Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung

The SISTEMA Cookbook 4

When the designated architectures don't match

Version 1.0 (EN)

Authors: Michael Hauke, Ralf Apfeld
Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA)
Alte Heerstraße 111
53757 Sankt Augustin, Germany
Tel.: +49 2241 231-02
Fax: +49 2241 231-2234
Internet: www.dguv.de/ifa

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

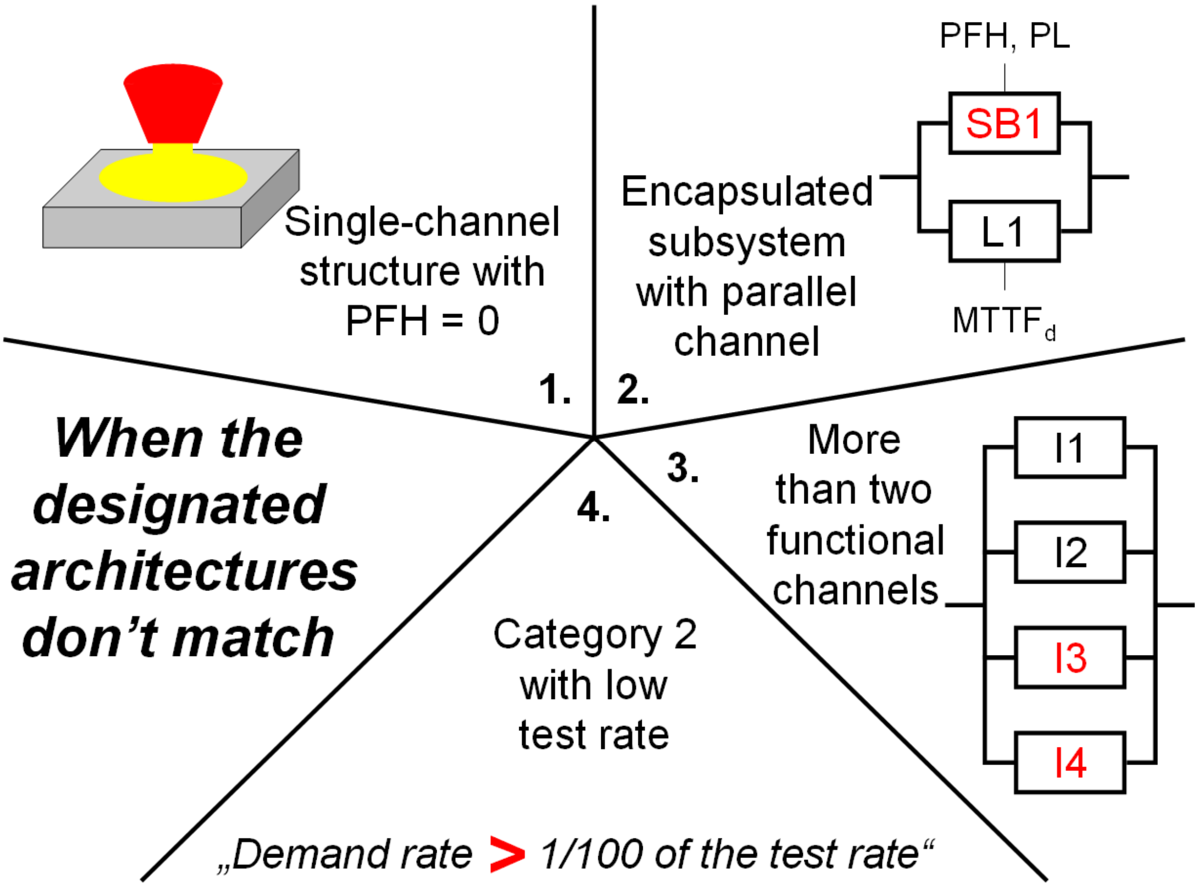
– March 2012 –

Contents

Introduction

A condition for determining of the probability of a dangerous failure per hour in accordance with the simplified method described in EN ISO 13849-1 is that 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 IFA's website in the download area at http://www.dguv.de/ifa/13849e, together with the SISTEMA cookbooks.

