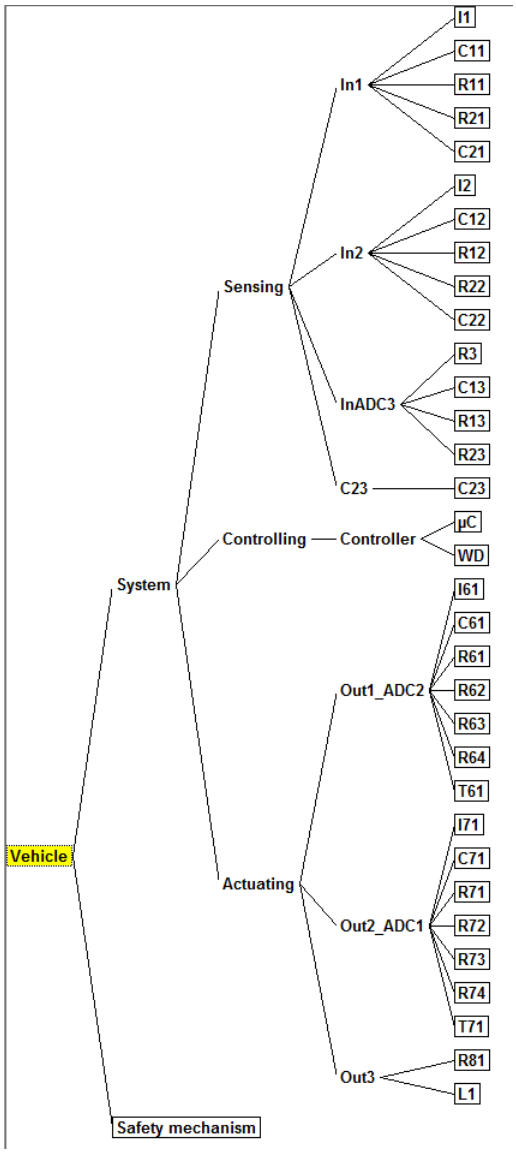
ISO 26262 example (Annex E) with APIS IQ-software

0 Prerequisites for the handling in the fme-example file

- IQ-flavor: APIS IQ-FMEA-PRO or APIS IQ-RM-PRO
- workstation settings | settings: enabled option "Enable mechatronics FMEA"
- structure editor, display options for the structure list: enabled options "Error detections/reactions" and "Parameters Functional Safety"
- failure net editor, display options for Functional Safety: enabled option "Parameters Functional Safety"

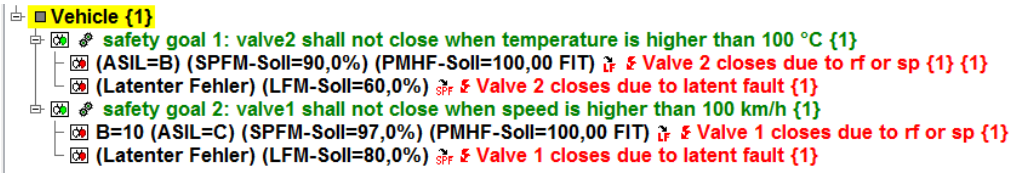
1 Structure tree



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

 © APIS Informationstechnologien GmbH

2 Define safety goals and the target values



3 Define the actual values (FIT-rates) and their proportion (%) in the FMEDA-form

APIS Informationstechnologien GmbH

FMEDA form
C:\Users\User1\Desktop\ISO 26262_DIS Exam

Summe FIT: 207,0000 | Summe FM FIT: 206,0000

No.	System element	FIT	Function	Failure mode	C	% Distr.	FM FIT
1.1.1.1.1	I1	4,0000	I1	open		70,00	2,8000
				closed		20,00	0,8000
				drift 0.5		5,00	0,2000
				drift 2		5,00	0,2000
1.1.1.1.2	C11	2,0000	C11	open		20,00	0,4000
				closed		80,00	1,6000
1.1.1.1.3	R11	2,0000	R11	open		90,00	1,8000
				closed		10,00	0,2000
1.1.1.1.4	R21	2,0000	R21	open		90,00	1,8000
				closed		10,00	0,2000
1.1.1.1.5	C21	2,0000	C21	open		20,00	0,4000
				closed		80,00	1,6000
1.1.1.2.1	I2	4,0000	I2	open		70,00	2,8000
				closed		20,00	0,8000
				drift 0.5		5,00	0,2000
				drift 2		5,00	0,2000
1.1.1.2.2	C12	2,0000	C12	open		20,00	0,4000
				closed		80,00	1,6000

