Functional Safety

DRAFT 2010-09-09

for personal use only

Please send any comments to:

juergen.eilers@apis.de

The contents of this document are currently being checked by experts.
The latest version of the document can be downloaded here at any time:

http://iq.apis.de/FunctionalSafety

The "functional safety" board within the APIS forum provides information about changed versions (please don't hesitate to write in English). If you wish to be informed of these automatically, please activate the board's subscription function. If you have no access to this board, permission needs to be granted. In this case, please send an email to:
info@apis.de

All information in this document is provided without warranty and may be changed without further notice. APIS Informationstechnologien GmbH does not enter into any obligation on the basis of such information. The software described in this document is provided on the basis of a licence contract.

Contents

Preface

This document describes functional safety procedures. Their application allows the development of electrical, electronic or programmable electronic systems (E/E/PE systems), which remain in or enter a safe state, should incidental or systemic failures with dangerous effects occur.

The APIS IQ software supports the IEC 61508 standard. The following description makes use of the ISO/DIS standard covering "road vehicles" to illustrate the software's functions. If the presentation is adapted to cover IEC 61508 or another norm derived from it, the examples and illustrations will need to be adapted in line with this.

Within the APIS IQ software, and consequently also in the screenshots shown, the terms used are only partially in accordance with ISO/DIS 26262. For example, the terms "SIL/ASIL" are both used, even though only "ASIL" is relevant in the context of ISO/DIS 26262.

Jürgen Eilers

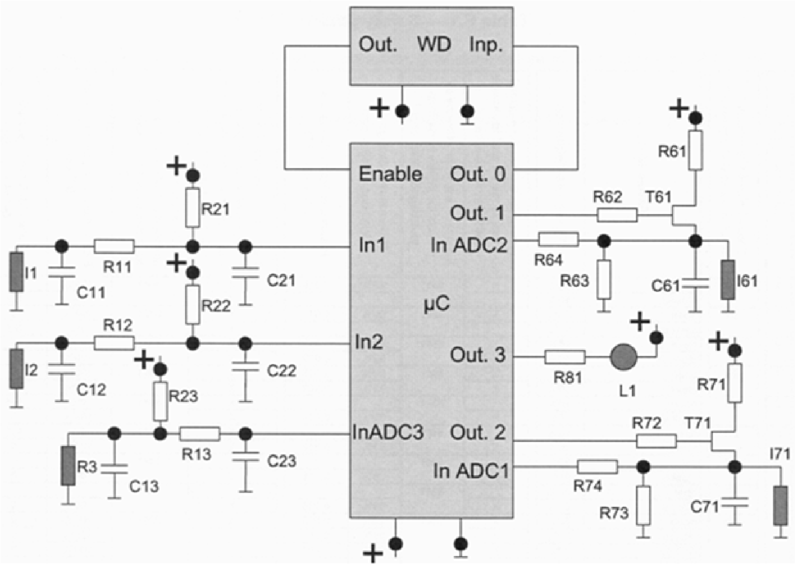
Email: juergen.eilers@apis.de

Abbreviations

E/E/PE-System	Electrical, electronic or programmable electronic system
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
DIS	Draft International Standard
SIL	Security Integrity Level
ASIL	Automotive Security Integrity Level
DC	Diagnostic Coverage
FIT	Failure in Time

The task

For a given system, the aim is to show that all functional safety requirements have been met.



Source: ISO/DIS 26262-5 (2009) - Annex F: Figure F.1 - Example Diagram

Illustration: Example system “Convertible hood control”

In the above system, an ECU (= µC) is used to activate two valves via the actuators I61 and I71. The available input signals are provided by wheel speed sensors I1 and I2. In addition, the temperature is measured using R3 sensor. The driver may be kept informed via LED L1. A watchdog, the electrical supply and various electronic components round out the system.

Therefore, the system appears as follows:

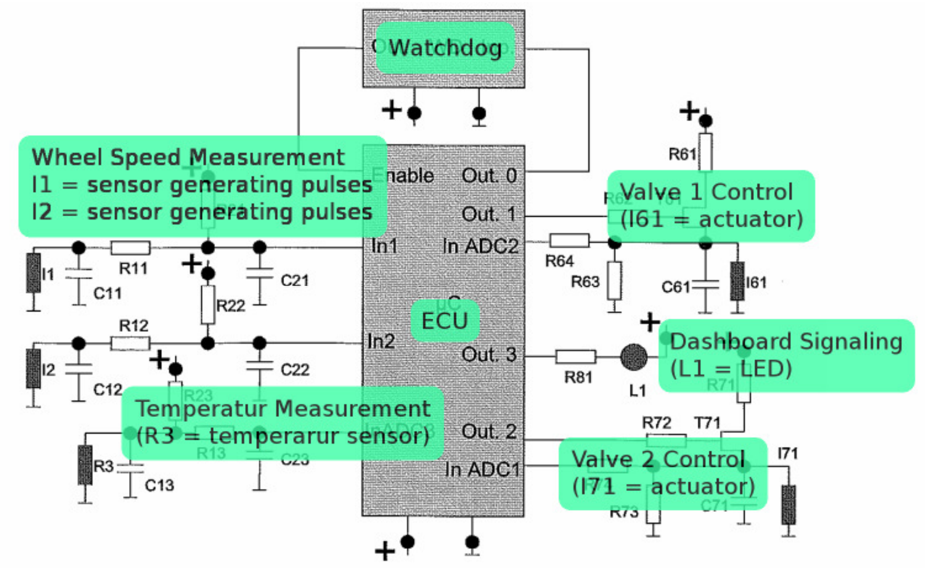


Illustration: Example system “Convertible hood control” (labelled)

We will initially consider faults in valve 1. Every potential failure at this location receives an ASIL value according to the ISO/DIS 26262-3 - Table 4 risk graph. Latent failures also need to be taken into account in order to carry out the calculation correctly.

For our example, we concentrate on the top-level fault “Valve 1 closes due to rf or sp”, which has been classified as ASIL C because it compromises the function “Valve 1 shall not close when speed is higher than 100 km/h”. In practical terms, this means that actuator I61 is incorrectly activated at a speed greater than 100 km/h.

The determination of an ASIL C leads to the following requirements according to ISO/DIS 26262-5 (2009) - Annexe E Table E.1:

- Single point faults metric (SPFM): > 97%
- Latent faults metrc (LFM): > 80%

A additional requirement arising from the top-level fault “Valve 1 shall not close when speed is higher than 100 km/h” is that the failure rate (failure in time (FIT)) must be below 100 FIT.

The developer now needs to state whether the system meets the requirements for this top-level fault. Generally, the expected component defect values are used for the calculation.

Solution

The APIS IQ software supports system modelling through the use of the structure tree, the function network and the failure network. For the moment, we will not consider the advantages that arise from the function network.

Structure tree and failure network

Showing part of the structure tree generated will make the failure network below easier to understand.