Figure 1:
Four 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

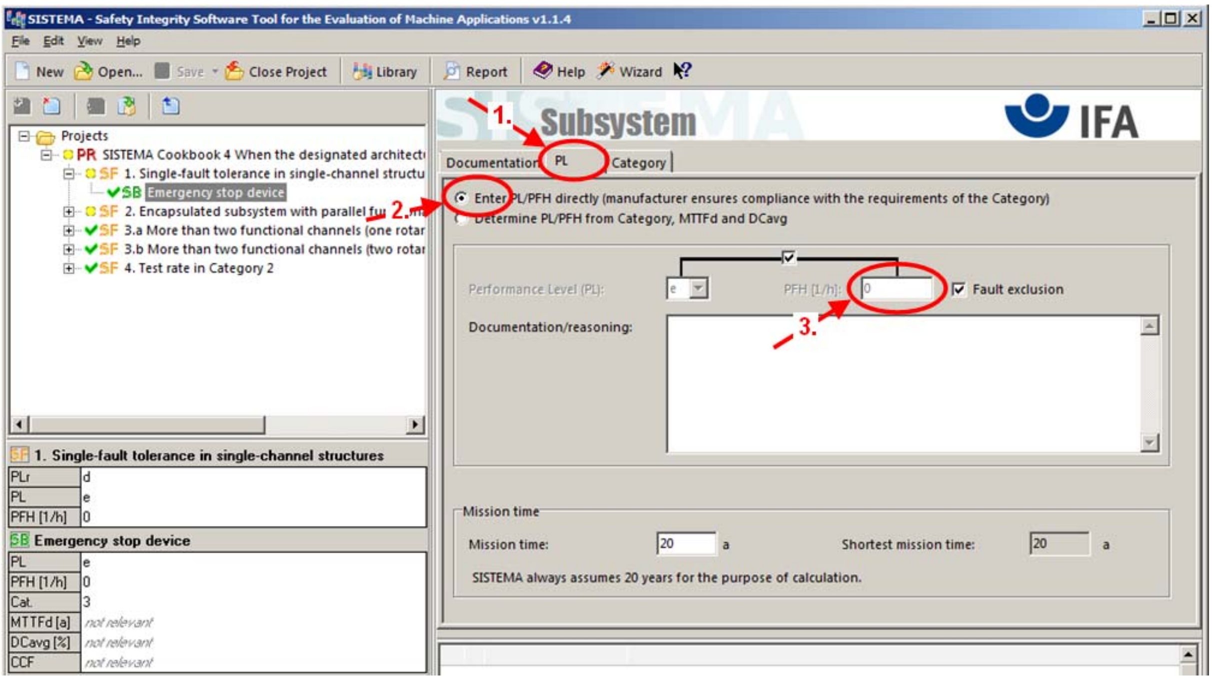
1.1 Description

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. This assumption applies for example to emergency stop devices that are designed in accordance with IEC 60947-5-5 and are not operated too frequently (cf. prEN ISO 13849-2:2010, Table D.8 and BGIA Report 2/2008e, Section D2.5). In this case, neither statement of a DC[1] nor analysis of the CCF[2] is necessary.

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[4] values are entered directly on the "PL" tab (1., 2.). The PFH value is "0" (3.). The input on the "Category" tab is for information only and is documented but not interpreted by SISTEMA.

Figure 2:
Emergency stop device with fault exclusion and PFH = 0 as a subsystem with fault exclusion in SISTEMA



