FUNCTIONAL SAFETY COURSE #4

Dr. FRANCK GALTIE

DIRECTEUR AUTOMOTIVE FUNCTIONAL SAFETY

COMPANY CONFIDENTIAL

SECURE CONNECTIONS
FOR A SMARTER WORLD

General Agenda

- Course #1 :

Functional Safety awareness

- Course #2 :

Brainstorming on power inverter architecture, potential failures and safety mechanisms (ie. safety concept)

- Course #3:

Continue on Safety Concept

- Course #4:

How to prove our concept and assess it

Course #4 agenda

- Functional Safety Analysis
- Confirmation measures

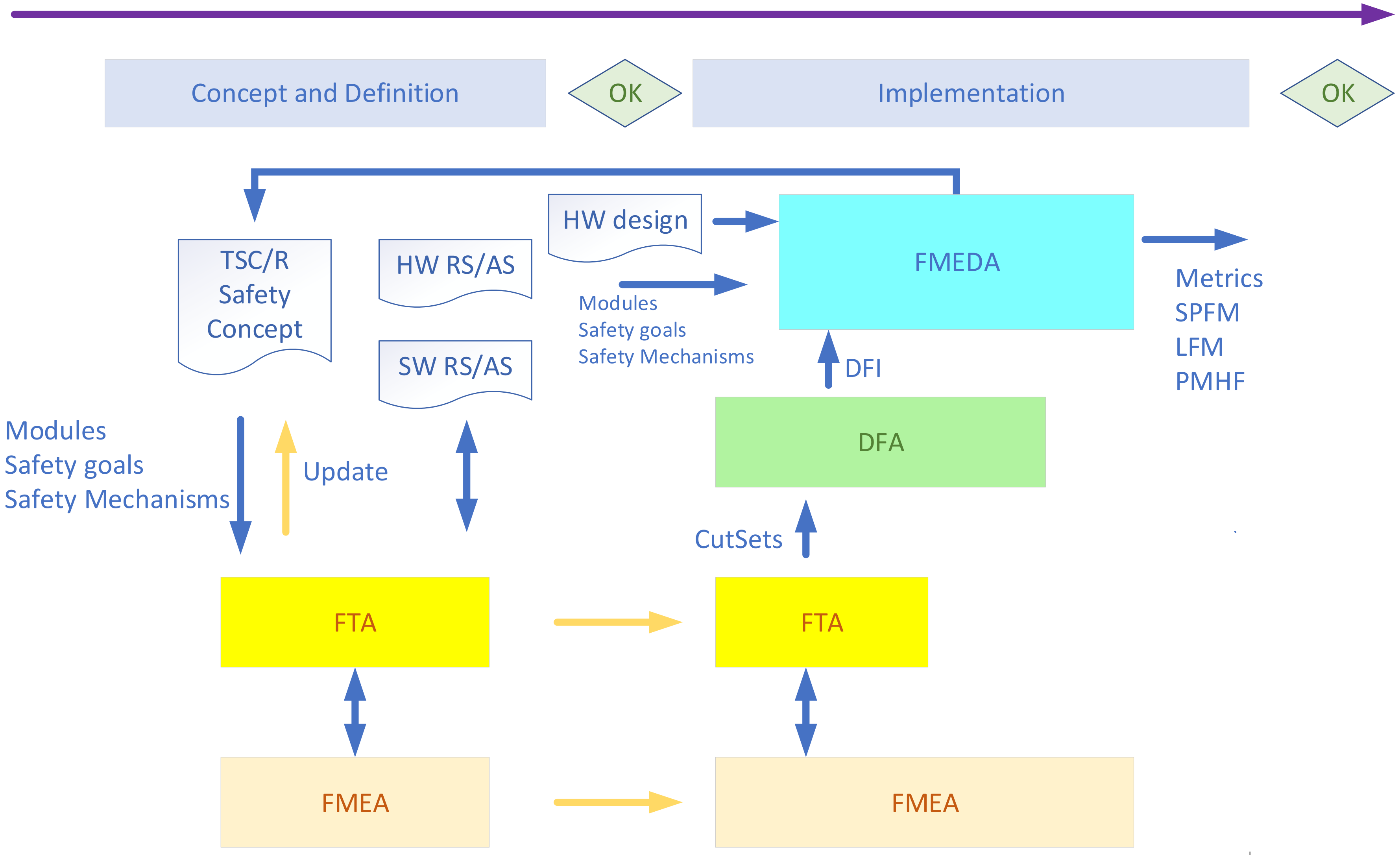
- Internship

01.