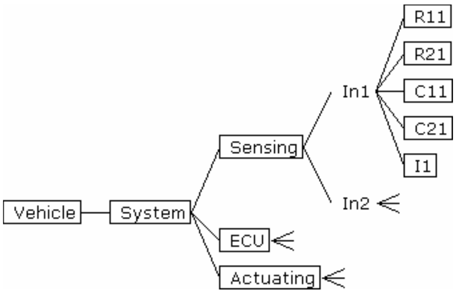


Illustration: Structure tree

The failure network links underlying faults in speed measurement per wheel rotation sensor I1 to the undesirable top-level event.

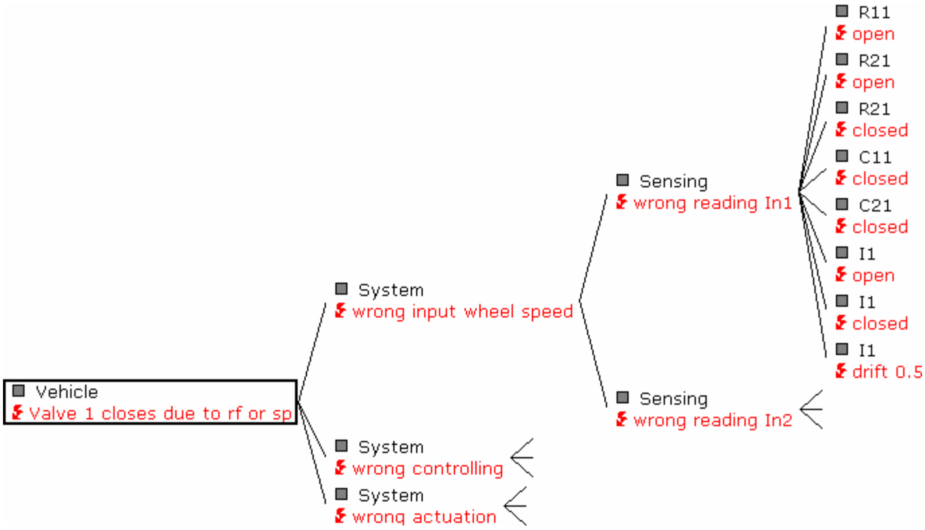


Illustration: Failure network (failure net)

The various ways in which components can go wrong are underlying faults. The failure network clearly shows which underlying faults may lead to the top-level failure. In the context of functional safety, the recognition of malfunctions is also important; this is documented as diagnostic coverage (DC) and may come up at any level within the failure network.

In the case of electrical and electronic components, there are relevant types of fault and expected values for the failure rate that do not depend on environmental conditions or the mode of operation. Details on these may be found in the corresponding norms and standards – one example would be the Siemens norm SN 29500.

Calculations within the failure network

The example used up to this point will be reduced in scope to make the calculations comprehensible and to familiarise you with the presentation of results.

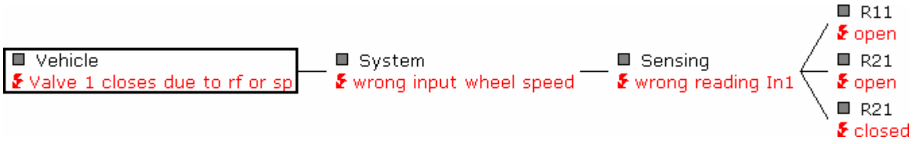


Illustration: Simplified failure network – two components with three malfunctions

Once the target values for the top malfunctions have been determined (ASIL, SPFM, PFH), and the attribute values for the underlying malfunctions (FR) have been entered together with the diagnostic coverage in the path to the malfunction, possibly at the level of the underlying malfunction, the result may be presented as follows:

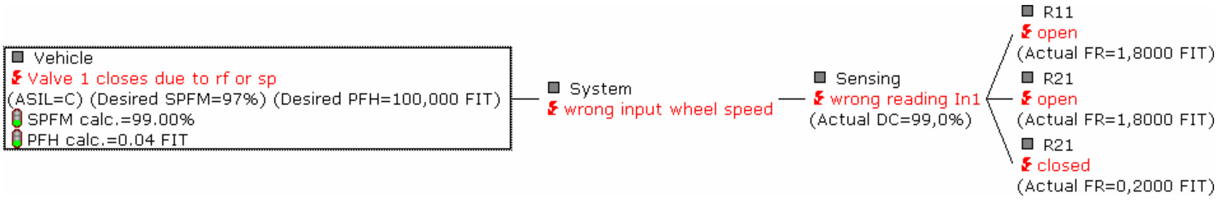


Illustration: Simplified failure network – displaying the functional safety parameters.

How should the information shown be interpreted? Let's begin at the right-hand side of the failure network. The assumed failure rates are shown for each malfunction, and the diagnostic coverage is shown for the malfunction one level above.

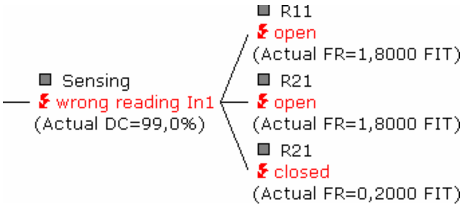


Illustration: Underlying fault with failure rate and diagnostic coverage (DC) for the malfunction one level above

To continue the calculation, the current failure rate is reduced at the next highest level, taking account of the best DC value. Another way of putting it is that the DC values in the failure network that are available at the next highest level are all attributed to the underlying faults. The failure rate (FIT value) of the underlying fault enters the calculation in the form of the maximum DC value.

The left-hand area of the failure network, containing top-level functions, is more interesting. This shows the target values and the calculated values, and there is a traffic light symbol to quickly make it clear whether the targets have been attained.

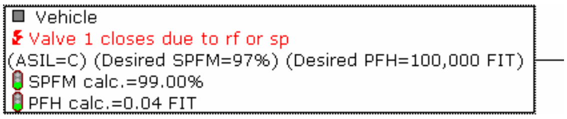

Vehicle
Valve 1 closes due to rf or sp
(ASIL=C) (Desired SPFM=97%) (Desired PFH=100,000 FIT)
SPFM calc.=99.00%
PFH calc.=0.04 FIT

Illustration: Top-level result with targets, and values as calculated

The first line, containing additional information, shows the requirements, i.e. the ASIL and the required SPFM and PFH. The remaining lines show the SPFM and PFH as calculated (SPFM calc. and PFH calc.). In the simplest case, the calculation is carried out according to the usual formula on the basis of the failure network.

< formula >

A traffic light symbol next to the calculated values shows the status of the comparison and whether all values needed for the calculation are available.