© APIS Informationstechnologien GmbH

1.1.1. 2.3	R12	2,0000	R12	open		90,00	1,8000
				closed		10,00	0,2000
1.1.1. 2.4	R22	2,0000	R22	open		90,00	1,8000
				closed		10,00	0,2000
1.1.1. 2.5	C22	2,0000	C22	open		20,00	0,4000
				closed		80,00	1,6000
1.1.1. 3.1	R3	3,0000	R3	open		30,00	0,9000
				closed		10,00	0,3000
				drift 0.5		30,00	0,9000
				drift 2		30,00	0,9000
1.1.1. 3.2	C13	2,0000	C13	open		20,00	0,4000
				closed		80,00	1,6000
1.1.1. 3.3	R13	2,0000	R13	open		90,00	1,8000
				closed		10,00	0,2000
1.1.1. 3.4	R23	2,0000	R23	open		90,00	1,8000
				closed		10,00	0,2000
1.1.1. 4.1	C23	2,0000	C23	open		20,00	0,4000
				closed		80,00	1,6000
1.1.2. 1.1	µC	100,0000	µC	Control Failure		50,00	50,0000
				Safe Failure		50,00	50,0000
1.1.2. 1.2	WD	20,0000	WD	Stuck at 1		50,00	10,0000
				Stuck at 0		50,00	10,0000

1.1.3. 1.1	I61	5,0000	I61	open		70,00
				close		20,00
1.1.3. 1.2	C61	2,0000	C61	open		20,00
				closed		80,00
1.1.3. 1.3	R61	2,0000	R61	open		90,00
				closed		10,00
1.1.3. 1.4	R62	2,0000	R62	open		90,00
				closed		10,00
1.1.3. 1.5	R63	2,0000	R63	open		90,00
				closed		10,00
1.1.3. 1.6	R64	2,0000	R64	open		90,00
				closed		10,00
1.1.3. 1.7	T61	5,0000	T61	open circuit		50,00
				short circuit		50,00