SAFETY ANALYSIS
FTA, DFA, FMEDA

Safety Analysis

Safety Analysis Flow



Safety Analysis

Qualitative Safety Analysis

FMEA

inputs

Catalog of failure modes /causes (design, process)

Lessons learnt

HW functions

SW functions

Safety goals/requirements

process

Design, Process FMEA
Pinout FMEA

Severity ranking

Measures for Occurrence removal & Detection at t=0

Safety measures for during operation

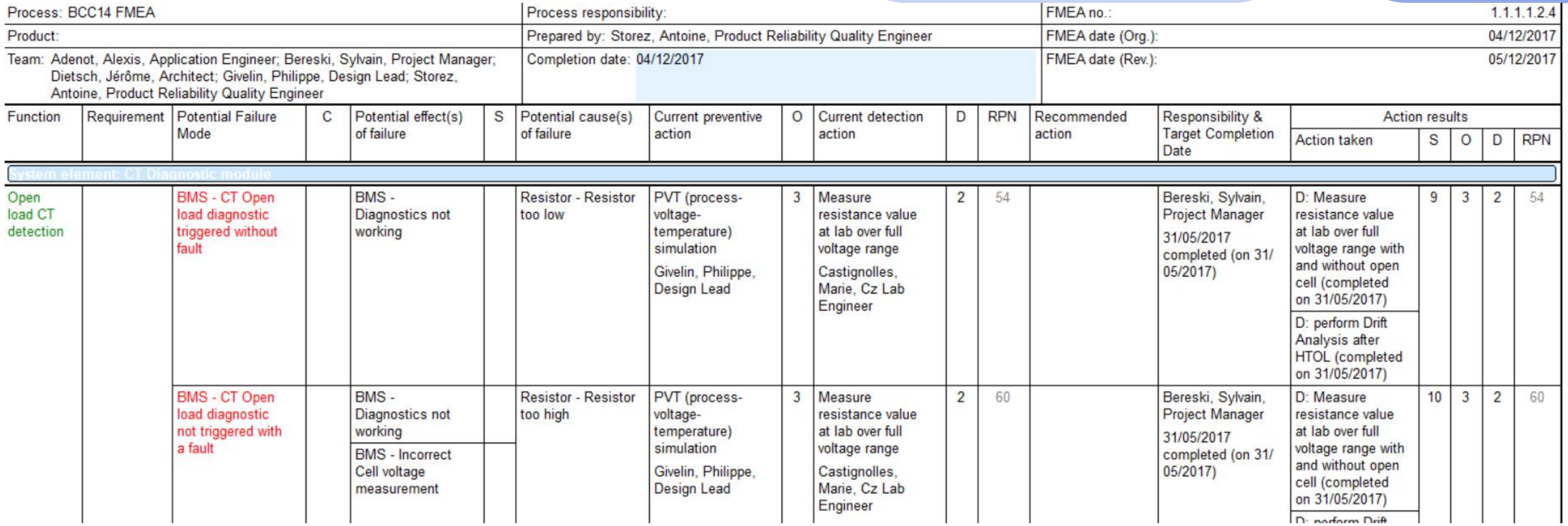
outputs

RPN values

Safety key characteristics

Safety measures evidence

Verification of the Safety Concept and design
(SYS, HW, SW)



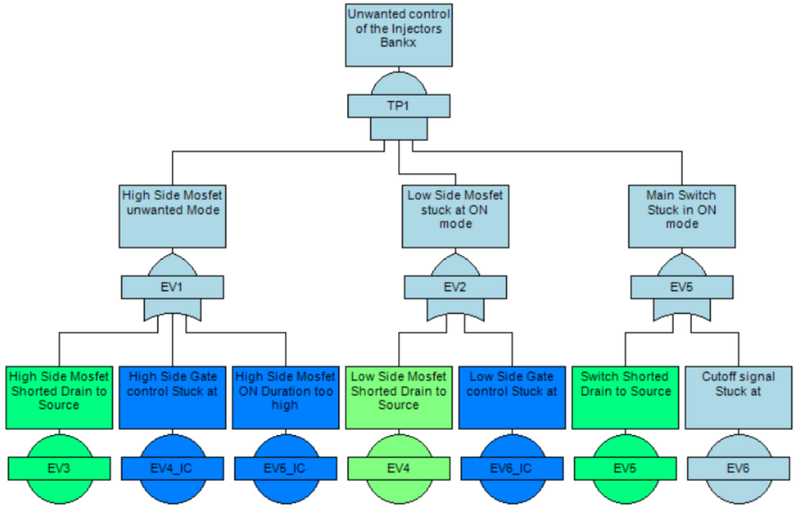
Process: BCC14 FMEA	Process responsibility:	FMEA no.: 1.1.1.1.2.4
Product:	Prepared by: Storez, Antoine, Product Reliability Quality Engineer	FMEA date (Org.): 04/12/2017
Team: Adenot, Alexis, Application Engineer; Bereski, Sylvain, Project Manager; Dietsch, Jérôme, Architect; Givelin, Philippe, Design Lead; Storez, Antoine, Product Reliability Quality Engineer	Completion date: 04/12/2017	FMEA date (Rev.): 05/12/2017

