ISO 26262:2018, 2nd ed: Example (Annex E) with APIS IQ software

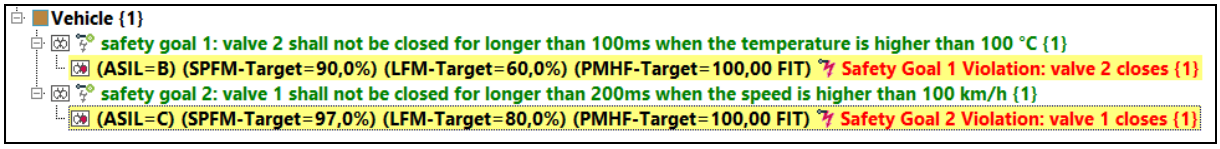
Step 0: Prerequisites for the handling in the fme-example file

1. **IQ-flavor:** APIS IQ-FMEA® PRO or APIS IQ-RM® PRO

2. **Structure editor:** display option for the *structure list*
   enabled option "Functional Safety parameters" in tab “Additional details”

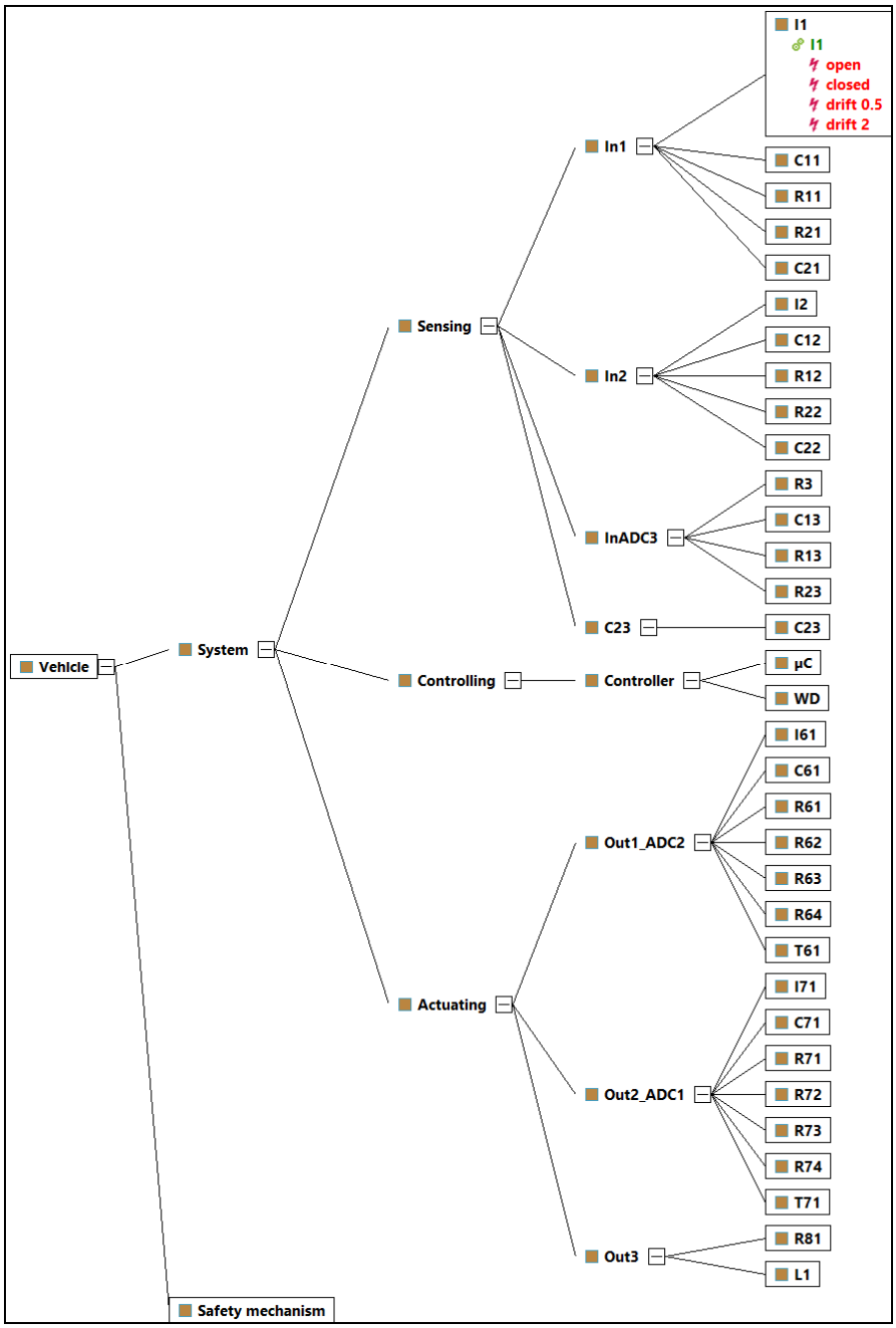
3. **Failure net editor:** display option
   enabled option "Functional Safety parameters" in tab “Functional Safety”