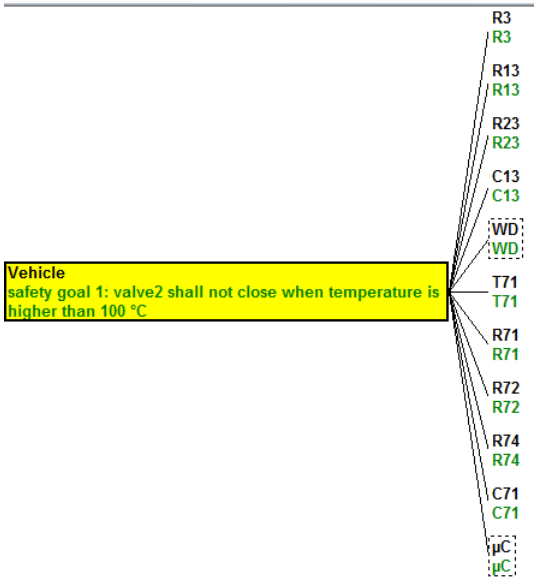
© APIS Informationstechnologien GmbH

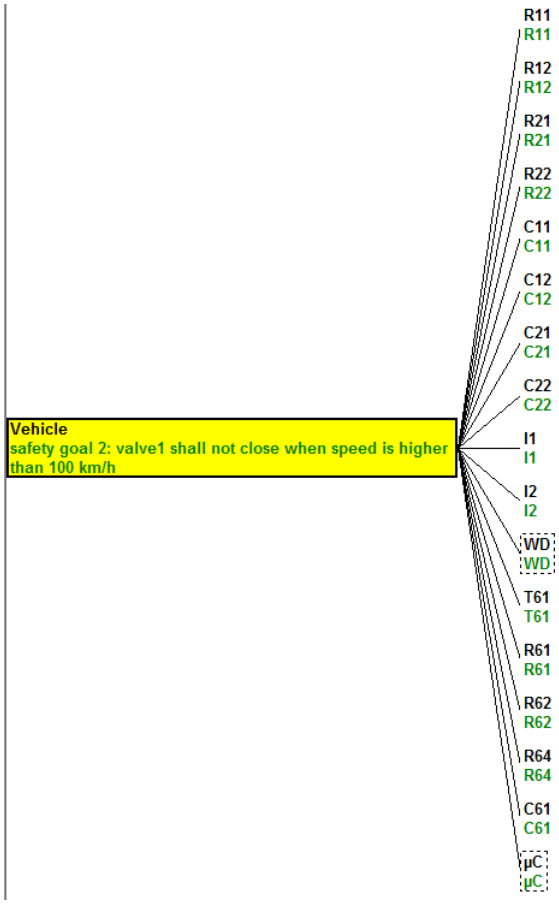
1.1.3.2.1	I71	5,0000	I71	open		70,00	
				close		20,00	
1.1.3.2.2	C71	2,0000	C71	open		20,00	
				closed		80,00	
1.1.3.2.3	R71	2,0000	R71	open		90,00	
				closed		10,00	
1.1.3.2.4	R72	2,0000	R72	open		90,00	
				closed		10,00	
1.1.3.2.5	R73	2,0000	R73	open		90,00	
				closed		10,00	
1.1.3.2.6	R74	2,0000	R74	open		90,00	
				closed		10,00	
1.1.3.2.7	T71	5,0000	T71	open circuit		50,00	
				short circuit		50,00	

1.1.3.3.1	R81	2,0000	R81	open		90,00	1,8000
				closed		10,00	0,2000
1.1.3.3.2	L1	10,0000	L1	open		90,00	9,0000
				closed		10,00	1,0000

© APIS Informationstechnologien GmbH

4 Link the function net in the correct manner for each safety goal





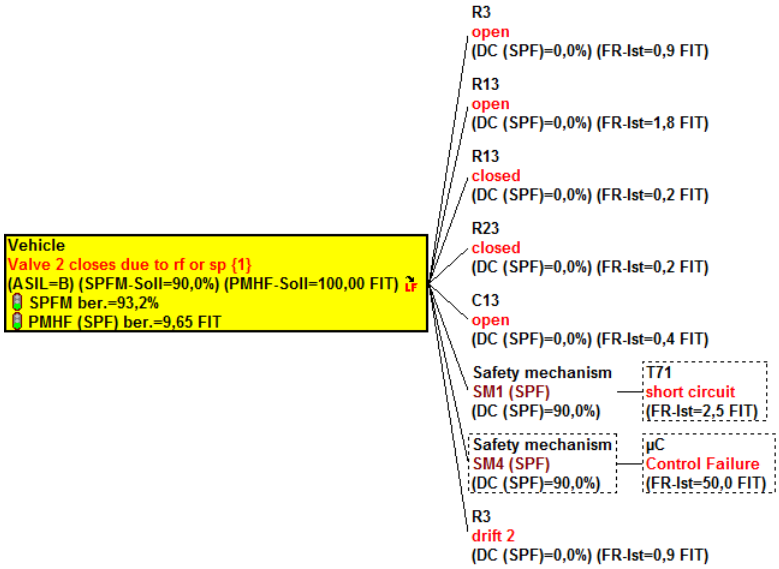
 © APIS Informationstechnologien GmbH

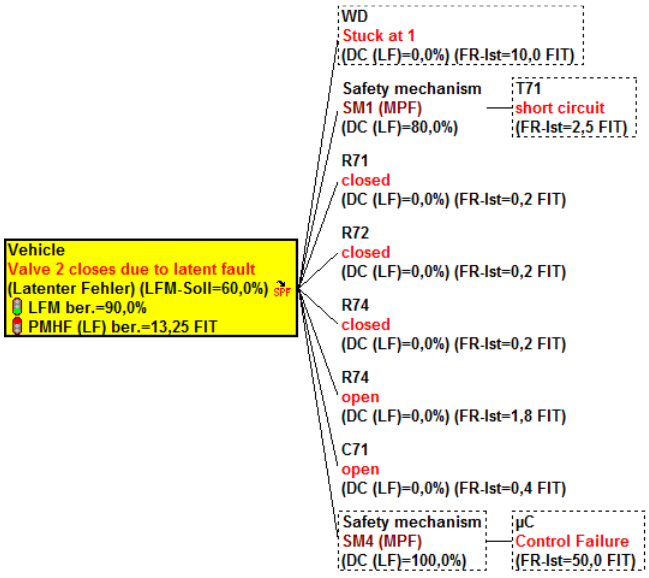
5 Define the safety mechanism and their DC-values