Function	Requirement	Potential Failure Mode	C	Potential effect(s) of failure	S	Potential cause(s) of failure	Current preventive action	O	Current detection action	D	RPN	Recommended action	Responsibility & Target Completion Date	Action results				
														Action taken	S	O	D	RPN
System element: CT Diagnostic module																		
Open load CT detection		BMS - CT Open load diagnostic triggered without fault		BMS - Diagnostics not working		Resistor - Resistor too low	PVT (process-voltage-temperature) simulation Givelin, Philippe, Design Lead	3	Measure resistance value at lab over full voltage range Castignolles, Marie, Cz Lab Engineer	2	54		Bereski, Sylvain, Project Manager 31/05/2017 completed (on 31/05/2017)	D: Measure resistance value at lab over full voltage range with and without open cell (completed on 31/05/2017) D: perform Drift Analysis after HTOL (completed on 31/05/2017)	9	3	2	54
		BMS - CT Open load diagnostic not triggered with a fault		BMS - Diagnostics not working BMS - Incorrect Cell voltage measurement		Resistor - Resistor too high	PVT (process-voltage-temperature) simulation Givelin, Philippe, Design Lead	3	Measure resistance value at lab over full voltage range Castignolles, Marie, Cz Lab Engineer	2	60		Bereski, Sylvain, Project Manager 31/05/2017 completed (on 31/05/2017)	D: Measure resistance value at lab over full voltage range with and without open cell (completed on 31/05/2017) D: perform Drift	10	3	2	60

Safety Analysis

Qualitative Safety Analysis

FTA



Unwanted control of the Injectors Bankx
TP1
High Side Mosfet unwanted Mode
Low Side Mosfet stuck at ON mode
Main Switch Stuck in ON mode
EV1
EV2
EV5
High Side Mosfet Shorted Drain to Source
High Side Gate control Stuck at
High Side Mosfet ON Duration too high
Low Side Mosfet Shorted Drain to Source
Low Side Gate control Stuck at
Switch Shorted Drain to Source
Cutoff signal Stuck at
EV3
EV4_IC
EV5_IC
EV4
EV6_IC
EV5
EV6

inputs

Functional Architecture (preliminary, system, hardware and software)

Set of rules for failure modes

Safety goals/requirements

Safety mechanisms

process

FTA
(System down to basic Elements)

Allocation of Safety mechanisms to faults

Definition of additional required Safety mechanism

outputs

Safe faults
Single Point fault
Common Cause fault

Pairs Fault – SM
Minimal cutsets

Verification of the Safety Concept and design (SYS, HW, SW)

Safety Analysis

Dependent Failure Analysis

DFA

inputs

Pairs faults – SM
Minimal cutsets

Catalog of Dependent Failure Initiators

Co-existing elements

Safety goals/requirements

process

DFA

Shared resources
Cascaded failure

Safety measure identification

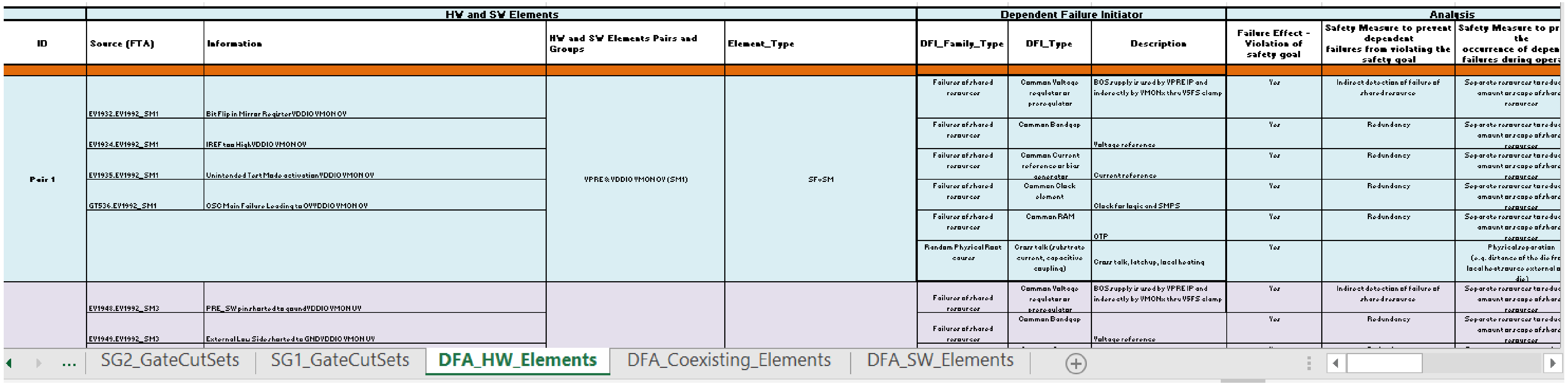
Verification of the Safety measures

outputs

DFI Elements for FMEDA

Verification of the Safety measures with fault injection, etc.