Step 1: Define safety goals with target values



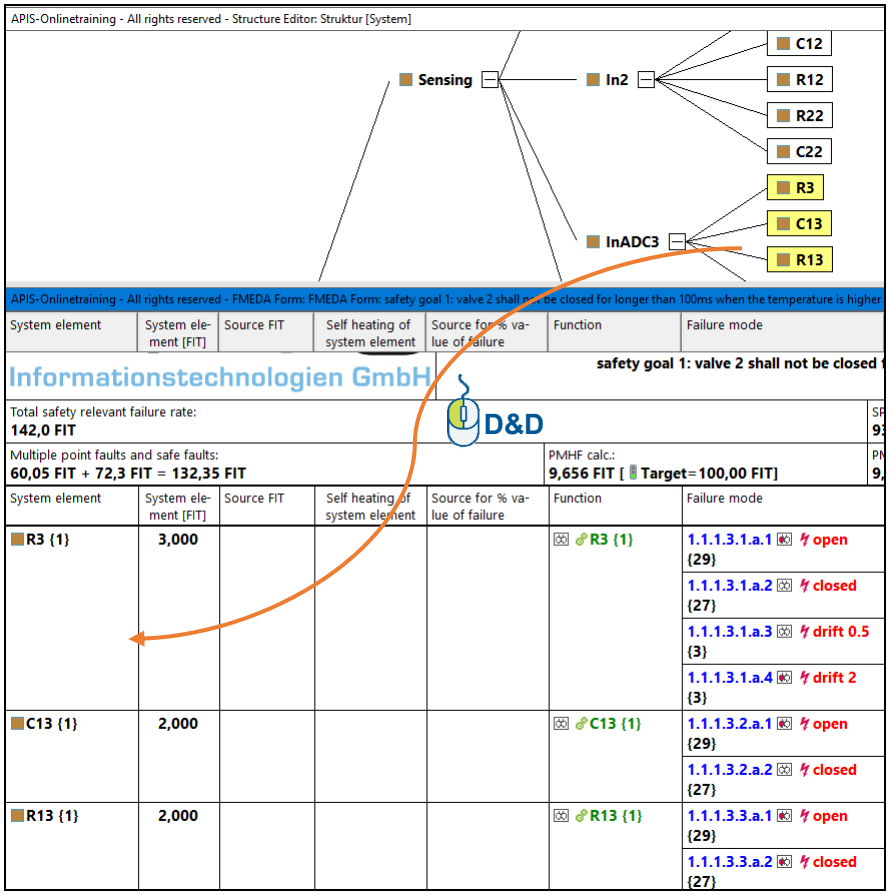
Step 2: Define E/E-components with actual values for each safety goal

2.1 Define the structure tree including functions and failures

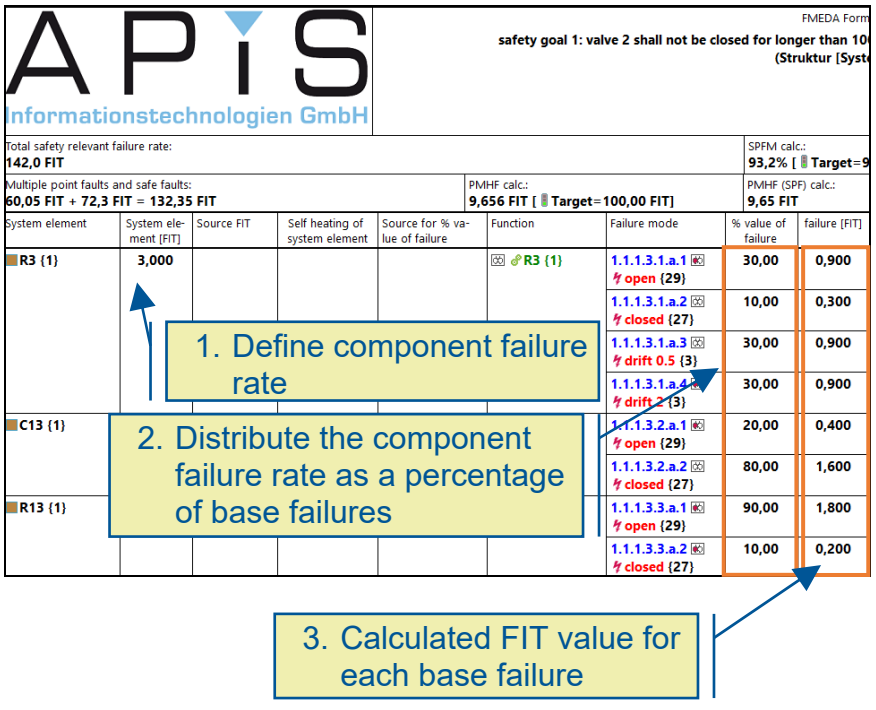


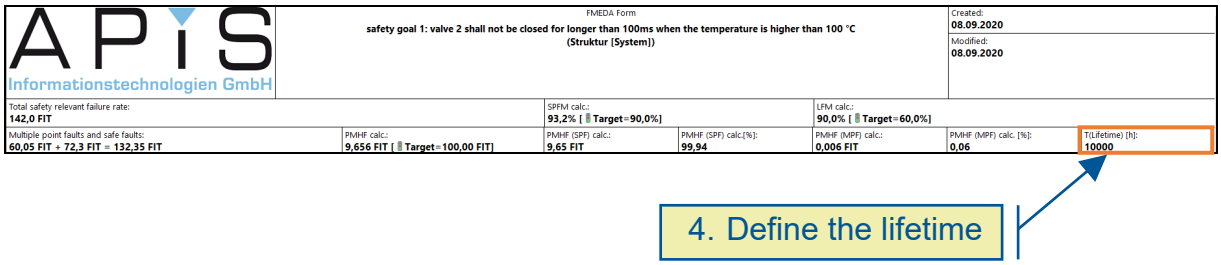
Remark: This tree is only one of the potential possibilities.