[1] DC = Diagnostic Coverage

[2] CCF = Common Cause Failure

[3] PL = Performance Level

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

1.3 Remarks

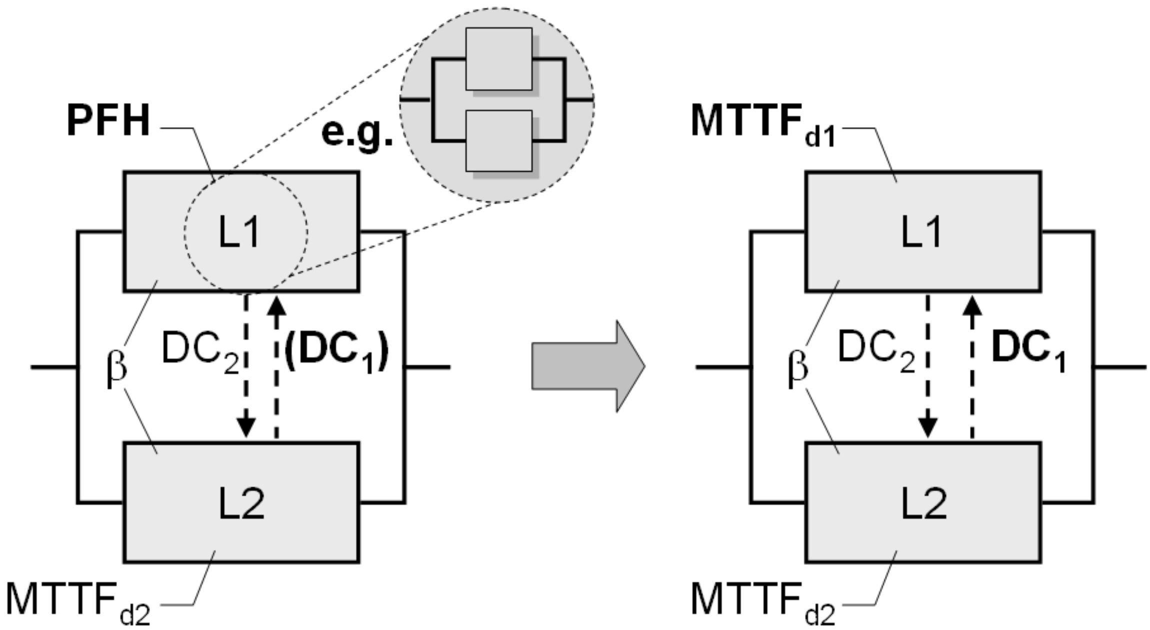
This method is possible from SISTEMA Version 1.1.2 onwards. For internal processing reasons, SISTEMA ticks fault exclusion in this case. If the subsystem with fault exclusion is the only subsystem below the safety function, SISTEMA indicates with a yellow warning message that the safety function is implemented 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 13849-1:2008-12, 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 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 and PL values stated by the manufacturer. The question is therefore how the encapsulated subsystem L1 with known PFH 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:

---

[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

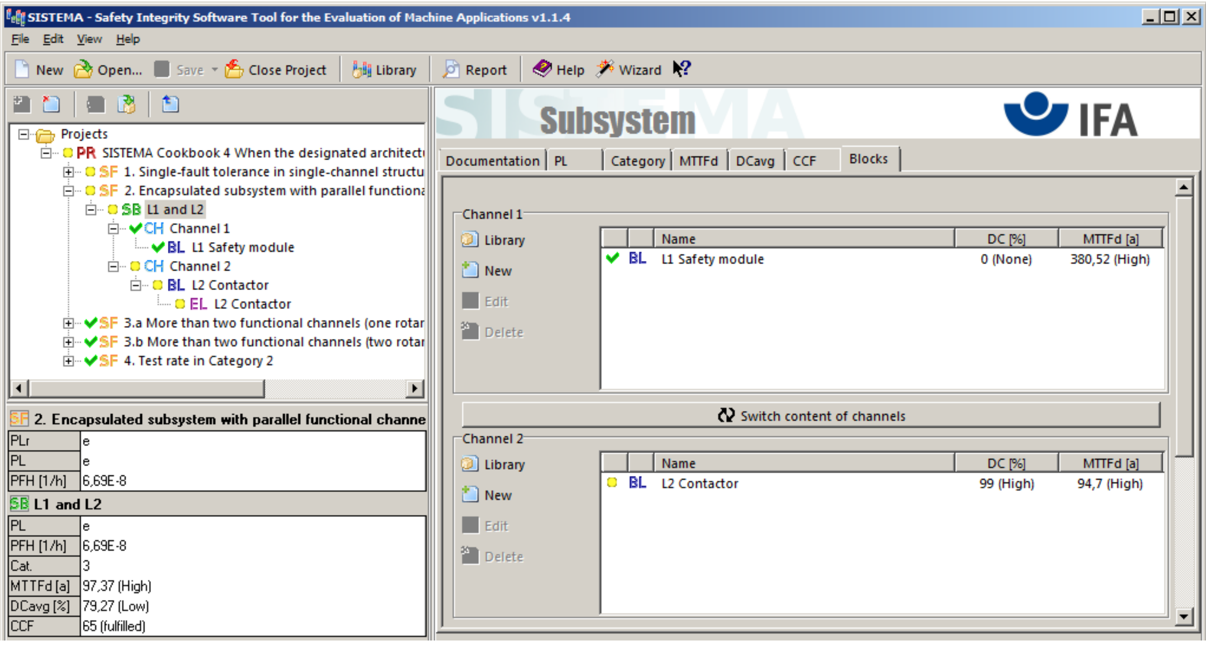
$$MTTF_{d1} = \frac{1}{PFH} \quad \text{and} \quad DC_1 = 0\%$$