Confirmation for sufficient Independence and freedom from interference



	HW and SW Elements				Dependent Failure Initiator			Analysis		
ID	Source (FTA)	Information	HW and SW Elements Pairs and Groups	Element_Type	DFI_Family_Type	DFI_Type	Description	Failure Effect - Violation of safety goal	Safety Measure to prevent dependent failures from violating the safety goal	Safety Measure to pr the occurrence of depen failures during opera
Pair 1	EV1932.EV1992_SM1	Bit Flip in Mirror Register VDDIO VMON OV	VPRE & VDDIO VMON OV (SM1)	SFvSM	Failures of shared resources	Common Voltage regulator or preregulator	BOS supply is used by VPRE IP and indirectly by VMONx thru V5FS clamp	Yes	Indirect detection of failure of shared resource	Separate resources to reduc amount or scope of shar resources
	EV1934.EV1992_SM1	IREF too High VDDIO VMON OV			Failures of shared resources	Common Bandgap	Voltage reference	Yes	Redundancy	Separate resources to reduc amount or scope of shar resources
	EV1935.EV1992_SM1	Unintended Test Mode activation VDDIO VMON OV			Failures of shared resources	Common Current reference or bias generator	Current reference	Yes	Redundancy	Separate resources to reduc amount or scope of shar resources
	GT536.EV1992_SM1	OSC Main Failure Leading to OV VDDIO VMON OV			Failures of shared resources	Common Clock element	Clock for logic and SMPS	Yes	Redundancy	Separate resources to reduc amount or scope of shar resources
					Failures of shared resources	Common RAM	OTP	Yes	Redundancy	Separate resources to reduc amount or scope of shar resources
					Random Physical Root causes	Cross talk (substrate current, capacitive coupling)	Cross talk, latchup, local heating	Yes		Physical separation (e.g. distance of the die fro local heat source external o die)
	EV1948.EV1992_SM3	PRE_SW pin shorted to gound VDDIO VMON UV			Failures of shared resources	Common Voltage regulator or preregulator	BOS supply is used by VPRE IP and indirectly by VMONx thru V5FS clamp	Yes	Indirect detection of failure of shared resource	Separate resources to reduc amount or scope of shar resources
	EV1949.EV1992_SM3	External Low Side shorted to GND VDDIO VMON UV			Failures of shared resources	Common Bandgap	Voltage reference	Yes	Redundancy	Separate resources to reduc amount or scope of shar resources

Safety Analysis

Quantitative Safety Analysis

FMEDA

inputs

Hardware elements
(close to HW implementation)

Failure rate

Catalog of failure modes

Safety goals/requirements

Safety mechanisms & DC

process

FMEDA

Violation of safety goal directly or in combination with a second fault

Safety mechanism allocation to the fault for Single point Fault and Latent Fault

outputs

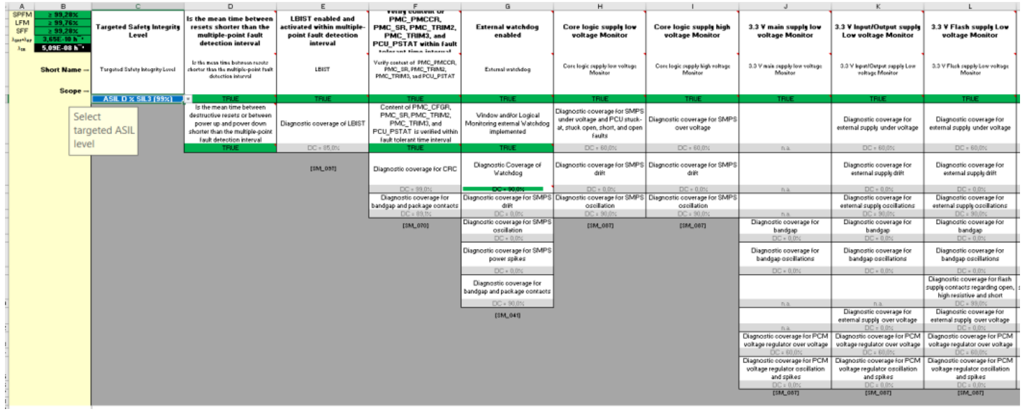
Single Point Fault Metric

Latent Fault Metric

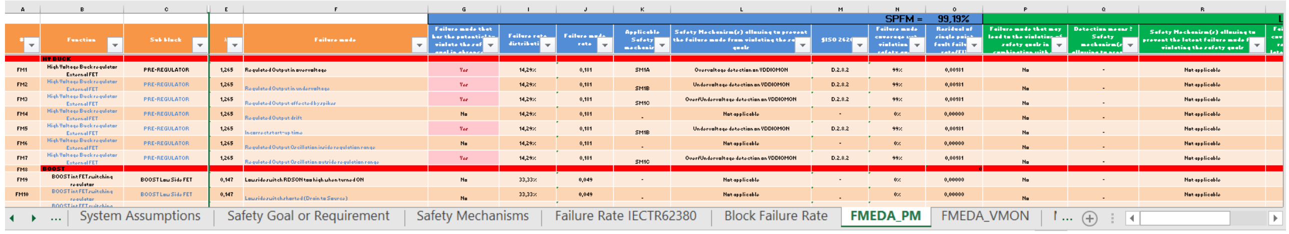
PMHF

(for each Safety goal)