2.2 Drag the relevant E/E-components into the FMEDA for a particular safety goal

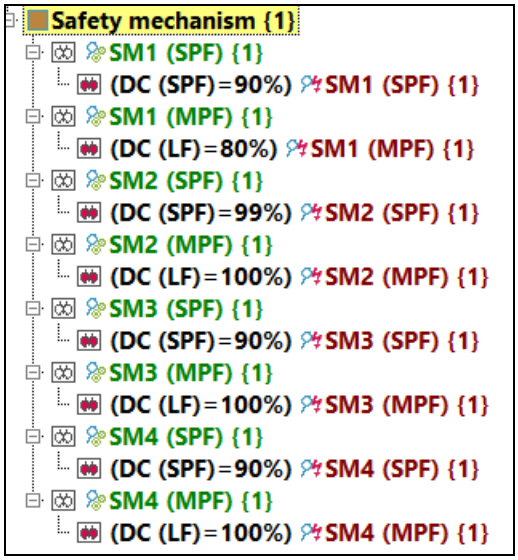


2.3 Define actual values within the FMEDA



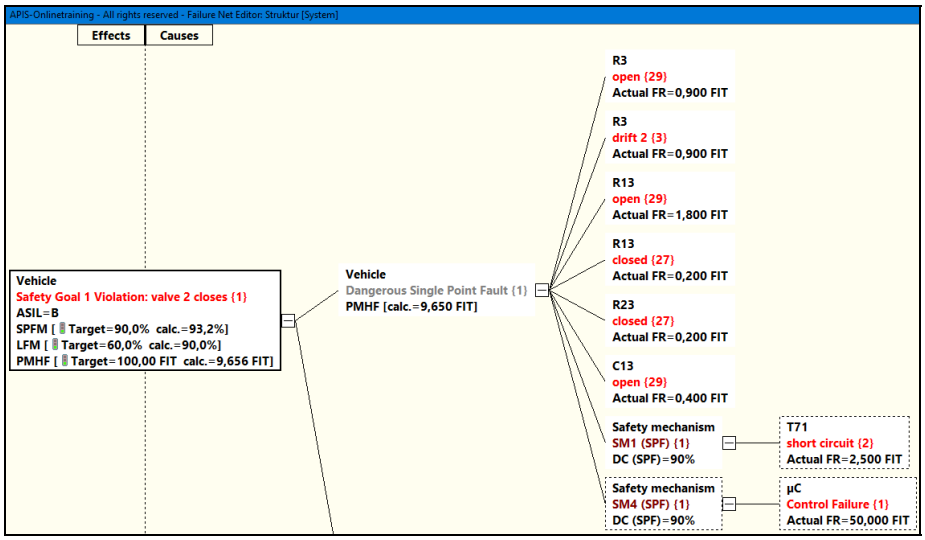


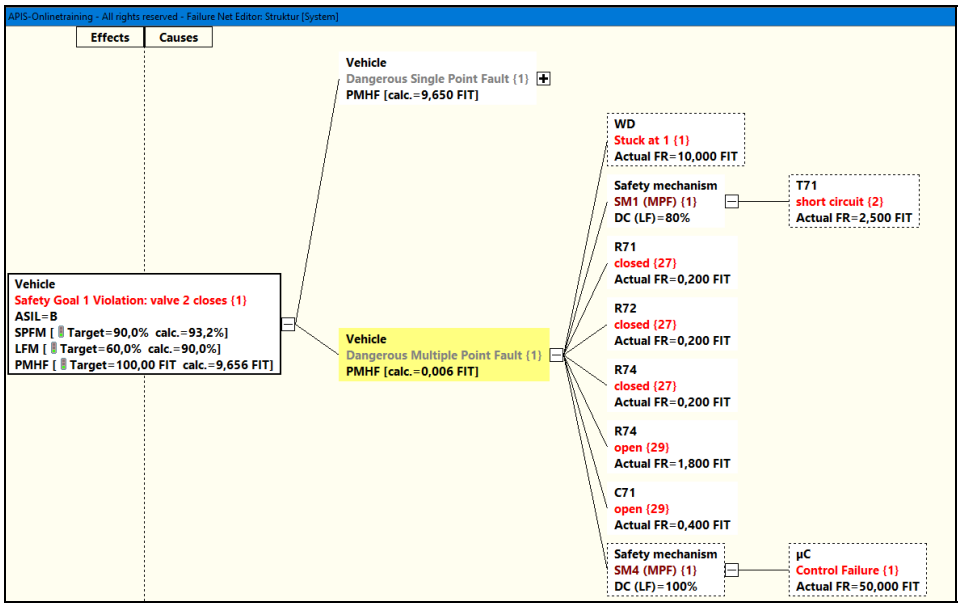
Step 3: Define the *safety mechanism* and their DC-values