- Safety mechanism {1}
  - SM1 (SPF) {1}
    - (DC (SPF)=90,0%) SM1 (SPF) {1}
  - SM1 (MPF) {1}
    - (DC (LF)=80,0%) SM1 (MPF) {1}
  - SM2 (SPF) {1}
    - (DC (SPF)=99,0%) SM2 (SPF) {1}
  - SM2 (MPF) {1}
    - (DC (LF)=100,0%) SM2 (MPF) {1}
  - SM3 (SPF) {1}
    - (DC (SPF)=90,0%) SM3 (SPF) {1}
  - SM3 (MPF) {1}
    - (DC (LF)=100,0%) SM3 (MPF) {1}
  - SM4 (SPF) {1}
    - (DC (SPF)=90,0%) SM4 (SPF) {1}
  - SM4 (MPF) {1}
    - (DC (LF)=100,0%) SM4 (MPF) {1}

6 Link the failure nets in the correct manner for each safety goal

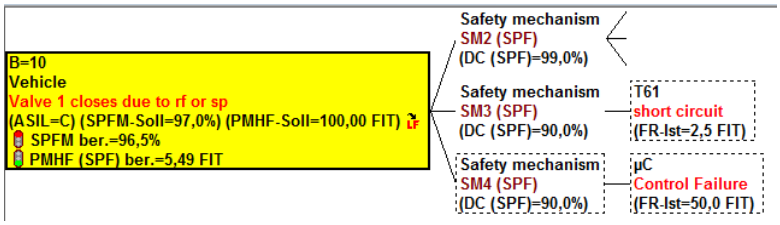
6.1 Failure nets for safety goal 1