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:

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

Figure 4 shows application of the approach in SISTEMA. The subsystem shown consists of a safety module in the form of an encapsulated subsystem (PL d, PFH = 3,00E-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.

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



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

2.3 Tip

The reciprocal is formed automatically by SISTEMA when the PFH value is entered in the "Dangerous failure rate" field on the $MTTF_d$ tab. For example, PFH = 3.00 E-7/h corresponds to an input of 300 FIT (1 FIT = 1 E^{-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, 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 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. 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. Under these circumstances, $DC_1 = 0$ must first be assumed. 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.

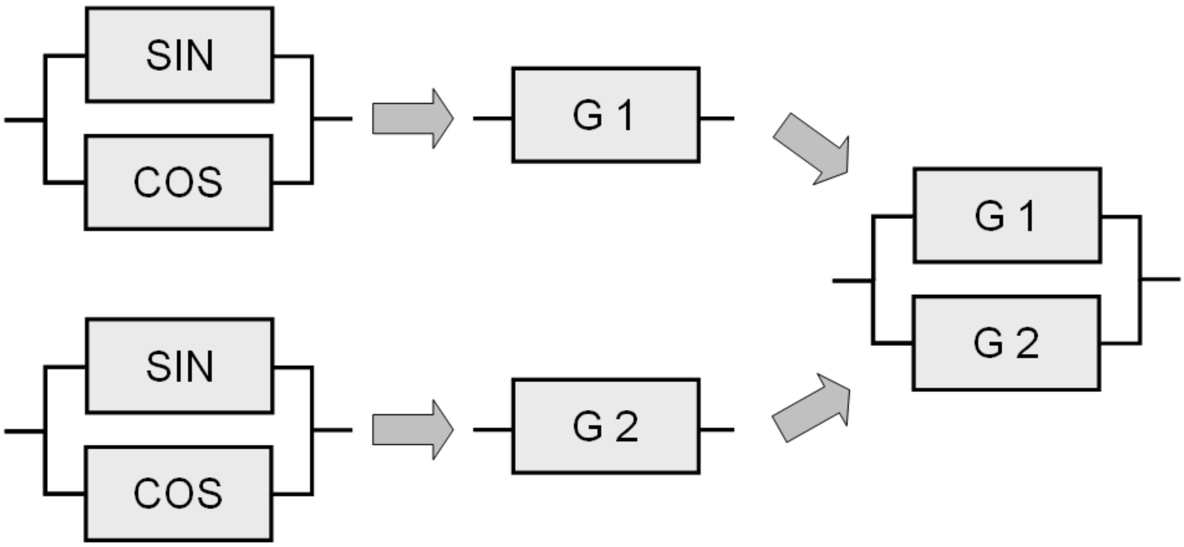
[8] With use of the 5% tolerance in accordance with Table 6 of the standard

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 attained PFH 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