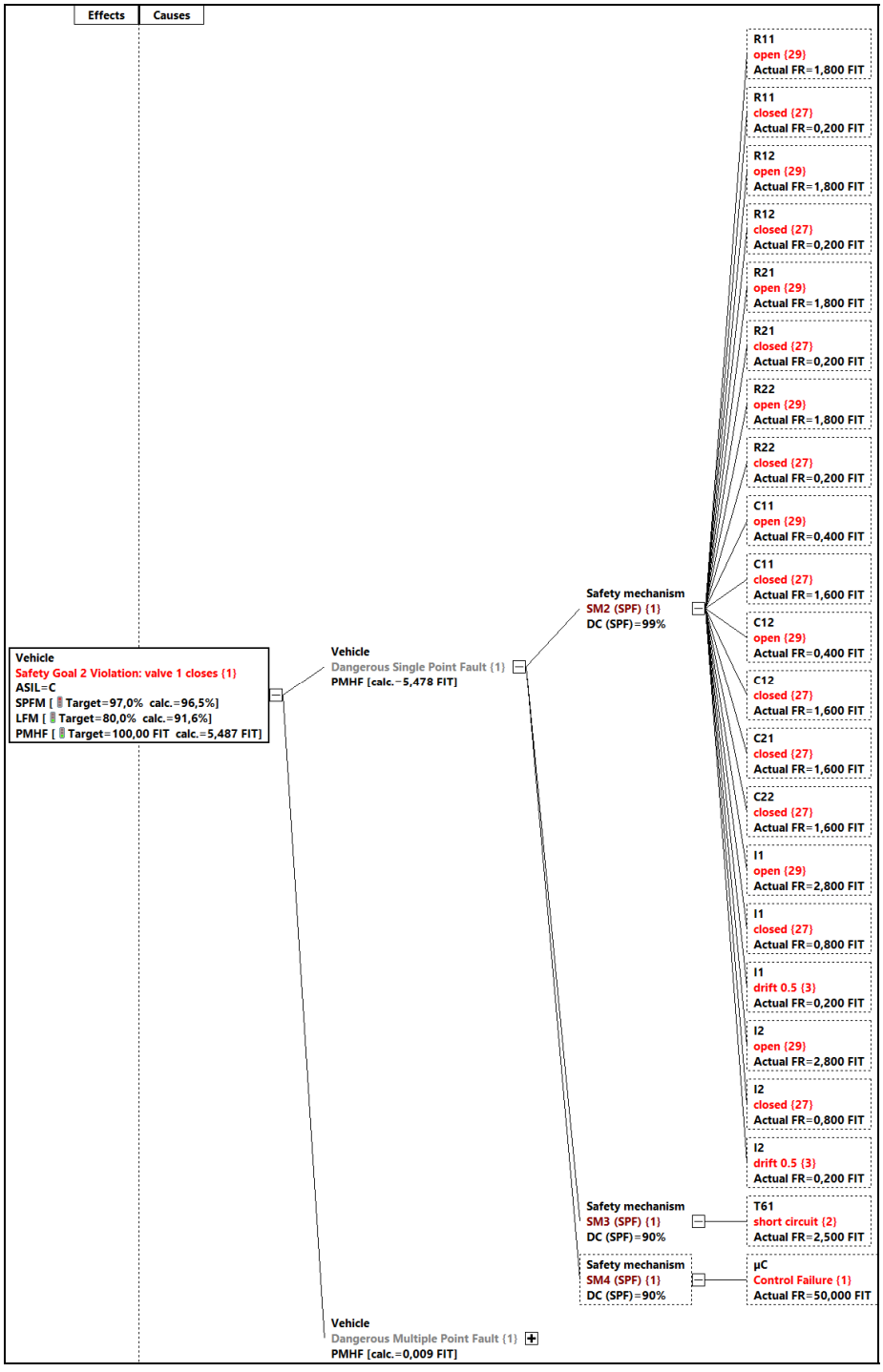
Step 4: Link the *failure nets* in the correct manner for each safety goal