!🚦 Target value not attained, underlying parameters incomplete

🚦 Target value not attained

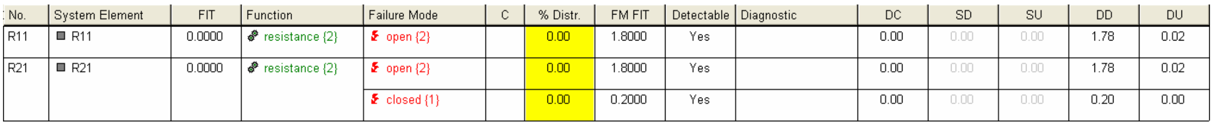
!🚦 Target value attained, underlying parameters incomplete

🚦 Target value attained

If the target value is not attained, or if the underlying parameters are incomplete, another subordinate function within the failure network can then be used as the focal element. The actual values are calculated for the selected sub-area, and a completeness check is made. A system may be iteratively optimised in this manner.

FMEDA form

The FMEDA form gives a clear overview of the functional safety parameters for underlying faults, e.g. malfunctions for construction elements, and the parameters can be efficiently processed within it.

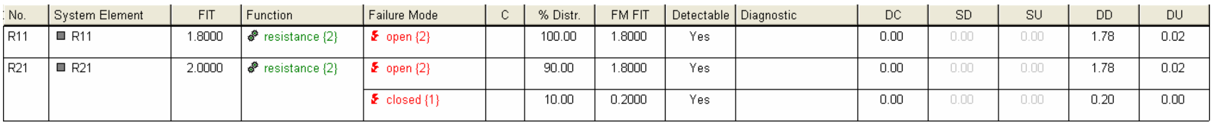


No.	System Element	FIT	Function	Failure Mode	C	% Distr.	FM FIT	Detectable	Diagnostic	DC	SD	SU	DD	DU
R11	■ R11	0.0000	resistance {2}	open {2}		0.00	1.8000	Yes		0.00	0.00	0.00	1.78	0.02
R21	■ R21	0.0000	resistance {2}	open {2}		0.00	1.8000	Yes		0.00	0.00	0.00	1.78	0.02
				closed {1}		0.00	0.2000	Yes		0.00	0.00	0.00	0.20	0.00

Illustration: FMEDA form – failure rates classified according to failure mode

The FMEDA table shows the functional safety attribute values for R11 and R12 resistances, which are then used for the calculation. The “FM FIT” column (more or less in the middle of the FMEDA form) shows the failure rates as they are fed into the malfunction. The last columns show the FIT values used for the calculation. Assuming a diagnostic coverage (DC) of 99%, the corresponding values for dangerous detectable (DD) and dangerous undetectable (DU) can be derived.

If the failure rates are to be used in the FMEDA form, they can alternatively be entered per construction element or as percentage per error type (% Distr.). The sum of the percentages may not be greater than 100%.



No.	System Element	FIT	Function	Failure Mode	C	% Distr.	FM FIT	Detectable	Diagnostic	DC	SD	SU	DD	DU
R11	■ R11	1.8000	resistance {2}	open {2}		100.00	1.8000	Yes		0.00	0.00	0.00	1.78	0.02
R21	■ R21	2.0000	resistance {2}	open {2}		90.00	1.8000	Yes		0.00	0.00	0.00	1.78	0.02
				closed {1}		10.00	0.2000	Yes		0.00	0.00	0.00	0.20	0.00

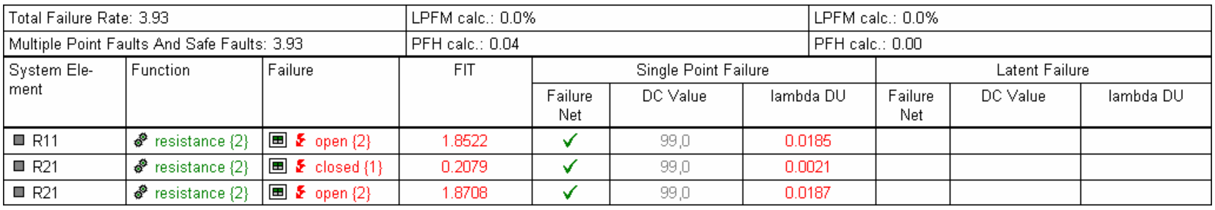
Illustration: FMEDA form – failure rates classified according to components and ranked according to the percentage per failure mode.

The “Detectable” column shows whether the failure mode has a diagnostic coverage value. The Diagnostic column shows the (preventative and) diagnostic measures available for that failure mode.

The ASIL classification of the top-level failure determines whether the failure rate is to be classified into safe detectable (SD) and safe undetectable (SU) classes, or dangerous detectable (DD) and dangerous undetectable (DU) classes. The appropriate risk graph helps establish the ASIL classification.

Failure table

The failure table may be called up via the failure network (context menu – functional safety failure table); similarly to the FMEDA form, it displays information on functional safety in the form of a table.



Total Failure Rate: 3.93	LPFM calc.: 0.0%	LPFM calc.: 0.0%
Multiple Point Faults And Safe Faults: 3.93	PFH calc.: 0.04	PFH calc.: 0.00

System Element	Function	Failure	FIT	Single Point Failure			Latent Failure		
				Failure Net	DC Value	lambda DU	Failure Net	DC Value	lambda DU
■ R11	resistance {2}	open {2}	1.8522	✓	99,0	0.0185			
■ R21	resistance {2}	closed {1}	0.2079	✓	99,0	0.0021			
■ R21	resistance {2}	open {2}	1.8708	✓	99,0	0.0187			

Illustration: Failure table

Risk graph for ASIL classification

		Exposure E	Controllability C		
			C1	C2	C3
Severity S	S1	E1	QM	QM	QM
		E2	QM	QM	QM
		E3	QM	QM	A
		E4	QM	A	B
	S2	E1	QM	QM	QM
		E2	QM	QM	A
		E3	QM	A	B
		E4	A	B	C
	S3	E1	QM	QM	A
		E2	QM	A	B
		E3	A	B	C
		E4	B	C	D

Table: Risk graph for SIL classification according to ISO DIS 26262-3(2009) Table 4

The top-level failure is categorised as QM, or ASIL A to D, in terms of its severity, exposure, and controllability, using the following categorisations per ISO/DIS 26262-3(2009) Annexe B).

Severity
S0: No danger of injury
S1: Mild and moderate injuries
S2: Serious and possibly fatal injuries
S3: Serious and probably fatal injuries

Exposure
E1: Rare: the situation affects most drivers less than once a year
E2: Occasional: the situation affects most drivers several times a year
E3: Fairly frequent: the situation affects average drivers once a month or more
E4: Frequent: the situation occurs during practically every journey

Controllability
C1: Easy to control: more than 99% of drivers or other road users are generally capable to avoid injury
C2: Average controllability: more than 90% of drivers or other road users are generally capable to avoid injury
C3: Difficult to control: fewer than 90% of drivers or other road users are generally capable to avoid injury

Safe or Dangerous

If the top-level failure is classed as QM, the failure rate of the underlying fault is classified as safe detectable (SD) or safe undetectable (SU). All ASIL categories are divided into the dangerous detectable (DD) or dangerous undetectable (DU) classes).

If the top-level fault is a latent failure, the corresponding underlying faults are classified as either SD or SU.