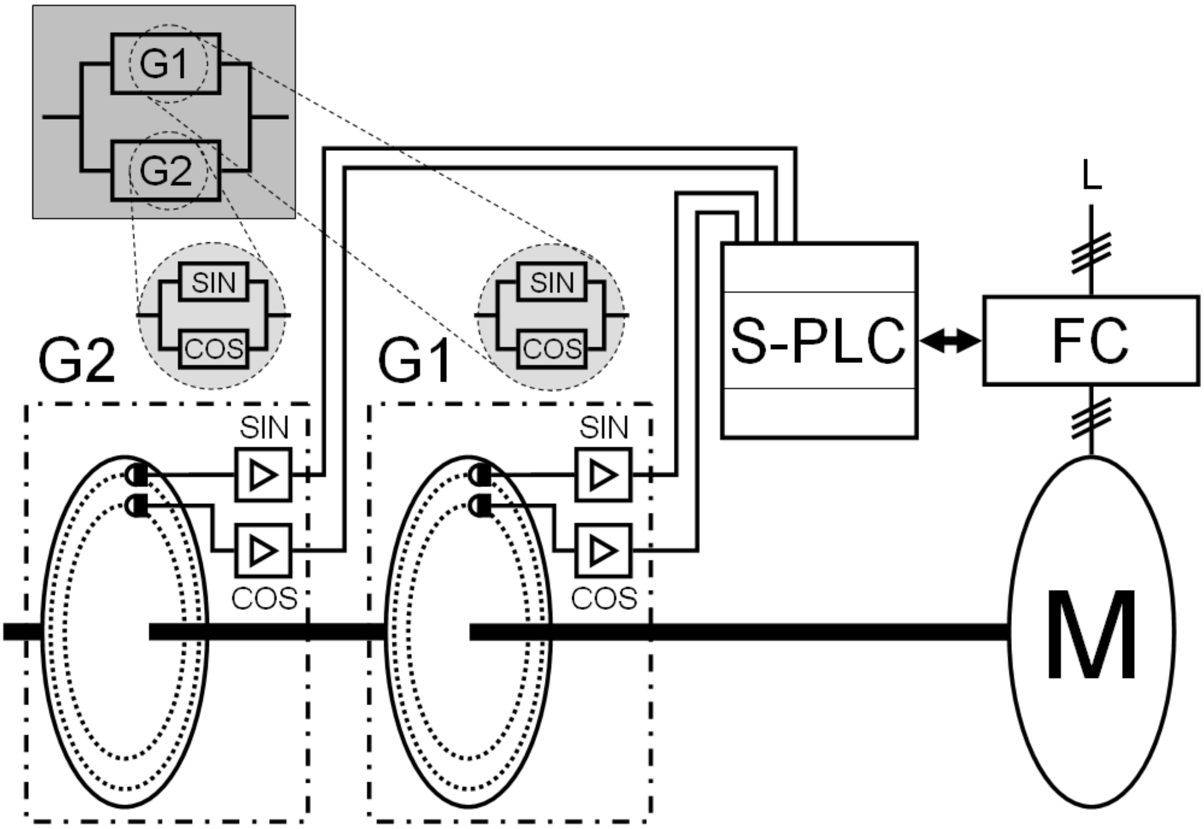


3.2 Input in SISTEMA

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 detect an angle of rotation α and supply the corresponding sine and cosine output signals. 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 to the safety function.

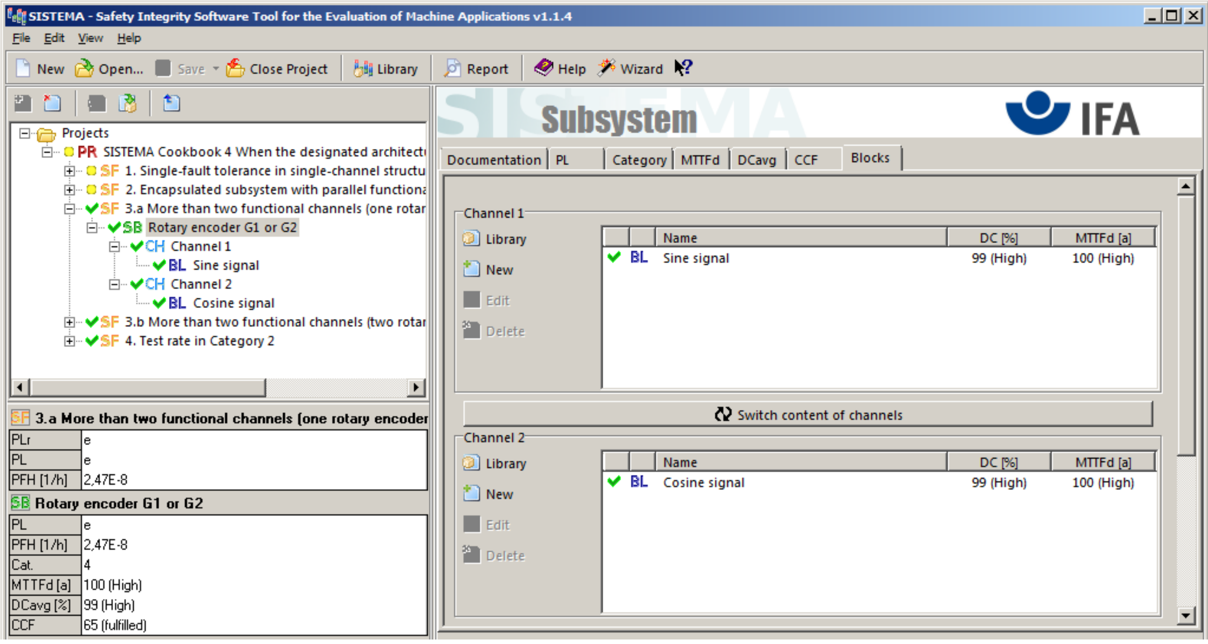
Figure 6:
Example of a four-channel structure for detection of a rotary angle α



