMA

A requirement for 15% to be added to the PFH_D for every five years added to the mission time can be implemented in SISTEMA as follows: where a subsystem is to have a mission time exceeding 20 years, its PFH_D value is calculated by SISTEMA in the usual way based upon the category, $MTTF_D$ and DC_{avg}[10]. The mission time is stated here as 20 years. In the same project, a second subsystem is then created the PL/PFH_D value of which is stated directly, as shown in Figure 11. The addition to the PFH_D which is determined manually is entered as the PFH_D value as described above, and 20 years selected once again as the mission time. The link between PFH_D and PL should remain checked. Under the "Category" tab, the same category can be stated as for the original subsystem. Reference to the

increased mission time can be made in the Documentation fields in the PL tab of both subsystems.

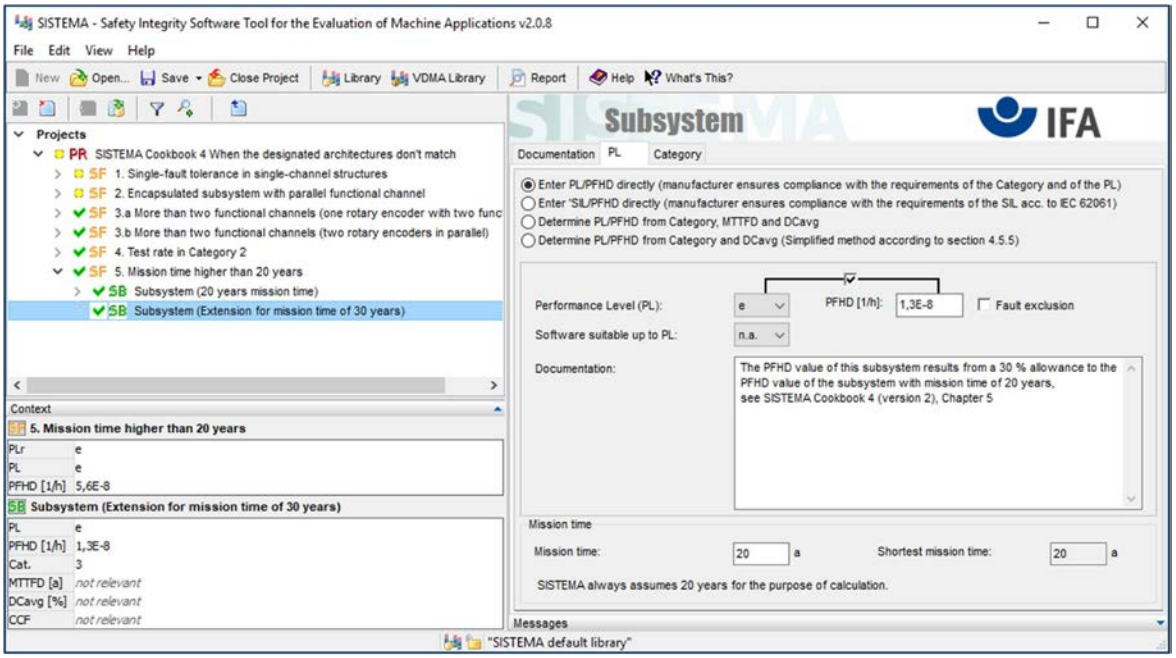

Abbildung 11:
SISTEMA screenshot for a mission time of 30 years