Calculations

The conceptual definitions needed to understand the calculation are listed in ISO/DIS 26262-1. The most important terms and their explanations are given here. The norm itself contains further remarks on individual terms.

fault abnormal condition that can cause an element or an item to fail

failure termination of the ability of an element or an item to perform a function as required

residual fault (λ_{RF}) portion of a fault that itself leads to the violation of a safety goal, occurring in a hardware element, where that portion of the fault is not covered by safety mechanisms

single point fault (λ_{SPF}) fault in an element that is not covered by safety mechanism and that leads directly to the violation of a safety goal

latent fault multiple point fault whose presence is not detected by a safety mechanism nor perceived by the driver within the multiple point fault detection interval

multiple point fault (λ_{MPF}) individual fault that, in combination with other independent faults, leads to a multiple point failure

multiple point failure failure, resulting from the combination of several independent faults, which leads directly to the violation of a safety goal

perceived fault fault whose presence is deducted by the driver within a prescribed time interval

detected fault fault whose presence is detected by a safety mechanism within a prescribed time

safe fault (λ_{S}) fault whose occurrence will not significantly increase the probability of violation of a safety goal

Function network procedure

The function network procedure expands upon the above description of the quantitative parameter calculation for top-level failures.

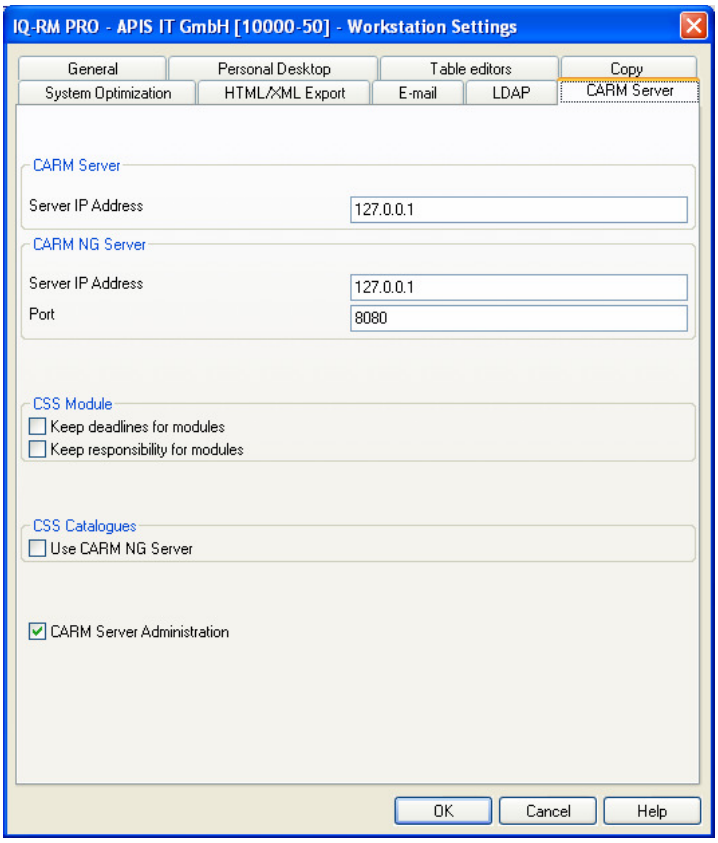
The function network is used to account for the calculation of failures that are not directly captured by the failure network. These faults may occur generally in a functional component group without having any direct effect on the observed top-level failure. They are categorised as safe faults (= λ_S). Starting from the function of the top-level failure, this involves consideration of all faults associated with the underlying functions (which may be determined using the function network.

Standard component catalogue

The failure rate of components constitutes the basis for calculating the reliability of systems. For this purpose, reference conditions are used to access known data. Expected values can be calculated for a system after construction. The operating conditions in each case provide the parameters for a suitable conversion model.

Existing or newly produced standards may be used to determine component failure rates. Based on data available for reference conditions for the relevant component type, together with a conversion model, the expected value for the failure rate under different conditions of use can be calculated. For example, the reference value λ_{ref} = 1 FIT for the component “passive construction element – resistance – carbon film - >100 kOhm” changes to 2.8 FIT at a temperature of 100 degrees

APIS CARM-NG-CSS Functional Safety was developed to facilitate this work. The address of the CARM-NG server is included in the workplace settings of the IQ software.



CARM Server

Server IP Address: 127.0.0.1

CARM NG Server

Server IP Address: 127.0.0.1

Port: 8080

CSS Module

□ Keep deadlines for modules

□ Keep responsibility for modules

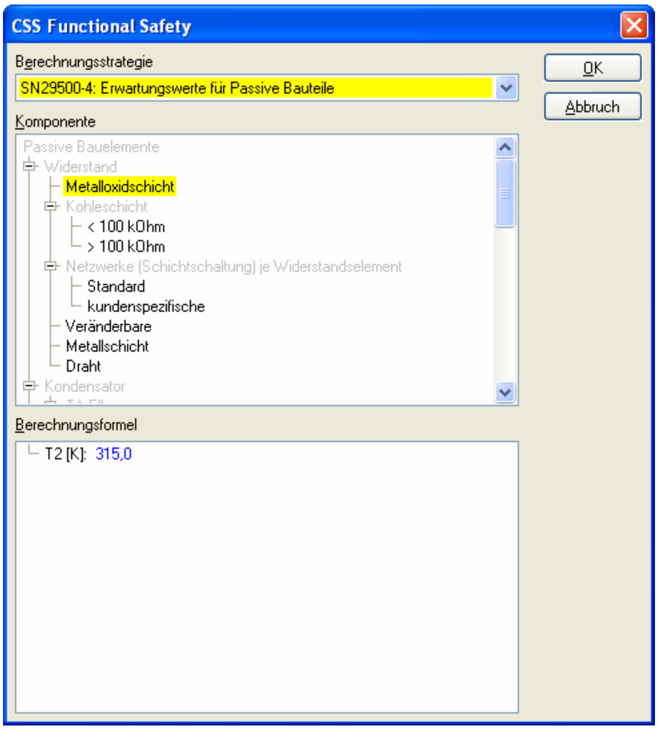
CSS Catalogues

□ Use CARM NG Server

☑ CARM Server Administration

Illustration: Workstation settings – CARM server/CARM NG server

It is then possible to assign an FIT value to all system elements via the FMEDA form. The menu item “Edit | Type of component | Set FIT value” calls up a dialog box to select the calculation strategy and components. The parameters for the calculation formula can also be entered in the same dialog box.