3.3 First step

The hardware for the sine and cosine signal from each encoder would normally 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 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 values determined for each of the two encoders are 2.47E-8/h and form the result of the first step (see Figure 7). These values are used in the second step.

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



3.4 Second step

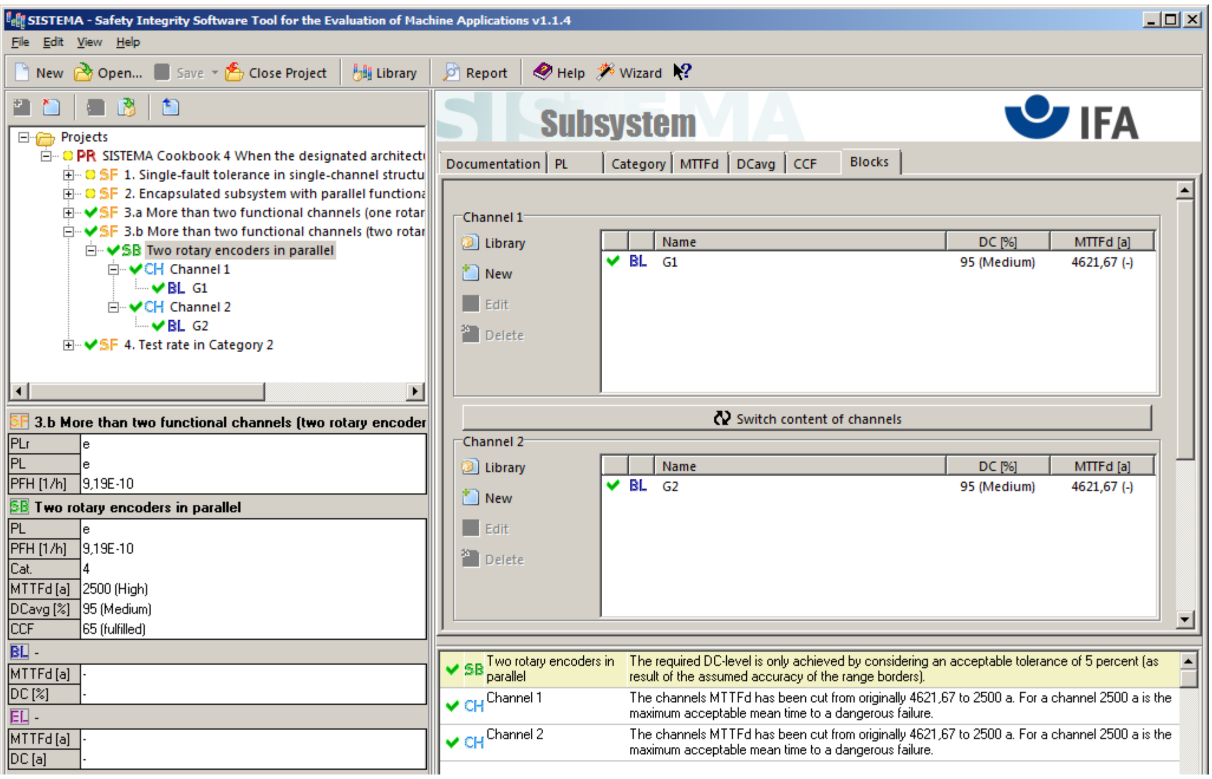
A new Category 3 or Category 4 two-channel subsystem in which each individual encoder is modelled as a block in a channel can be created for the overall system from two encoders, as described in Chapter 2.