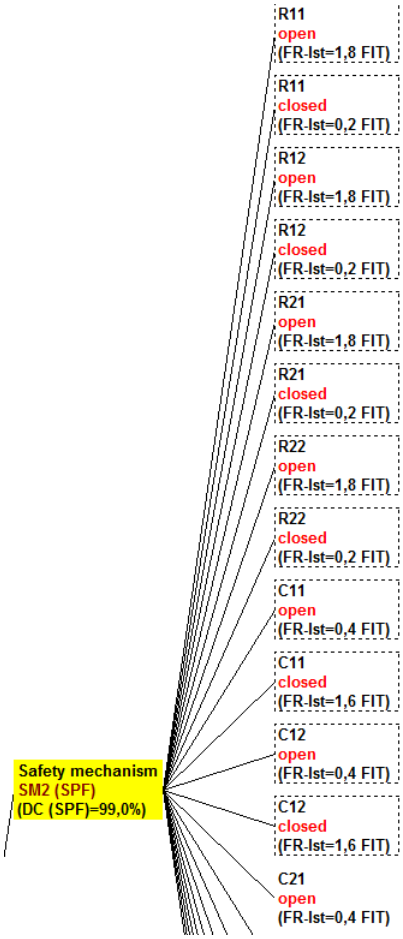




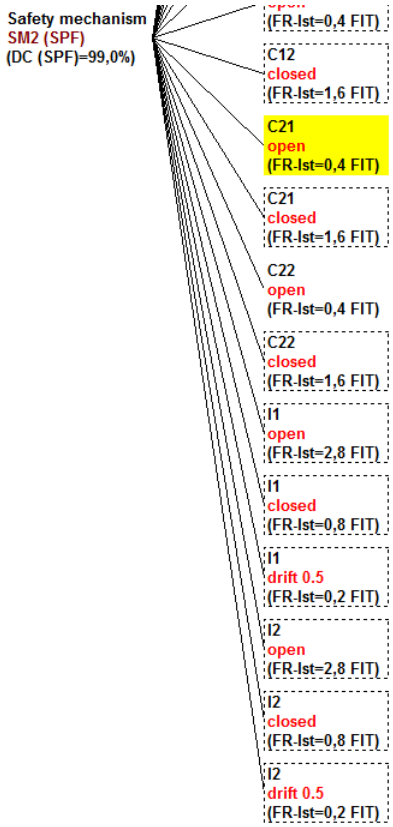
 © APIS Informationstechnologien GmbH

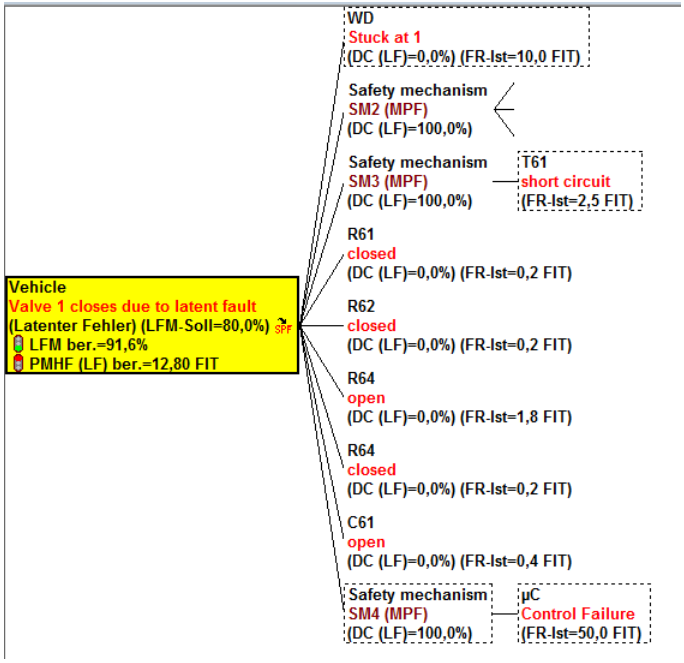
6.2 Failure nets for safety goal 2



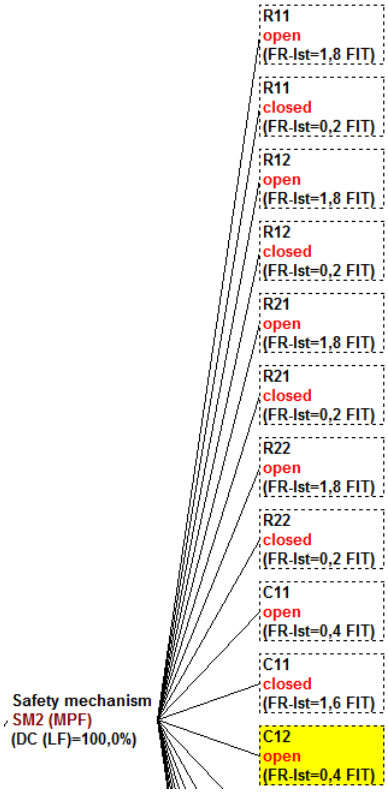


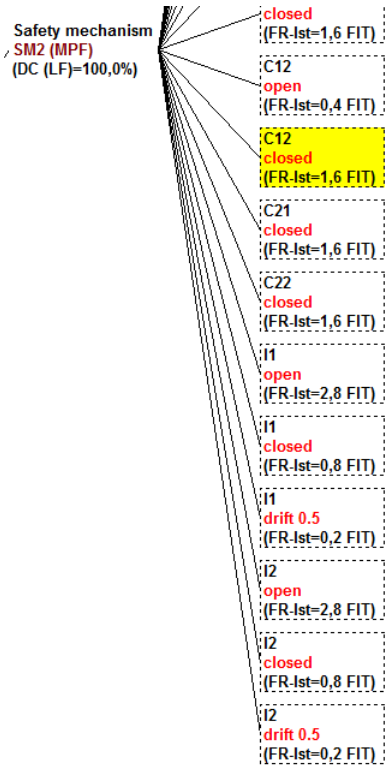
 © APIS Informationstechnologien GmbH





 © APIS Informationstechnologien GmbH

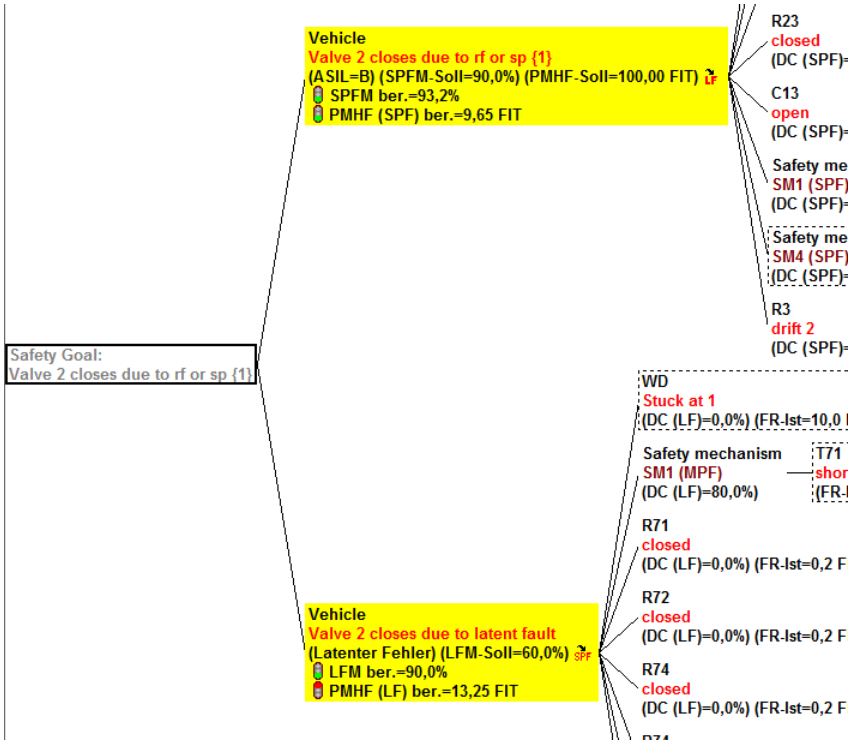




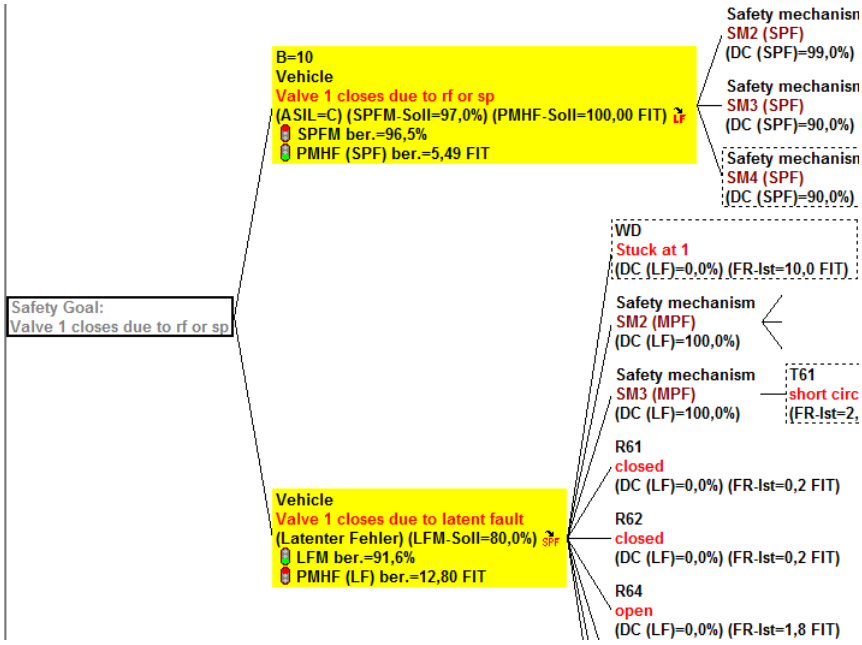
 © APIS Informationstechnologien GmbH

7 Check the calculation results in the failure net (traffic light) for each safety goal

7.1 Failure net (combination of 2 nets) for safety goal 1



7.2 Failure net (combination of 2 nets) for safety goal 2



 © APIS Informationstechnologien GmbH

8 Check the calculation results in the Functional Safety failure table for each safety goal

8.1 Functional Safety failure table for safety goal 1

APIS Informationstechnologien GmbH

Functional Safety - failure table
Valve 2 closes due to rf or sp {1}
ASIL=B

Total failure rate: **142,00 FIT**	SPFM calc.: **93,2%**	LFM calc.: **90,0%**
Mehrfachfehler + Sichere Fehler (47,25 FIT + 85,10 FIT): 132,35 FIT	PMHF (SPF) calc.: **9,65 FIT**	PMHF (LF) calc.: **13,25 FIT**