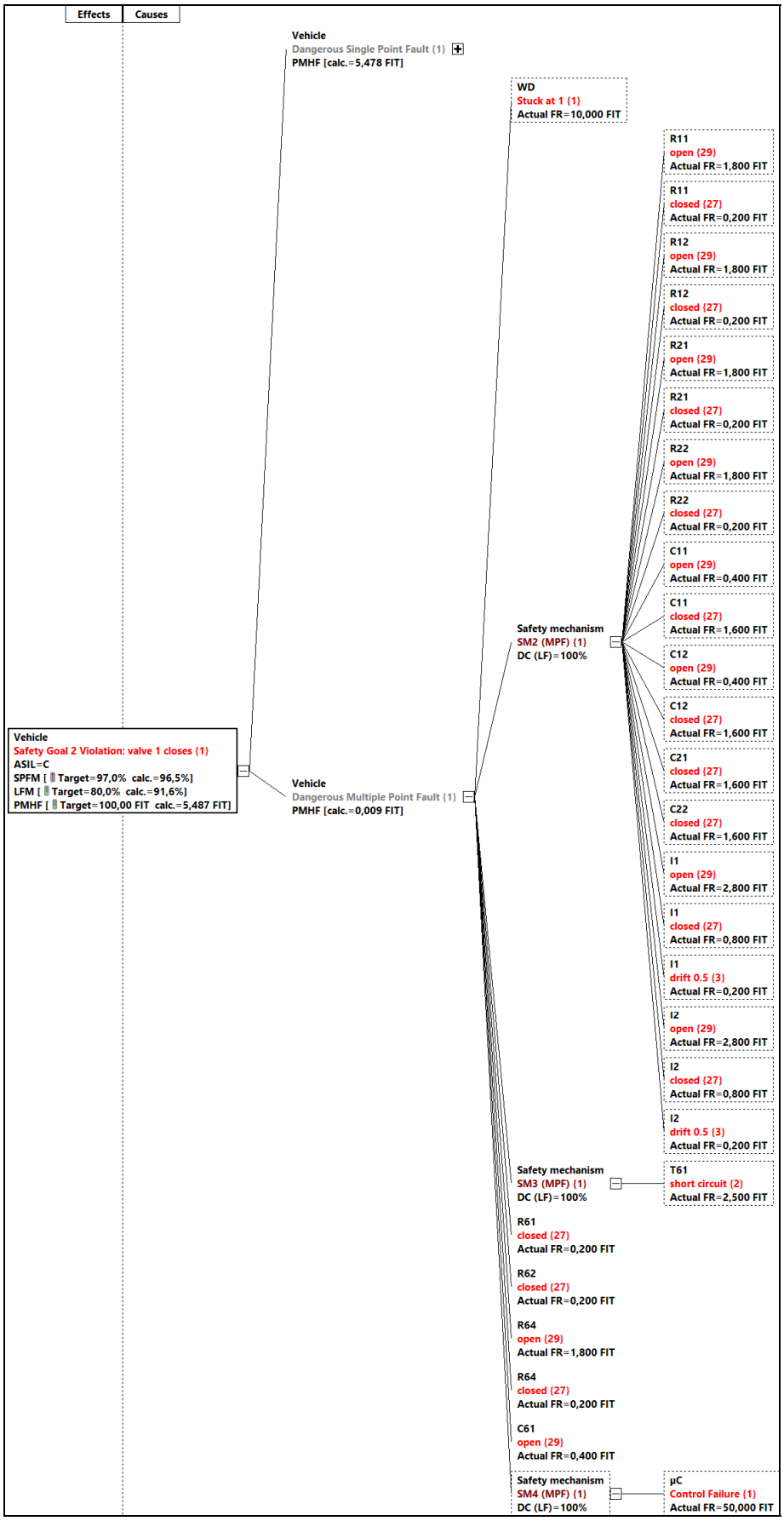
4.1 Failure net for *safety goal 1*



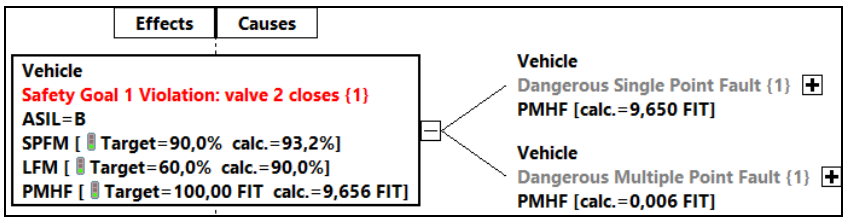


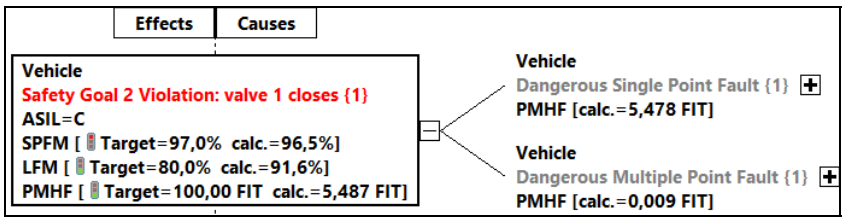
4.2 Failure net for *safety goal 2*




Effects
Causes
Vehicle
Dangerous Single Point Fault {1}
PMHF [calc.=5,478 FIT]
WD
Stuck at 1 {1}
Actual FR=10,000 FIT
R11
open {29}
Actual FR=1,800 FIT
R11
closed {27}
Actual FR=0,200 FIT
R12
open {29}
Actual FR=1,800 FIT
R12
closed {27}
Actual FR=0,200 FIT
R21
open {29}
Actual FR=1,800 FIT
R21
closed {27}
Actual FR=0,200 FIT
R22
open {29}
Actual FR=1,800 FIT
R22
closed {27}
Actual FR=0,200 FIT
C11
open {29}
Actual FR=0,400 FIT
C11
closed {27}
Actual FR=1,600 FIT
C12
open {29}
Actual FR=0,400 FIT
C12
closed {27}
Actual FR=1,600 FIT
C21
closed {27}
Actual FR=1,600 FIT
C22
closed {27}
Actual FR=1,600 FIT
I1
open {29}
Actual FR=2,800 FIT
I1
closed {27}
Actual FR=0,800 FIT
I1
drift 0.5 {3}
Actual FR=0,200 FIT
I2
open {29}
Actual FR=2,800 FIT
I2
closed {27}
Actual FR=0,800 FIT
I2
drift 0.5 {3}
Actual FR=0,200 FIT
Safety mechanism
SM2 (MPF) {1}
DC (LF)=100%
Vehicle
Safety Goal 2 Violation: valve 1 closes {1}
ASIL=C
SPFM [Target=97,0% calc.=96,5%]
LFM [Target=80,0% calc.=91,6%]
PMHF [Target=100,00 FIT calc.=5,487 FIT]
Vehicle
Dangerous Multiple Point Fault {1}
PMHF [calc.=0,009 FIT]
Safety mechanism
SM3 (MPF) {1}
DC (LF)=100%
T61
short circuit {2}
Actual FR=2,500 FIT
R61
closed {27}
Actual FR=0,200 FIT
R62
closed {27}
Actual FR=0,200 FIT
R64
open {29}
Actual FR=1,800 FIT
R64
closed {27}
Actual FR=0,200 FIT
C61
open {29}
Actual FR=0,400 FIT
Safety mechanism
SM4 (MPF) {1}
DC (LF)=100%
µC
Control Failure {1}
Actual FR=50,000 FIT