The reciprocal of the PFH for an individual encoder is employed as the $MTTF_d$ of the blocks ($MTTF_d$ = 1/PFH). In this case, the resulting $MTTF_d$ values for each of the two encoders are 4621.67 years, i.e. the reciprocal of 2.47E-8/h or an input of 24.7 FIT for the dangerous failure rate. In SISTEMA, the expert option of "Raise the $MTTF_d$ capping for Category 4 from 100 to 2500 years" should also be activated[9].

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 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).

[9] German comment for the amendment of the standard, cf. Apfeld, R.; Bömer, T.; Hauke, M.; Huelke, M.; Schaefer, M.: Praktische Erfahrungen mit der DIN EN ISO 13849-1. openautomation (2009) Nr. 6, S. 34-37, online at www.dguv.de/ifa/13849e

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 for encoders for safety-related applications. Where this is the case, the first step can be skipped.

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 geometry of the light-sensitive parts of 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 is nevertheless 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 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: 2007, Table D.16.

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.

4 Test rate in Category 2

4.1 Description

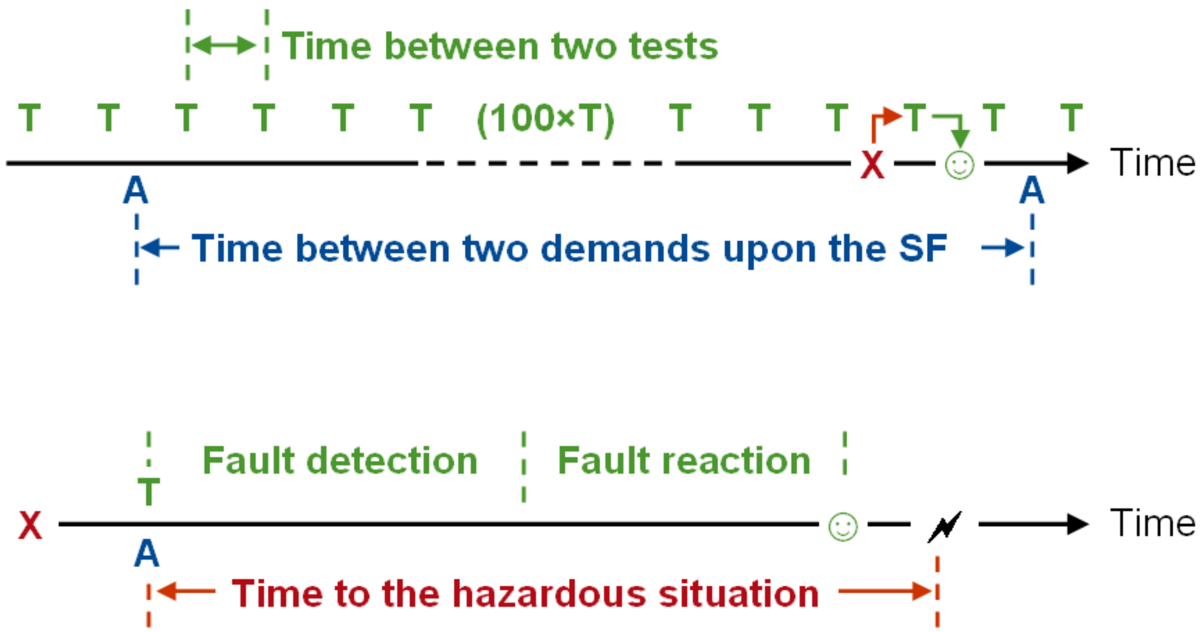
The reliability of a single-channel tested architecture, as provided for by Category 2, depends strongly upon the test rate. If a test is performed too infrequently, the safety it provides is deceptive: as the test interval increases, so does the probability of a dangerous failure of the safety function 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 in the following two cases:

Case 1 The ratio of the test rate to the demand rate upon the safety function is lower than 100 but at least 25. Calculation is then possible with use of a PFH allowance.