Confirmation for achieved ASIL



A	B	C	D	E	F	G	H	I	J	K	L
SPFM	≥ 99,28%	Targeted Safety Integrity Level	Is the mean time between resets shorter than the multiple-point fault detection interval	LBIST enabled and activated within multiple-point fault detection interval	Verify content of PMC_PMCCR, PMC_SR, PMC_TRIM2, PMC_TRIM3, and PCU_PSTAT within fault tolerant time interval	External watchdog enabled	Core logic supply low voltage Monitor	Core logic supply high voltage Monitor	3.3 V main supply low voltage Monitor	3.3 V Input/Output supply Low voltage Monitor	3.3 V Flash supply Low voltage Monitor
LFM	≥ 99,76%										
SFF	≥ 99,28%										
λ_{SPF+RF}	3,65E-10 h^{-1}										
λ_{SR}	5,09E-08 h^{-1}										
	Short Name →	Targeted Safety Integrity Level	Is the mean time between resets shorter than the multiple-point fault detection interval	LBIST	Verify content of PMC_PMCCR, PMC_SR, PMC_TRIM2, PMC_TRIM3, and PCU_PSTAT	External watchdog	Core logic supply low voltage Monitor	Core logic supply high voltage Monitor	3.3 V main supply low voltage Monitor	3.3 V Input/Output supply Low voltage Monitor	3.3 V Flash supply Low voltage Monitor
	Scope →	ASIL D ≍ SIL3 (99%)	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE
		Select targeted ASIL level	Is the mean time between destructive resets or between power up and power down shorter than the multiple-point fault detection interval TRUE	Diagnostic coverage of LBIST DC = 85,0%	Content of PMC_CFGR, PMC_SR, PMC_TRIM2, PMC_TRIM3, and PCU_PSTAT is verified within fault tolerant time interval TRUE	Window and/or Logical Monitoring external Watchdog implemented TRUE	Diagnostic coverage for SMPS under voltage and PCU stuck-at, stuck open, short, and open faults DC = 60,0%	Diagnostic coverage for SMPS over voltage DC = 60,0%	n.a.	Diagnostic coverage for external supply under voltage DC = 60,0%	Diagnostic coverage for external supply under voltage DC = 60,0%
				[SM_097]	Diagnostic coverage for CRC DC = 99,0%	Diagnostic Coverage of Watchdog DC = 90,0%	Diagnostic coverage for SMPS drift DC = 0,0%	Diagnostic coverage for SMPS drift DC = 0,0%	n.a.	Diagnostic coverage for external supply drift DC = 0,0%	Diagnostic coverage for external supply drift DC = 0,0%
					Diagnostic coverage for bandgap and package contacts DC = 89,1%	Diagnostic coverage for SMPS drift DC = 0,0%	Diagnostic coverage for SMPS oscillation DC = 90,0%	Diagnostic coverage for SMPS oscillation DC = 90,0%	n.a.	Diagnostic coverage for external supply oscillations DC = 90,0%	Diagnostic coverage for external supply oscillations DC = 90,0%
					[SM_070]	Diagnostic coverage for SMPS oscillation DC = 0,0%	[SM_087]	[SM_087]	Diagnostic coverage for bandgap DC = 0,0%	Diagnostic coverage for bandgap DC = 0,0%	Diagnostic coverage for bandgap DC = 0,0%
						Diagnostic coverage for SMPS power spikes DC = 0,0%			Diagnostic coverage for bandgap oscillations DC = 0,0%	Diagnostic coverage for bandgap oscillations DC = 0,0%	Diagnostic coverage for bandgap oscillations DC = 0,0%
						Diagnostic coverage for bandgap and package contacts DC = 90,0%			n.a.	n.a.	Diagnostic coverage for flash supply contacts regarding open, high resistive and short DC = 99,0%
						[SM_041]			n.a.	Diagnostic coverage for external supply over voltage DC = 0,0%	Diagnostic coverage for external supply over voltage DC = 0,0%
									Diagnostic coverage for PCM voltage regulator over voltage DC = 60,0%	Diagnostic coverage for PCM voltage regulator over voltage DC = 60,0%	Diagnostic coverage for PCM voltage regulator over voltage DC = 60,0%
									Diagnostic coverage for PCM voltage regulator oscillation and spikes DC = 0,0%	Diagnostic coverage for PCM voltage regulator oscillation and spikes DC = 0,0%	Diagnostic coverage for PCM voltage regulator oscillation and spikes DC = 0,0%
									[SM_087]	[SM_087]	[SM_087]