Step 5, *option 1*: Check the calculation results in the *Failure net* (traffic light) for each safety goal





Step 5, *option 2*: Check the calculation results in the *FMEDA* (traffic light) for each safety goal

5.1 FMEDA for *Safety Goal 1*

APIS Informationstechnologien GmbH

FMEDA Form

safety goal 1: valve 2 shall not be closed for longer than 100ms when the temperature is higher than 100 °C
(Struktur [System])

Created: **08.09.2020**
Modified: **08.09.2020**

Total safety relevant failure rate: **142,0 FIT**
SPFM calc.: **93,2% [Target=90,0%]**
LFM calc.: **90,0% [Target=60,0%]**
Multiple point faults and safe faults: **60,05 FIT + 72,3 FIT = 132,35 FIT**
PMHF calc.: **9,656 FIT [Target=100,00 FIT]**
PMHF (SPF) calc.: **9,65 FIT**
PMHF (SPF) calc.[%]: **99,94**
PMHF (MPF) calc.: **0,006 FIT**
PMHF (MPF) calc. [%]: **0,06**
T(Lifetime) [h]: **10000**

System element	System element [FIT]	Source FIT	Self heating of system element	Source for % value of failure	Function	Failure mode	% value of failure	failure [FIT]	SPF	Safety mechanism (SPF)	DC (SPF) impl. [%]	lambda RF [FIT]	MPF	Safety mechanism (MPF)	DC (LF) impl. [%]	lambda MPF, L [FIT]	lambda MPF, D [FIT]	Ratio PMHF [%]
R3 (1)	3,000				R3 (1)	1.1.1.3.1.a.1 open (29)	30,00	0,900	✓			0,900						9,32
						1.1.1.3.1.a.2 closed (27)	10,00	0,300										
						1.1.1.3.1.a.3 drift 0.5 (3)	30,00	0,900										
						1.1.1.3.1.a.4 drift 2 (3)	30,00	0,900	✓			0,900						9,32
C13 (1)	2,000				C13 (1)	1.1.1.3.2.a.1 open (29)	20,00	0,400	✓			0,400						4,14
						1.1.1.3.2.a.2 closed (27)	80,00	1,600										
R13 (1)	2,000				R13 (1)	1.1.1.3.3.a.1 open (29)	90,00	1,800	✓			1,800						18,64
						1.1.1.3.3.a.2 closed (27)	10,00	0,200	✓			0,200						2,07
R23 (1)	2,000				R23 (1)	1.1.1.3.4.a.1 open (29)	90,00	1,800										
						1.1.1.3.4.a.2 closed (27)	10,00	0,200	✓			0,200						2,07
µC (1)	100,000				µC (1)	1.1.2.1.1.a.1 Control Failure (1)	50,00	50,000	✓	1.2.g.1 SM4 (SPF) (1)	90	5,000	✓	1.2.h.1 SM4 (MPF) (1)	100		45,000	51,78
						1.1.2.1.1.a.2 Safe Failure (1)	50,00	50,000										
WD (1)	20,000				WD (1)	1.1.2.1.2.a.1 Stuck at 1 (1)	50,00	10,000					✓			10,000		0,05
						1.1.2.1.2.a.2 Stuck at 0 (1)	50,00	10,000										
C71 (1)	2,000				C71 (1)	1.1.3.2.2.a.1 open (29)	20,00	0,400					✓			0,400		0,00
						1.1.3.2.2.a.2 closed (27)	80,00	1,600										
R71 (1)	2,000				R71 (1)	1.1.3.2.3.a.1 open (29)	90,00	1,800										
						1.1.3.2.3.a.2 closed (27)	10,00	0,200					✓			0,200		0,00
R72 (1)	2,000				R72 (1)	1.1.3.2.4.a.1 open (29)	90,00	1,800										
						1.1.3.2.4.a.2 closed (27)	10,00	0,200					✓			0,200		0,00
R74 (1)	2,000				R74 (1)	1.1.3.2.6.a.1 open (29)	90,00	1,800					✓			1,800		0,01
						1.1.3.2.6.a.2 closed (27)	10,00	0,200					✓			0,200		0,00
T71 (1)	5,000				T71 (1)	1.1.3.2.7.a.1 open circuit (2	50,00	2,500										
						1.1.3.2.7.a.2 short circuit (2	50,00	2,500	✓	1.2.a.1 SM1 (SPF) (1)	90	0,250	✓	1.2.b.1 SM1 (MPF) (1)	80	0,450	1,800	2,59