Berechnungsstrategie: SN29500-4: Erwartungswerte für Passive Bauteile

Komponente:

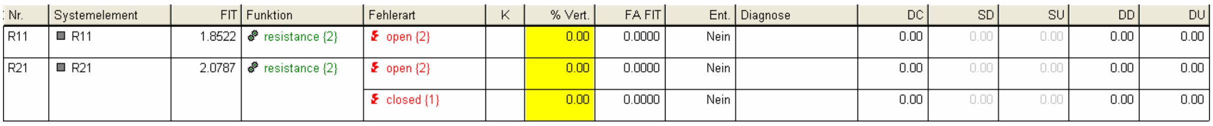
- Passive Bauelemente
- Widerstand
  - Metalloxidschicht
  - Kohleschicht
    - < 100 kOhm
    - > 100 kOhm
  - Netzwerke (Schichtschaltung) je Widerstandselement
    - Standard
    - kundenspezifische
  - Veränderbare
  - Metallschicht
  - Draht
- Kondensator

Berechnungsformel

T2 [K]: 315,0

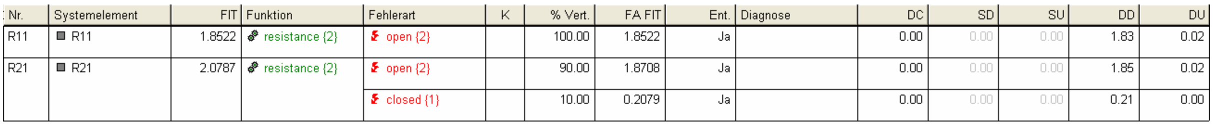
Illustration: Setting component and FIT value with support from CSS Functional Safety

Once the calculated FIT values have been applied, the FMEDA form shows the component-related FIT values, which are then proportionally allocated to the malfunctions by inputting the percentage in each case.



Nr.	Systemelement	FIT	Funktion	Fehlerart	K	% Vert.	FA FIT	Ent.	Diagnose	DC	SD	SU	DD	DU
R11	■ R11	1.8522	resistance {2}	open {2}		0.00	0.0000	Nein		0.00	0.00	0.00	0.00	0.00
R21	■ R21	2.0787	resistance {2}	open {2}		0.00	0.0000	Nein		0.00	0.00	0.00	0.00	0.00
				closed {1}		0.00	0.0000	Nein		0.00	0.00	0.00	0.00	0.00

Illustration: Components with calculated FIT values based on the central component catalogue



Nr.	Systemelement	FIT	Funktion	Fehlerart	K	% Vert.	FA FIT	Ent.	Diagnose	DC	SD	SU	DD	DU
R11	■ R11	1.8522	resistance {2}	open {2}		100.00	1.8522	Ja		0.00	0.00	0.00	1.83	0.02
R21	■ R21	2.0787	resistance {2}	open {2}		90.00	1.8708	Ja		0.00	0.00	0.00	1.85	0.02
				closed {1}		10.00	0.2079	Ja		0.00	0.00	0.00	0.21	0.00

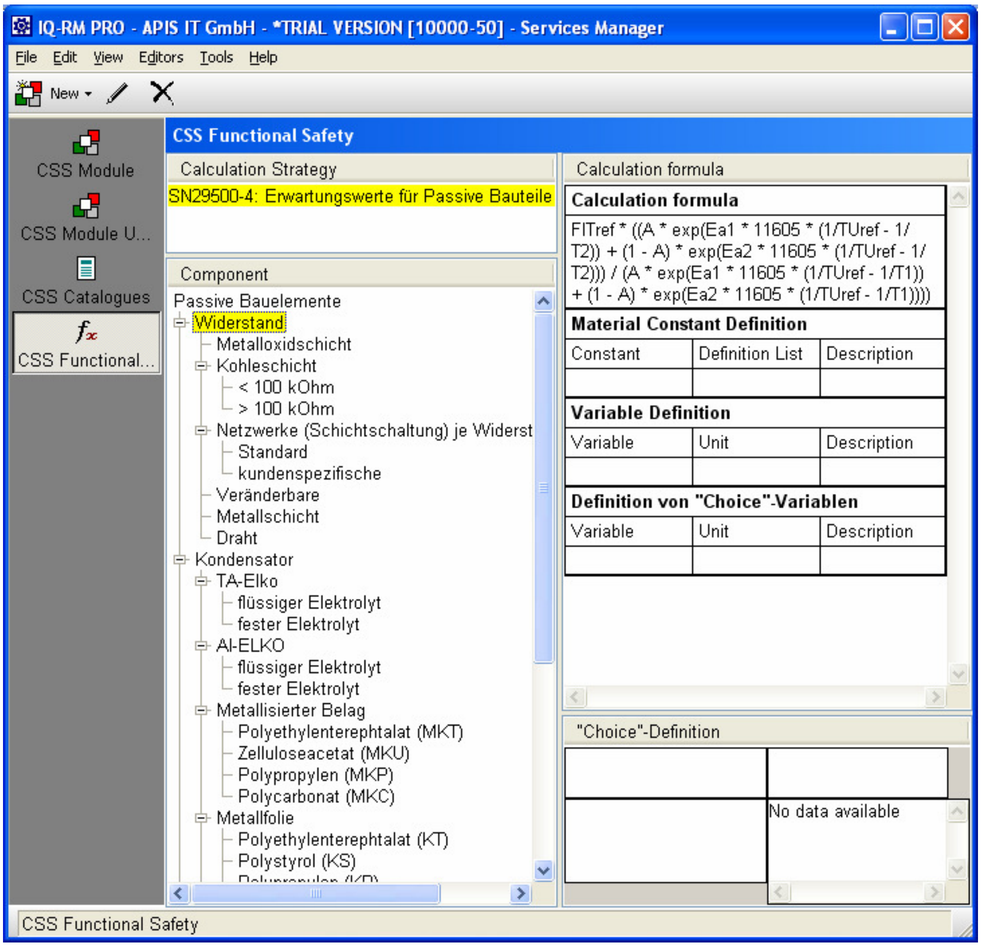
Illustration: Fault types of the components with proportional FIT values, taking into account diagnostic coverage

Calculation strategies

The calculation strategy for determining the component-related FIT values are available to all users of APIS IQ software via a CARM NG Server Service – CSS Functional Safety. Calculation strategies can be defined by users themselves. This means it is possible to integrate existing standards, such as Siemens standard SN 29500, into CSS Functional Safety as a basis for further use.

The functionalities in a calculation strategy are explained with reference to the implementation of SN 29000-4 “Expected values for passive components”.

As with any other CARM Server Service (CSS), administrator functions can be reached via the menu item “CARM Server | Administration”. The appropriate item in workstation settings that grants administration must be activated.