SPFM = 99,19%

#	Function	Sub block	λ	Failure mode	Failure mode that has the potential to violate the saf goal in absence	Failure rate distributi	Failure mode rate	Applicable Safety mechanis	Safety Mechanism(s) allowing to prevent the failure mode from violating the sa goals	§ISO 262	Failure mode coverage wrt violation safety go	Residual of single point fault failu rate/FI	Failure mode that may lead to the violation of safety goals in combination with	Detection means ? Safety mechanism(s allowing to prev	Safety Mechanism(s) allowing to prevent the latent failure mode f violating the safety goals
	HV BUCK														
FM1	High Voltage Buck regulator External FET	PRE-REGULATOR	1,265	Regulated Output in overvoltage	Yes	14,29%	0,181	SM1A	Overvoltage detection on VDDIOMON	D.2.8.2	99%	0,00181	No	-	Not applicable
FM2	High Voltage Buck regulator External FET	PRE-REGULATOR	1,265	Regulated Output in undervoltage	Yes	14,29%	0,181	SM1B	Undervoltage detection on VDDIOMON	D.2.8.2	99%	0,00181	No	-	Not applicable
FM3	High Voltage Buck regulator External FET	PRE-REGULATOR	1,265	Regulated Output affected by spikes	Yes	14,29%	0,181	SM1C	Over/Undervoltage detection on VDDIOMON	D.2.8.2	99%	0,00181	No	-	Not applicable
FM4	High Voltage Buck regulator External FET	PRE-REGULATOR	1,265	Regulated Output drift	No	14,29%	0,181	-	Not applicable	-	0%	0,00000	No	-	Not applicable
FM5	High Voltage Buck regulator External FET	PRE-REGULATOR	1,265	Incorrect start-up time	Yes	14,29%	0,181	SM1B	Undervoltage detection on VDDIOMON	D.2.8.2	99%	0,00181	No	-	Not applicable
FM6	High Voltage Buck regulator External FET	PRE-REGULATOR	1,265	Regulated Output Oscillation inside regulation range	No	14,29%	0,181	-	Not applicable	-	0%	0,00000	No	-	Not applicable
FM7	High Voltage Buck regulator External FET	PRE-REGULATOR	1,265	Regulated Output Oscillation outside regulation range	Yes	14,29%	0,181	SM1C	Over/Undervoltage detection on VDDIOMON	D.2.8.2	99%	0,00181	No	-	Not applicable
FM8	BOOST														
FM9	BOOST int FET switching regulator	BOOST Low Side FET	0,147	Low side switch RDSON too high when turned ON	No	33,33%	0,049	-	Not applicable	-	0%	0,00000	No	-	Not applicable
FM10	BOOST int FET switching regulator	BOOST Low Side FET	0,147	Low side switch shorted (Drain to Source)	No	33,33%	0,049	-	Not applicable	-	0%	0,00000	No	-	Not applicable

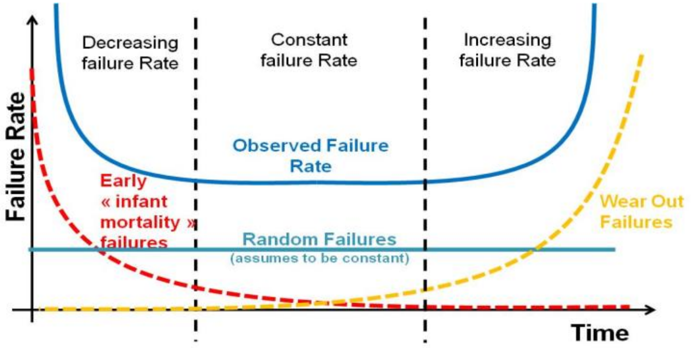
	FMEDA_OP	FMEDA_PM	FMEDA_MON
SPFM	**99,19%**	**99,19%**	**NA**
LFM	**96,00%**	**96,57%**	**95,26%**
PMHF (10^-9)	**0,433**		

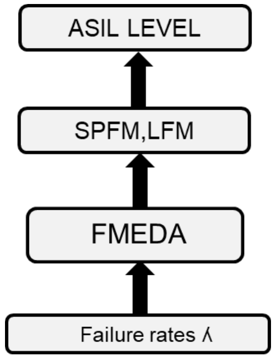
What is Failure Rate and Why Do We Want to Evaluate It?

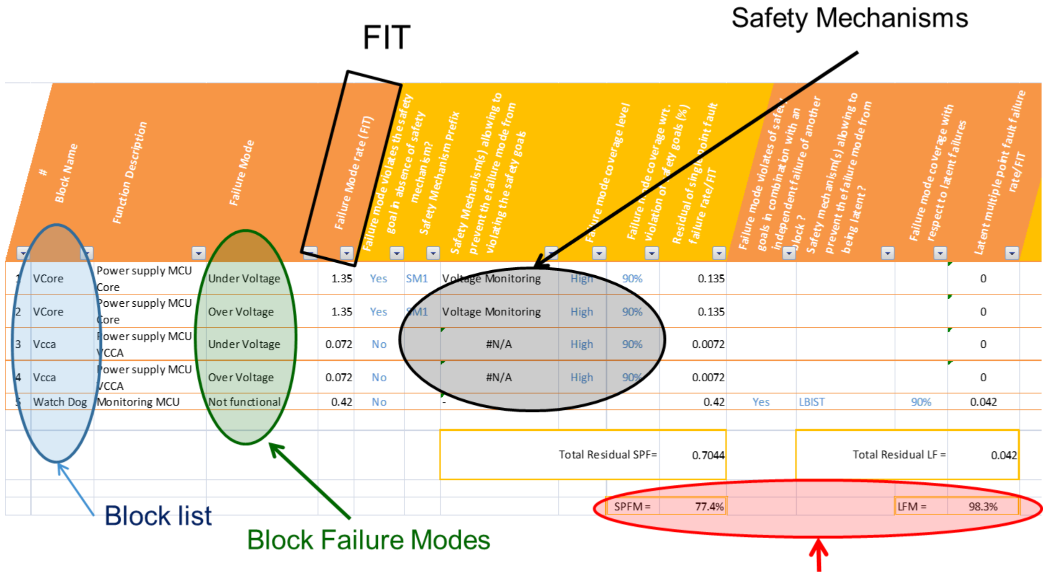
Many standardized models use a “bathtub curve” simplication, which assumes:

- Early life defects are screened by the supplier (Infant mortality).
- The useful lifetime of components must not be exceeded.(wear–out period).

- A constant failure rate is assumed by the probabilistic estimation method and requested by ISO 26262
- The reference conditions must be known : NXP preferred standards is **IEC62380**







#	Block Name	Function Description	Failure Mode	Failure Mode rate (FIT)	Failure mode violates the safety goal in absence of safety mechanism?	Safety Mechanism Prefix	Safety Mechanism(s) allowing to prevent the failure mode from violating the safety goals	Failure mode coverage level	Failure mode coverage wrt. violation of safety goals (%)	Residual of single point fault failure rate/FIT	Failure mode violates of safety goals in combination with an independent failure of another block ?	Safety mechanism(s) allowing to prevent the failure mode from being latent ?	Failure mode coverage with respect to latent failures	Latent multiple point fault failure rate/FIT
1	VCore	Power supply MCU Core	Under Voltage	1.35	Yes	SM1	Voltage Monitoring	High	90%	0.135				0
2	VCore	Power supply MCU Core	Over Voltage	1.35	Yes	SM1	Voltage Monitoring	High	90%	0.135				0
3	Vcca	Power supply MCU VCCA	Under Voltage	0.072	No		#N/A	High	90%	0.0072				0
4	Vcca	Power supply MCU VCCA	Over Voltage	0.072	No		#N/A	High	90%	0.0072				0
5	Watch Dog	Monitoring MCU	Not functional	0.42	No		-			0.42	Yes	LBIST	90%	0.042
									Total Residual SPF=	0.7044			Total Residual LF =	0.042
									SPFM =	77.4%			LFM =	98.3%

Safety Analysis

FMEDA Process

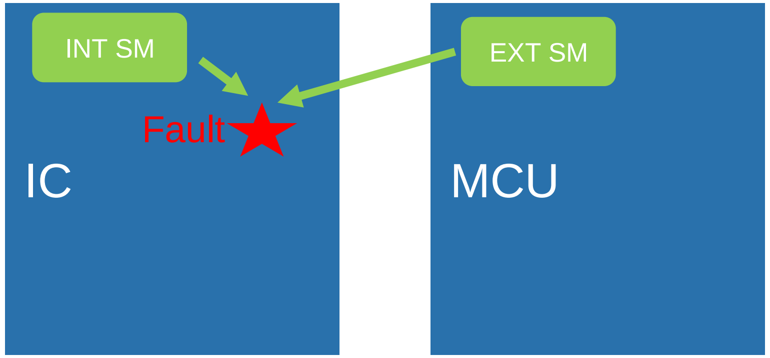
Collection of Safety Mechanisms

Two types of Safety Mechanisms:

1. to prevent faults from being SPF
   Diagnostics shall be effective within the FTTI at system level
2. to prevent faults from being LF
   Diagnostics shall be effective within the MPFTI at system level

Safety Mechanism implementation:

1. embedded in the IC **(INT SM)**
2. external to the IC **(EXT SM)**
3. combined embedded and external
   (for instance requiring MCU decision for the reaction to a safe state)
4. Hardware and or Software solution **(HW SM, SW SM)**