5.2 FMEDA for *Safety Goal 2*

APIS Informationstechnologien GmbH

FMEDA Form

safety goal 2: valve 1 shall not be closed for longer than 200ms when the speed is higher than 100 km/h
(Struktur [System])

Created: **08.09.2020**
Modified: **08.09.2020**

Total safety relevant failure rate: **157,0 FIT**
SPFM calc.: **96,5% [Target=97,0%]**
LFM calc.: **91,6% [Target=80,0%]**
Multiple point faults and safe faults: **82,622 FIT + 68,9 FIT = 151,522 FIT**
PMHF calc.: **5,487 FIT [Target=100,00 FIT]**
PMHF (SPF) calc.: **5,478 FIT**
PMHF (SPF) calc.[%]: **99,84**
PMHF (MPF) calc.: **0,009 FIT**
PMHF (MPF) calc. [%]: **0,16**
T(Lifetime) [h]: **10000**

System element	System element [FIT]	Source FIT	Self heating of system element	Source for % value of failure	Function	Failure mode	% value of failure	failure [FIT]	SPF	Safety mechanism (SPF)	DC (SPF) impl. [%]	lambda RF [FIT]	MPF	Safety mechanism (MPF)	DC (LF) impl. [%]	lambda MPF, L [FIT]	lambda MPF, D [FIT]	Ratio PMHF [%]
I1 (1)	4,000				I1 (1)	1.1.1.1.a.1 open (29)	70,00	2,800	✓	1.2.c. 1 SM2 (SPF) (1)	99	0,028	✓	1.2.d. 1 SM2 (MPF) (1)	100		2,772	0,51
						1.1.1.1.a.2 closed (27)	20,00	0,800	✓	1.2.c. 1 SM2 (SPF) (1)	99	0,008	✓	1.2.d. 1 SM2 (MPF) (1)	100		0,792	0,15
						1.1.1.1.a.3 drift 0.5 (3)	5,00	0,200	✓	1.2.c. 1 SM2 (SPF) (1)	99	0,002	✓	1.2.d. 1 SM2 (MPF) (1)	100		0,198	0,04
						1.1.1.1.a.4 drift 2 (3)	5,00	0,200										
C11 (1)	2,000				C11 (1)	1.1.1.2.a.1 open (29)	20,00	0,400	✓	1.2.c. 1 SM2 (SPF) (1)	99	0,004	✓	1.2.d. 1 SM2 (MPF) (1)	100		0,396	0,07
						1.1.1.2.a.2 closed (27)	80,00	1,600	✓	1.2.c. 1 SM2 (SPF) (1)	99	0,016	✓	1.2.d. 1 SM2 (MPF) (1)	100		1,584	0,29
R11 (1)	2,000				R11 (1)	1.1.1.3.a.1 open (29)	90,00	1,800	✓	1.2.c. 1 SM2 (SPF) (1)	99	0,018	✓	1.2.d. 1 SM2 (MPF) (1)	100		1,782	0,33
						1.1.1.3.a.2 closed (27)	10,00	0,200	✓	1.2.c. 1 SM2 (SPF) (1)	99	0,002	✓	1.2.d. 1 SM2 (MPF) (1)	100		0,198	0,04
R21 (1)	2,000				R21 (1)	1.1.1.4.a.1 open (29)	90,00	1,800	✓	1.2.c. 1 SM2 (SPF) (1)	99	0,018	✓	1.2.d. 1 SM2 (MPF) (1)	100		1,782	0,33
						1.1.1.4.a.2 closed (27)	10,00	0,200	✓	1.2.c. 1 SM2 (SPF) (1)	99	0,002	✓	1.2.d. 1 SM2 (MPF) (1)	100		0,198	0,04
C21 (1)	2,000				C21 (1)	1.1.1.5.a.1 open (29)	20,00	0,400										
						1.1.1.5.a.2 closed (27)	80,00	1,600	✓	1.2.c. 1 SM2 (SPF) (1)	99	0,016	✓	1.2.d. 1 SM2 (MPF) (1)	100		1,584	0,29
I2 (1)	4,000				I2 (1)	1.1.2.1.a.1 open (29)	70,00	2,800	✓	1.2.c. 1 SM2 (SPF) (1)	99	0,028	✓	1.2.d. 1 SM2 (MPF) (1)	100		2,772	0,51
						1.1.2.1.a.2 closed (27)	20,00	0,800	✓	1.2.c. 1 SM2 (SPF) (1)	99	0,008	✓	1.2.d. 1 SM2 (MPF) (1)	100		0,792	0,15
						1.1.2.1.a.3 drift 0.5 (3)	5,00	0,200	✓	1.2.c. 1 SM2 (SPF) (1)	99	0,002	✓	1.2.d. 1 SM2 (MPF) (1)	100		0,198	0,04
						1.1.2.1.a.4 drift 2 (3)	5,00	0,200										
C12 (1)	2,000				C12 (1)	1.1.2.2.a.1 open (29)	20,00	0,400	✓	1.2.c. 1 SM2 (SPF) (1)	99	0,004	✓	1.2.d. 1 SM2 (MPF) (1)	100		0,396	0,07
						1.1.2.2.a.2 closed (27)	80,00	1,600	✓	1.2.c. 1 SM2 (SPF) (1)	99	0,016	✓	1.2.d. 1 SM2 (MPF) (1)	100		1,584	0,29
R12 (1)	2,000				R12 (1)	1.1.2.3.a.1 open (29)	90,00	1,800	✓	1.2.c. 1 SM2 (SPF) (1)	99	0,018	✓	1.2.d. 1 SM2 (MPF) (1)	100		1,782	0,33
						1.1.2.3.a.2 closed (27)	10,00	0,200	✓	1.2.c. 1 SM2 (SPF) (1)	99	0,002	✓	1.2.d. 1 SM2 (MPF) (1)	100		0,198	0,04
R22 (1)	2,000				R22 (1)	1.1.2.4.a.1 open (29)	90,00	1,800	✓	1.2.c. 1 SM2 (SPF) (1)	99	0,018	✓	1.2.d. 1 SM2 (MPF) (1)	100		1,782	0,33
						1.1.2.4.a.2 closed (27)	10,00	0,200	✓	1.2.c. 1 SM2 (SPF) (1)	99	0,002	✓	1.2.d. 1 SM2 (MPF) (1)	100		0,198	0,04
C22 (1)	2,000				C22 (1)	1.1.2.5.a.1 open (29)	20,00	0,400										
						1.1.2.5.a.2 closed (27)	80,00	1,600	✓	1.2.c. 1 SM2 (SPF) (1)	99	0,016	✓	1.2.d. 1 SM2 (MPF) (1)	100		1,584	0,29
µC (1)	100,000				µC (1)	1.1.2.1.1.a.1 Control Failure (1)	50,00	50,000	✓	1.2. g.1 SM4 (SPF) (1)	90	5,000	✓	1.2.h. 1 SM4 (MPF) (1)	100		45,000	91,13
						1.1.2.1.1.a.2 Safe Failure (1)	50,00	50,000										
WD (1)	20,000				WD (1)	1.1.2.1.2.a.1 Stuck at 1 (1)	50,00	10,000					✓			10,000		0,13
						1.1.2.1.2.a.2 Stuck at 0 (1)	50,00	10,000										
C61 (1)	2,000				C61 (1)	1.1.3.1.2.a.1 open (29)	20,00	0,400					✓			0,400		0,01
						1.1.3.1.2.a.2 closed (27)	80,00	1,600										
R61 (1)	2,000				R61 (1)	1.1.3.1.3.a.1 open (29)	90,00	1,800										
						1.1.3.1.3.a.2 closed (27)	10,00	0,200					✓			0,200		0,00
R62 (1)	2,000				R62 (1)	1.1.3.1.4.a.1 open (29)	90,00	1,800										
						1.1.3.1.4.a.2 closed (27)	10,00	0,200					✓			0,200		0,00
R64 (1)	2,000				R64 (1)	1.1.3.1.6.a.1 open (29)	90,00	1,800					✓			1,800		0,02
						1.1.3.1.6.a.2 closed (27)	10,00	0,200					✓			0,200		0,00
T61 (1)	5,000				T61 (1)	1.1.3.1.7.a.1 open circuit (2	50,00	2,500										
						1.1.3.1.7.a.2 short circuit (2	50,00	2,500	✓	1.2.e. 1 SM3 (SPF) (1)	90	0,250	✓	1.2.f. 1 SM3 (MPF) (1)	100		2,250	4,56