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



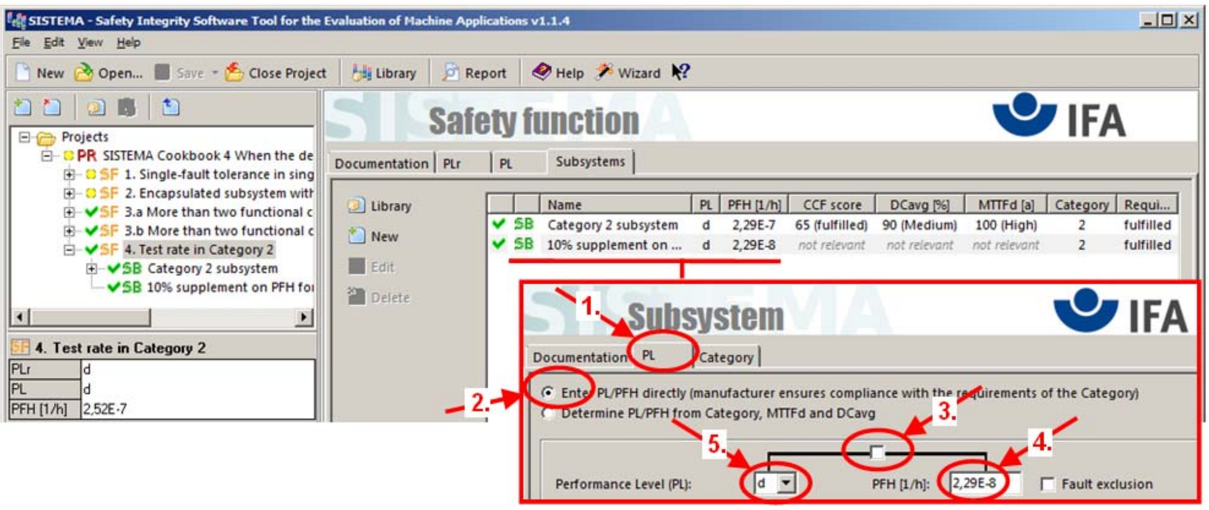
4.2 Case 1: The ratio of the test rate to the demand rate upon the safety function is lower than 100 but at least 25

A second subsystem the PFH value of which reflects the PFH allowance with respect to the ratio of 100 is added to the original Category 2 subsystem with a suboptimal rate ratio. The PFH value to be entered directly is 10% of the PFH value of the first Category 2 subsystem (see Section 4.3).

For this purpose, Category 2 must be selected on the "Category" tab in the first subsystem, and the condition "The demand rate upon the safety function is lower than or equal to 1/100 of the test rate" nevertheless marked as satisfied under "Requirements of the Category". Attention should be drawn in the documentation field for the subsystem to the particular issues and to the fact that the two subsystems belong together.

Figure 10 shows the example of a Category 2 subsystem with $MTTF_d$ = 100 years, DC = 90%, and a value of 25 for the ratio of the test rate to the demand rate upon the safety function. SISTEMA calculates a PFH value of 2.29E-7/h (PL d) subject to the ratio between the rates being 100. In accordance with the above procedure, the PFH allowance is calculated as 0.1 x 2.29E-7/h = 2.29E-8/h. For the additional subsystem, the PL and PFH value must be entered directly (2.) on the "PL" tab (1.). For this purpose, the PL input is decoupled from the PFH value (3.), a PFH value of 2.29E-8/h entered (4.), and d also entered as the PL (5.). Category 2 can also be entered for the additional subsystem.

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



4.3 Remarks

The increase in the probability of failure as a function of the ratio of the test rate to the demand rate can be determined by Markov modelling. At a ratio of at least 25, the maximum relative PFH allowance applicable under worst-case conditions is approximately 10%. The relative allowance refers to the PFH value of the Category 2 subsystem determinable by SISTEMA with an optimum ratio of the test rate to the demand rate of 100 or higher.

4.4 Case 2: Fault detection and fault reaction are triggered by the demand upon the safety function and occur more quickly than incidence of the hazardous situation

Under "Requirements of the category" on the "Category" tab of a Category 2 subsystem in SISTEMA, the condition "The demand rate upon the safety function is lower than or equal to 1/100 of the test rate" can also be marked as satisfied 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 don't match", Chapter 4)".

4.5 Remarks

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 also described in BGIA Report 2/2008e, Section 6.2.14, Point 3 and in Section 6.3.2 of IEC 62061. This is also the subject of a current proposal for an amendment to EN ISO 13849-1. Suitable model circuits are shown in BGIA Report 2/2008e, 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.