System element	Function	Failure	Base fault [FIT]	Single point fault			Multiple point fault		
				SPF	DC (SPF) impl.	lambda RF	MPF	DC (LF) impl.	lambda MPFL
µC	µC {1}	1.1.2.1.1.a.1 Control Failure {1}	50,0000	✓	*90,00*	5,0000	✓	100,00	0,0000
µC	µC {1}	1.1.2.1.1.a.2 Safe Failure {1}	50,0000						
C13	C13 {1}	1.1.1.3.2.a.2 closed {27}	1,6000						
C13	C13 {1}	1.1.1.3.2.a.1 open {29}	0,4000	✓	0,00	0,4000			
C71	C71 {1}	1.1.3.2.2.a.2 closed {27}	1,6000						
C71	C71 {1}	1.1.3.2.2.a.1 open {29}	0,4000				✓	0,00	0,4000
R13	R13 {1}	1.1.1.3.3.a.2 closed {27}	0,2000	✓	0,00	0,2000			
R13	R13 {1}	1.1.1.3.3.a.1 open {29}	1,8000	✓	0,00	1,8000			
R23	R23 {1}	1.1.1.3.4.a.2 closed {27}	0,2000	✓	0,00	0,2000			
R23	R23 {1}	1.1.1.3.4.a.1 open {29}	1,8000						
R3	R3 {1}	1.1.1.3.1.a.2 closed {27}	0,3000						
R3	R3 {1}	1.1.1.3.1.a.3 drift 0.5 {3}	0,9000						
R3	R3 {1}	1.1.1.3.1.a.4 drift 2 {3}	0,9000	✓	0,00	0,9000			
R3	R3 {1}	1.1.1.3.1.a.1 open {29}	0,9000	✓	0,00	0,9000			
R71	R71 {1}	1.1.3.2.3.a.2 closed {27}	0,2000				✓	0,00	0,2000
R71	R71 {1}	1.1.3.2.3.a.1 open {29}	1,8000						
R72	R72 {1}	1.1.3.2.4.a.2 closed {27}	0,2000				✓	0,00	0,2000
R72	R72 {1}	1.1.3.2.4.a.1 open {29}	1,8000						
R74	R74 {1}	1.1.3.2.6.a.2 closed {27}	0,2000				✓	0,00	0,2000
R74	R74 {1}	1.1.3.2.6.a.1 open {29}	1,8000				✓	0,00	1,8000
T71	T71 {1}	1.1.3.2.7.a.1 open circuit {2}	2,5000						
T71	T71 {1}	1.1.3.2.7.a.2 short circuit {2}	2,5000	✓	*90,00*	0,2500	✓	80,00	0,4500
WD	WD {1}	1.1.2.1.2.a.2 Stuck at 0 {1}	10,0000						
WD	WD {1}	1.1.2.1.2.a.1 Stuck at 1 {1}	10,0000				✓	0,00	10,0000

8.2 Functional Safety failure table for safety goal 2

APIS Informationstechnologien GmbH

Functional Safety - failure table
Valve 1 closes due to rf or sp
ASIL=C

Total failure rate: **157,00 FIT**	SPFM calc.: **96,5%**	LFM calc.: **91,6%**
Mehrfachfehler + Sichere Fehler (70,61 FIT + 80,90 FIT): 151,51 FIT	PMHF (SPF) calc.: **5,49 FIT**	PMHF (LF) calc.: **12,80 FIT**