For further details on the correct use of IQ Software in the area of Functional Safety, you are welcome to participate in our training:

TR06.2 ISO 26262 - Hardware safety analysis (FMEDA) using the IQ-Software

- **Brief introduction to quantitative safety analysis according to ISO 26262: Analysis of single-point and multiple-point failures (note: detailed introduction in seminar TR06.1)**
- **Important terminology and procedures: ASIL, SPFM, LFM, PMHF**
- **Tool-assisted calculation of Functional Safety metrics and comparison of actual/target performance**
- **Consistent, systematic analysis of the item from FMEA to FMEDA and to fault tree analysis (FTA)**
- **Modelling of safety mechanisms (diagnoses) and their malfunctions (latent failure, false failure)**
- **Practical implementation of a Functional Safety project using the training example of "low beam light"**

Systems with electrical and/or electronic components that carry out safety functions are to be assessed with regard to safety aspects (so-called *hardware safety analysis*). For this purpose, you need to create a FMEA (often a System FMEA). Depending on the ASIL classification of the safety goal, you need to additionally calculate the quantitative parameters of the random hardware failures (SPFM, LFM, and PMHF) and verify the compliance with the required target values.

In this seminar, you will be presented an IQ-Software procedure using the example of "low beam light" to use the already modelled system behavior (function and failure nets) from your (System) FMEA to calculate the Functional Safety (FMEDA). Furthermore, you will learn how to use the single-point failures from the FMEA analysis as the starting point of a fault tree analysis (FTA). All three analyses (FMEA, FMEDA, and FTA) are based on a database. Thus, you avoid redundant data management and tool disruption.