CSS Functional Safety

Calculation Strategy

SN29500-4: Erwartungswerte für Passive Bauteile

Component

- Passive Bauelemente
  - Widerstand
    - Metalloxidschicht
    - Kohleschicht
      - < 100 kOhm
      - > 100 kOhm
    - Netzwerke (Schichtschaltung) je Widerst
      - Standard
      - kundenspezifische
    - Veränderbare
    - Metallschicht
    - Draht
  - Kondensator
    - TA-Elko
      - flüssiger Elektrolyt
      - fester Elektrolyt
    - Al-ELKO
      - flüssiger Elektrolyt
      - fester Elektrolyt
    - Metallisierter Belag
      - Polyethylenterephtalat (MKT)
      - Zelluloseacetat (MKU)
      - Polypropylen (MKP)
      - Polycarbonat (MKC)
    - Metallfolie
      - Polyethylenterephtalat (KT)
      - Polystyrol (KS)
      - Polypropylen (KP)

Calculation formula

Calculation formula

FITref * ((A * exp(Ea1 * 11605 * (1/TUref - 1/T2)) + (1 - A) * exp(Ea2 * 11605 * (1/TUref - 1/T2))) / (A * exp(Ea1 * 11605 * (1/TUref - 1/T1)) + (1 - A) * exp(Ea2 * 11605 * (1/TUref - 1/T1))))

Material Constant Definition

Constant	Definition List	Description

Variable Definition

Variable	Unit	Description

Definition von "Choice"-Variablen

Variable	Unit	Description

"Choice"-Definition

No data available

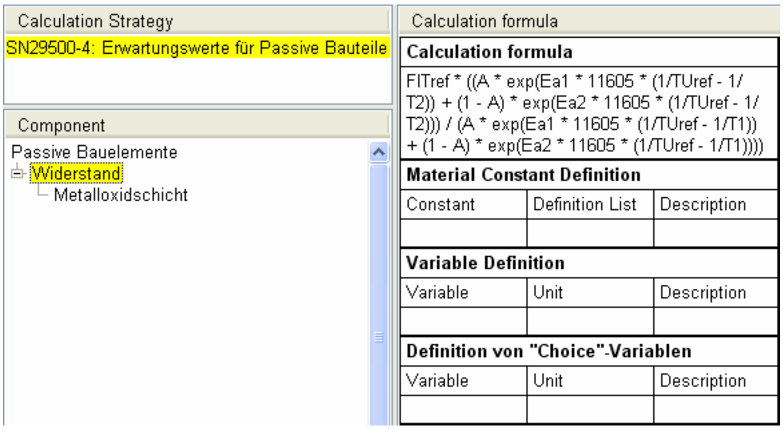
CSS Functional Safety

Illustration: CARM Server Administration with active CSS Functional Safety section and selected component category "Resistance"

The CSS Functional Safety section contains four subsections:

Calculation Strategy	Contains the name of the calculation strategy
Component	Contains a hierarchical tree of components; the entries related to the calculation formula are passed down within the tree
Calculation formula	Contains the mathematical calculation formula with constants, variables and "choice" variables
„Choice"-Definition	Selection from a pre-defined list

The calculation formula shown can be used as a template for your own calculation formulas. Determining the constants is self-explanatory. A reminder that all information is "passed down", i.e. a specific component doesn't require a calculation formula and constants if they have already been defined at a higher level in the hierarchical tree.



Calculation Strategy

SN29500-4: Erwartungswerte für Passive Bauteile

Component

Passive Bauelemente
- Widerstand
  - Metalloxidschicht

Calculation formula

Calculation formula
FITref * ((A * exp(Ea1 * 11605 * (1/TUref - 1/T2)) + (1 - A) * exp(Ea2 * 11605 * (1/TUref - 1/T2))) / (A * exp(Ea1 * 11605 * (1/TUref - 1/T1)) + (1 - A) * exp(Ea2 * 11605 * (1/TUref - 1/T1))))

Material Constant Definition

Constant	Definition List	Description

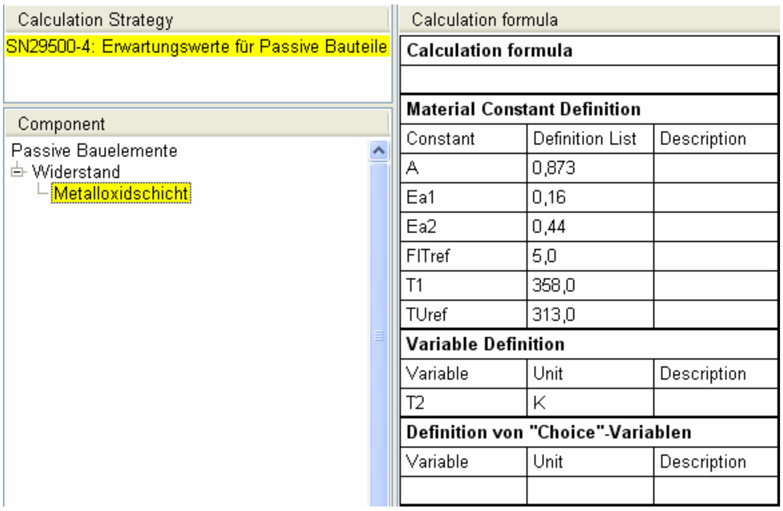
Variable Definition

Variable	Unit	Description

Definition von "Choice"-Variablen

Variable	Unit	Description

Illustration: Calculation formula for resistance



Calculation Strategy

SN29500-4: Erwartungswerte für Passive Bauteile

Component

Passive Bauelemente
- Widerstand
  - Metalloxidschicht

Calculation formula

Calculation formula

Material Constant Definition

Constant	Definition List	Description
A	0,873	
Ea1	0,16	
Ea2	0,44	
FITref	5,0	
T1	358,0	
TUref	313,0	

Variable Definition

Variable	Unit	Description
T2	K	

Definition von "Choice"-Variablen

Variable	Unit	Description

Illustration: Defining the constants and determining the variables that are needed in the calculation formula.

Safety policy

The calculation strategies stored on the CARM-NG server contain sensitive information on practical knowledge of components and calculation strategies. This means that access to the CARM NG server is subject to a role-based policy. Only users who are assigned the roles of “FS Admin” or “FS User” have access to CSS Functional Safety information. Users can be assigned the roles via a security configuration wizard.

A connection to the active directory or LDAP connection can be set up.

Quantitative parameters and formulas

A detailed description of the quantitative parameters for functional safety can be found in ISO DIS 26262. Top-level faults can alternatively be placed in one of the following classifications: QM, ASIL A, ASIL B, ASIL C, ASIL D or latent fault.

If one of the ASIL classes has been assigned, the demand level for the SPFM target and PFH target should then be compared with the calculated values “SPFM calculated” and “PFH calculated”.

For the relevant fault types, the ISO/DIS faults model makes a distinction between safe fault (λ_{S}), detected multiple point fault ($\lambda_{\text{MPF detected}}$, or $\lambda_{\text{MPF D}}$), perceived multiple point fault ($\lambda_{\text{MPF perceived}}$, or $\lambda_{\text{MPF P}}$), latent multiple point faults ($\lambda_{\text{MPF latent}}$, or $\lambda_{\text{MPF L}}$), single point fault (λ_{SPF}) and residual fault (λ_{RP})

Das Fehlermodell (Faults Model) der ISO/DIS unterscheidet bei den relevanten Fehlerarten zwischen Safe Fault (λ_{S}), Detected Multiple Point Fault ($\lambda_{\text{MPF detected}}$; auch $\lambda_{\text{MPF D}}$), Perceived Multiple Point Fault ($\lambda_{\text{MPF perceived}}$; auch $\lambda_{\text{MPF P}}$), Latent Multiple Point Faults ($\lambda_{\text{MPF latent}}$; auch $\lambda_{\text{MPF L}}$), Single Point Fault (λ_{SPF}) und Residual Fault (λ_{RF}).