System element	Function	Failure	Base fault [FIT]	Single point fault			Multiple point fault		
				SPF	DC (SPF) impl.	lambda RF	MPF	DC (LF) impl.	lambda MPFL
µC	µC {1}	1.1.2.1.1.a.1 Control Failure {1}	50,0000	✓	*90,00*	5,0000	✓	100,00	0,0000
µC	µC {1}	1.1.2.1.1.a.2 Safe Failure {1}	50,0000						
C11	C11 {1}	1.1.1.1.2.a.2 closed {27}	1,6000	✓	*99,00*	0,0160	✓	100,00	0,0000
C11	C11 {1}	1.1.1.1.2.a.1 open {29}	0,4000	✓	*99,00*	0,0040	✓	100,00	0,0000
C12	C12 {1}	1.1.1.2.2.a.2 closed {27}	1,6000	✓	*99,00*	0,0160	✓	100,00	0,0000
C12	C12 {1}	1.1.1.2.2.a.1 open {29}	0,4000	✓	*99,00*	0,0040	✓	100,00	0,0000
C21	C21 {1}	1.1.1.1.5.a.2 closed {27}	1,6000	✓	*99,00*	0,0160	✓	100,00	0,0000
C21	C21 {1}	1.1.1.1.5.a.1 open {29}	0,4000	✓	*99,00*	0,0040			
C22	C22 {1}	1.1.1.2.5.a.2 closed {27}	1,6000	✓	*99,00*	0,0160	✓	100,00	0,0000
C22	C22 {1}	1.1.1.2.5.a.1 open {29}	0,4000	✓	*99,00*	0,0040			
C61	C61 {1}	1.1.3.1.2.a.2 closed {27}	1,6000						
C61	C61 {1}	1.1.3.1.2.a.1 open {29}	0,4000				✓	0,00	0,4000
I1	I1 {1}	1.1.1.1.1.a.2 closed {27}	0,8000	✓	*99,00*	0,0080	✓	100,00	0,0000
I1	I1 {1}	1.1.1.1.1.a.3 drift 0.5 {3}	0,2000	✓	*99,00*	0,0020	✓	100,00	0,0000
I1	I1 {1}	1.1.1.1.1.a.4 drift 2 {3}	0,2000						
I1	I1 {1}	1.1.1.1.1.a.1 open {29}	2,8000	✓	*99,00*	0,0280	✓	100,00	0,0000
I2	I2 {1}	1.1.1.2.1.a.2 closed {27}	0,8000	✓	*99,00*	0,0080	✓	100,00	0,0000
I2	I2 {1}	1.1.1.2.1.a.3 drift 0.5 {3}	0,2000	✓	*99,00*	0,0020	✓	100,00	0,0000
I2	I2 {1}	1.1.1.2.1.a.4 drift 2 {3}	0,2000						
I2	I2 {1}	1.1.1.2.1.a.1 open {29}	2,8000	✓	*99,00*	0,0280	✓	100,00	0,0000
R11	R11 {1}	1.1.1.1.3.a.2 closed {27}	0,2000	✓	*99,00*	0,0020	✓	100,00	0,0000
R11	R11 {1}	1.1.1.1.3.a.1 open {29}	1,8000	✓	*99,00*	0,0180	✓	100,00	0,0000
R12	R12 {1}	1.1.1.2.3.a.2 closed {27}	0,2000	✓	*99,00*	0,0020	✓	100,00	0,0000
R12	R12 {1}	1.1.1.2.3.a.1 open {29}	1,8000	✓	*99,00*	0,0180	✓	100,00	0,0000
R21	R21 {1}	1.1.1.1.4.a.2 closed {27}	0,2000	✓	*99,00*	0,0020	✓	100,00	0,0000
R21	R21 {1}	1.1.1.1.4.a.1 open {29}	1,8000	✓	*99,00*	0,0180	✓	100,00	0,0000
R22	R22 {1}	1.1.1.2.4.a.2 closed {27}	0,2000	✓	*99,00*	0,0020	✓	100,00	0,0000
R22	R22 {1}	1.1.1.2.4.a.1 open {29}	1,8000	✓	*99,00*	0,0180	✓	100,00	0,0000
R61	R61 {1}	1.1.3.1.3.a.2 closed {27}	0,2000				✓	0,00	0,2000
R61	R61 {1}	1.1.3.1.3.a.1 open {29}	1,8000						
R62	R62 {1}	1.1.3.1.4.a.2 closed {27}	0,2000				✓	0,00	0,2000
R62	R62 {1}	1.1.3.1.4.a.1 open {29}	1,8000						
R64	R64 {1}	1.1.3.1.6.a.2 closed {27}	0,2000				✓	0,00	0,2000
R64	R64 {1}	1.1.3.1.6.a.1 open {29}	1,8000				✓	0,00	1,8000
T61	T61 {1}	1.1.3.1.7.a.1 open circuit {2}	2,5000						
T61	T61 {1}	1.1.3.1.7.a.2 short circuit {2}	2,5000	✓	*90,00*	0,2500	✓	100,00	0,0000
WD	WD {1}	1.1.2.1.2.a.2 Stuck at 0 {1}	10,0000						
WD	WD {1}	1.1.2.1.2.a.1 Stuck at 1 {1}	10,0000				✓	0,00	10,0000

© APIS Informationstechnologien GmbH