Graphic: < Faults model: ISO/DIS 26262-5 C.1-page 34)

Image: Faults model according to ISO/DIS 26262(2009)

Calculating the single point fault metric (SPFM) is described in ISO/DIS 26262 as follows:

SPFM calculated = <formula ISO/DIS 26262-5 C.2-page 36>

Graphic: < Graphic representation of the single point fault metric; ISO/DIS 26262-5 C.2-page 36>

Image: Graphic representation of the single point fault metric (SPFM) according to ISO/DIS 26262(2009)

SPFM for a top-level fault is, according to ISO/DIS 26262, the percentage of all relevant fault types (λ), which are NOT dangerous undetected (=(= $\lambda_{\text{SPF}} + \lambda_{\text{RF}}$). SPFM therefore tends to improve if additional components with relevant fault types are added, provided they are multiple point faults (detected, perceived or latent). Alternatively, an attempt can be made to reduce the percentage in the dangerous undetected section via improved diagnostic coverage.

LFM calculated = <formula ISO/DIS 26262-5 C.3-page 37>

Graphic: <Graphic representation of the latent fault metric; ISO/DIS 26262-5 C.3-page 37>

Image: Graphic representation of the latent fault metric (LFM) according to ISO/DIS 26262(2009)

As regards LFM, the percentage of NON-latent faults is taken into account according to ISO/DIS. Only the relevant fault types are included in the basic total reduced by dangerous undetected ones $\lambda_{\text{SPF}} + \lambda_{\text{RF}}$).

Calculating in APIS IQ Software

APIS IQ software uses the following calculation formulas (source: IQ Software Help, status as of 2010-09-02):

SFF (individual fault)

$$\text{sff} = \frac{(\text{lambda SU} + \text{lambda SD} + \text{lambda DD})}{(\text{lambda SU} + \text{lmabda SD} + \text{lambda DD} + \text{lambda DU})}$$

Here, the relevant lambda values are the sum of all lambda values of the underlying faults from the failure network of the individual fault (safety target). The lambdaS values are determined via the function network of the function in which the individual fault is rooted.

SFF (latent)

$$\text{sff} = 1 - \frac{\text{lambda DU}}{\text{lambda} - \text{lambda RF}}$$

lambdaRF (Residual Faults) ::= corresponds to the lambdaDU of the individual fault.

PFH value:

the sum of all lambdaDU values of the underlying fault of the individual fault or latent fault.

FTA

Fault tree analysis (FTA) allows the user to: see the OR operators implicitly used in the FMEA in the causality relationships of the malfunctions (fault effects – fault type – fault cause), change the OR operators, or insert additional operators and allocate the malfunctions to these additional operators. In particular, AND operators can also be inserted.

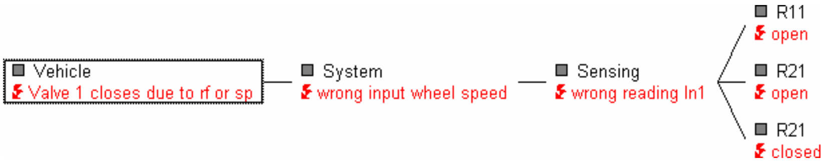


Illustration: Failure network "Valve 1 closes due to rf or sp"

If a fault tree is created for an existing failure network, OR operators are initially included there as additional nodes.

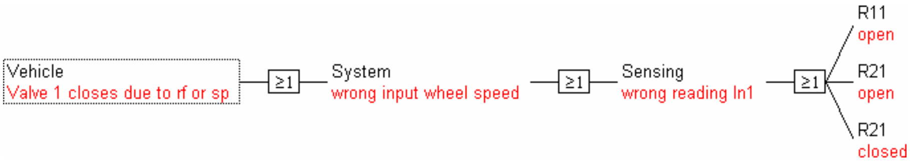


Illustration: Fault tree "Valve 1 closes due to rf or sp"

Minimal cut

The minimal cut is used to calculate the quantitative parameters for the top-level fault. This shows which underlying faults connected to which operators lead to the top-level fault. In unchanged fault trees that are based on failure networks, all underlying faults are allocated to the top-level fault with an OR operator, with no redundancy.

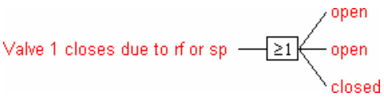


Illustration: Minimal cut to the fault tree "Valve 1 closes due to rf or sp"

The minimal cut is the basis for calculations in the fault tree based on ppm or alpha, beta, lambda and mu. This means that the corresponding attribute values only need to be recorded if the underlying faults that are included in the minimal cut.

In the case shown above, the minimal cut can be manually created in a simple process. If additional operators are included in the fault tree and a combination of OR/AND operators is present, minimising the basic malfunctions to the minimal situation with the operators that are then required can only be efficiently carried out using program support. The example shown is an only slightly expanded fault tree and the corresponding minimal cut.

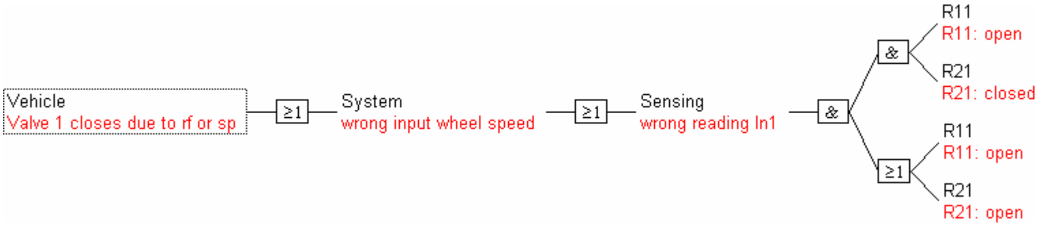


Illustration: Fault tree "Valve 1 closes due to rf or sp" with additional operators, i.e. a combination of AND and OR operators

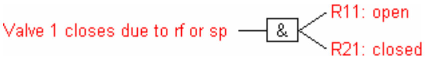


Illustration: Minimal cut of fault tree "Valve 1 closes due to rf or sp" with additional operators

Calculations within the fault tree

Potential calculations in the fault tree with a fault rate in ppm or unavailability and fault frequency will not be discussed here. More information on this can be found in the integrated Help or in the relevant seminars given by APIS Informationstechnologien GmbH.

FTA minimal cuts

FTA minimal cuts are highly relevant when it comes to fault classes in the area of functional safety, which are termed multiple point faults. A footnote in ISO/DIS 26262-1 (2009) defining a multiple point fault reads, "A 'multiple point fault' can only be recognized after the identification of 'multiple point failure' e.g. from cut set analysis of a fault tree."

If, in this context, we take a closer look at the ISO/DIS 26262-5 faults model and the statements about it, the direct connection with the minimal cut becomes clear.

Graphic: <Faults model: ISO/DIS 26262-5 C.1-page 34)

Illustration: Faults model according to ISO/DIS 26262(2009)

Citations from ISO/DIS 26262-5(2009)

"Multiple point fault: one fault of several independent faults that in combination, leads to a multiple point failure (either perceived, detected of latent)"
"Safe fault: fault whose occurrence will not significantly increase the probability of violation of a safety goal"
"The distance 'n' (Anm: im kreisförmigen Faults Modell eine Schicht mit Abstand ‚n' vom Zentrum) represents the number of independent faults present at the same time that cause a violation of the safety goal (n = 1 for single point faults, n = 2 for dual point faults, etc.);"
"Multiple point faults of distance strictly higher than n = 2 are to be considered as safe faults unless shown relevant in the functional or technical safety concept."

Based on these statements, minimal cuts can reveal the layer in the faults model in which the underlying faults are located. An underlying fault, which is directly connected to the top-level fault via an OR operator in the minimal cut, belongs to the underlying faults in order 1. An underlying fault which leads to the top-level fault together with another underlying fault via an AND operator belongs to order 2. If more than two underlying faults occur at the same time, these combinations correspondingly belong to order "n".

During a validation process according to ISO/DIS 26262, minimal cuts should be considered up to an appropriate order. The statement that "Multiple point faults of distance strictly higher than n = 2 are to be considered as safe faults …" is only justifiable based on certain assumptions. In particular, it must be ascertained that no common cause, which was not previously taken into account, has been forgotten.

APIS IQ software makes it possible to export the minimal cuts, which means the information can be easily incorporated in a validation report.

DC in detection procedures/mechatronics FMEA EA

Up to now, it has been assumed that diagnostic coverage is either directly available as an attribute value in the underlying fault or was recorded in another malfunction in the causality chain up to the top-level malfunction. A reminder: the best DC value is propagated to the underlying fault and then considered in the calculation as detectable or undetectable parts of the fault rate.

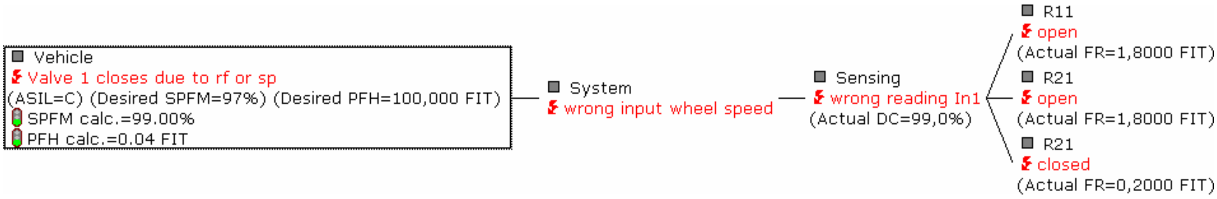


Illustration: Simplified failure network – displaying parameters for functional safety.

It is now possible to expand the failure network with elements of the mechatronics FMEA. Additional operating conditions, error detections and error responses are available there. A DC value can also be recorded in error detection and error response, which can then be accordingly considered in the calculation.

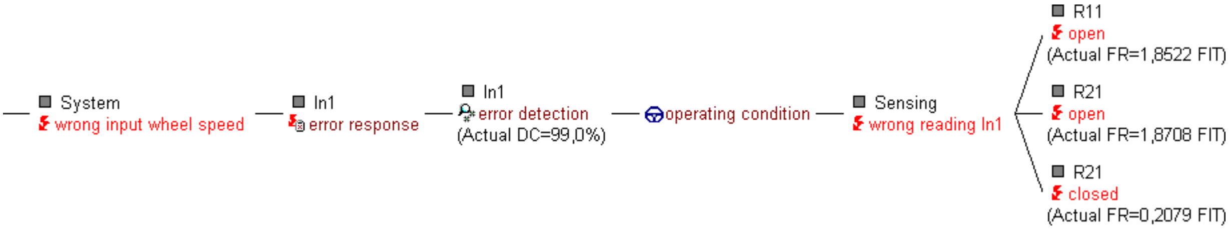


Illustration: Failure network with operating condition, error detection and error response, and DC in the error detection

In addition to this alternative for collecting the diagnostic coverage, the diagnostic coverage can also be collected in a preventative or detection measure. This attribute value is then propagated to the malfunction in which the measure is situated, and then used as normal in the calculation of the parameters for functional safety.

Control questions

[] Additional DC values in the failure network only have an effect on calculated values if these are above the previous maximum DC value.

Annexe: Possible topics for a presentation

Topic: Functional safety – support options with APIS IQ-Software

- System modelling: structure tree, function network and failure network
- Fault tree and minimal cuts
- Object attributes for functional safety
- Diagnostic Coverage
- Calculating in failure network
- FMEDA form
- Function network procedure
- CARM-NG server and standard component catalogues

APIS IQ software and functional safety roadmap

Concrete plans for developing functionalities in functional safety include:

Multi-channel ability	Mapping systems with hardware redundancy is to be improved.
DC	Calculating the SPFM and LFM is currently only possible using failure networks with the diagnostic coverage applicable in each case. Discussions with users are currently taking place about whether it is possible to document two different DC values in malfunctions and hence simplify the calculation
FMEDA layout	The tabular presentations for functional safety are to be made consistent. Discussions will take place on how the FMEDA form and the fault table can be combined.
Variant-specific	For users who also work with variants in functional safety, the necessary attribute values are to be defined in a variant-specific way.
Calculation strategies	Support from calculation strategies are to be expanded to guarantee that the project is up-to-date when retroactive changes are made to the calculation strategy.

Best practice

Examples are to be used to illustrate the possibilities of APIS IQ software. If you would like to submit your own attempts at solutions, then please send an email to Jürgen Eilers (juergen.eilers@apis.de).

Validation report with support from minimal cuts

The underlying faults, and their effects on top-level faults, that are to be considered in a validation report can be arranged and then exported out of the minimal cuts view. These exported files can then be examined in more detail up to the necessary order.

Firstly, as complete a failure network as possible is created. This is then turned into a fault tree. Operators can then be changed and inserted. Collecting new malfunctions is also possible. No quantitative parameters for calculation in the fault tree are collected, as the aim of exporting minimal cuts is possible without these files.

Components with malfunctions

If a components list is to be converted into a structure tree and these components are to receive standard functions and malfunctions, the following procedure should then be carried out:

First, the components list is carried over to the structure tree, e.g. a list in Word, Excel, or similar program, is highlighted and then copied to the clipboard using the Copy command (or CTRL+C). The components can now adopted in the IQ software using “Edit | Insert text content”. Next, the type of component and relevant malfunction is assigned, as a function, to each component from a catalogue. Any normal FME file can be used as a catalogue file and is opened in a second workspace to be used as a template.