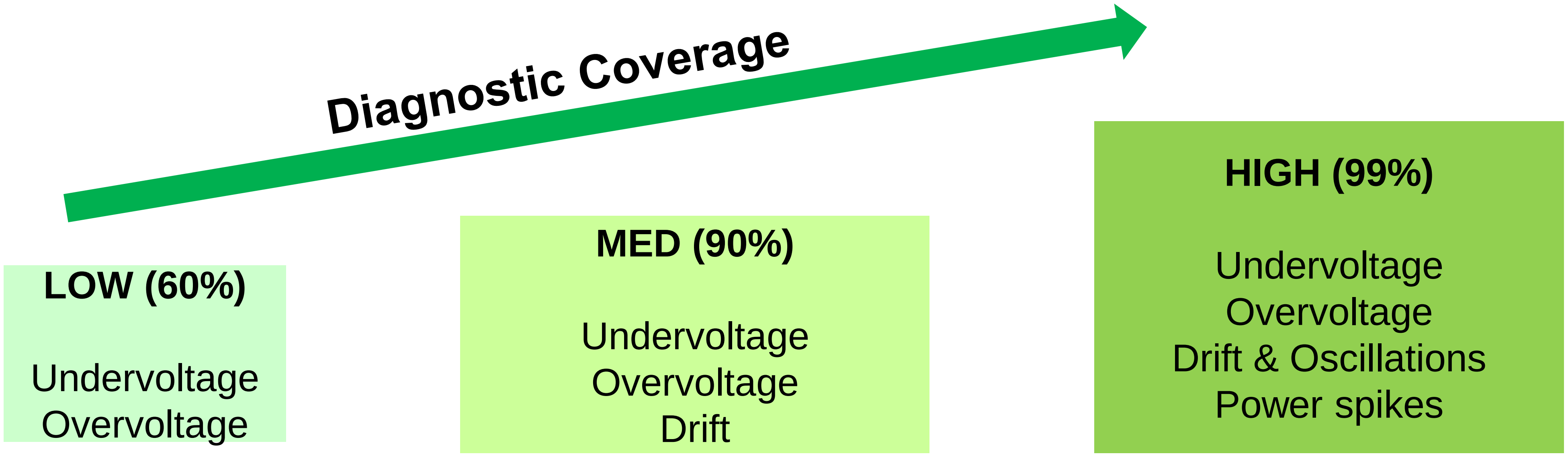
→ Safety mechanism requirements are defined in the safety concept

Safety Analysis

FMEDA Process

Diagnostic Coverage of the Safety Mechanisms

Proportion of the hardware **element failure rate** that is detected or controlled by the implemented **safety mechanisms**



Diagnostic Coverage

LOW (60%)

Undervoltage
Overvoltage

MED (90%)

Undervoltage
Overvoltage
Drift

HIGH (99%)

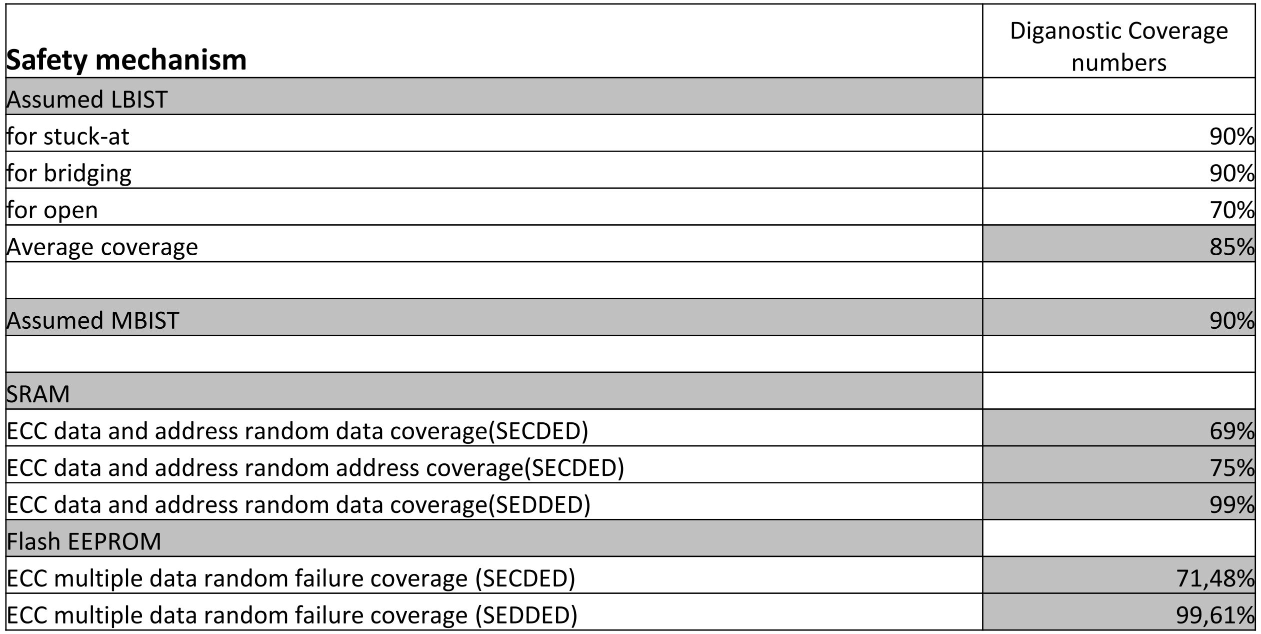
Undervoltage
Overvoltage
Drift & Oscillations
Power spikes

ISO26262 – 5 - Annex D

Safety Analysis

Examples of Safety Mechanisms and Diagnostic Coverage

#	Safety mechanism	§ ISO 26262	Level of Diagnostic coverage	Used?	DC (%)
-	Not applicable	-	-	-	0%
SM1	Overvoltage detection on VDDIOMON	D.2.8.2	High	Yes	99%
SM2	Undervoltage detection on VDDIOMON	D.2.8.2	High	Yes	99%
SM23	CRC check on SPI protocol	D.2.7.6, D.2.7.7, D.2.7.8	High	Yes	99%

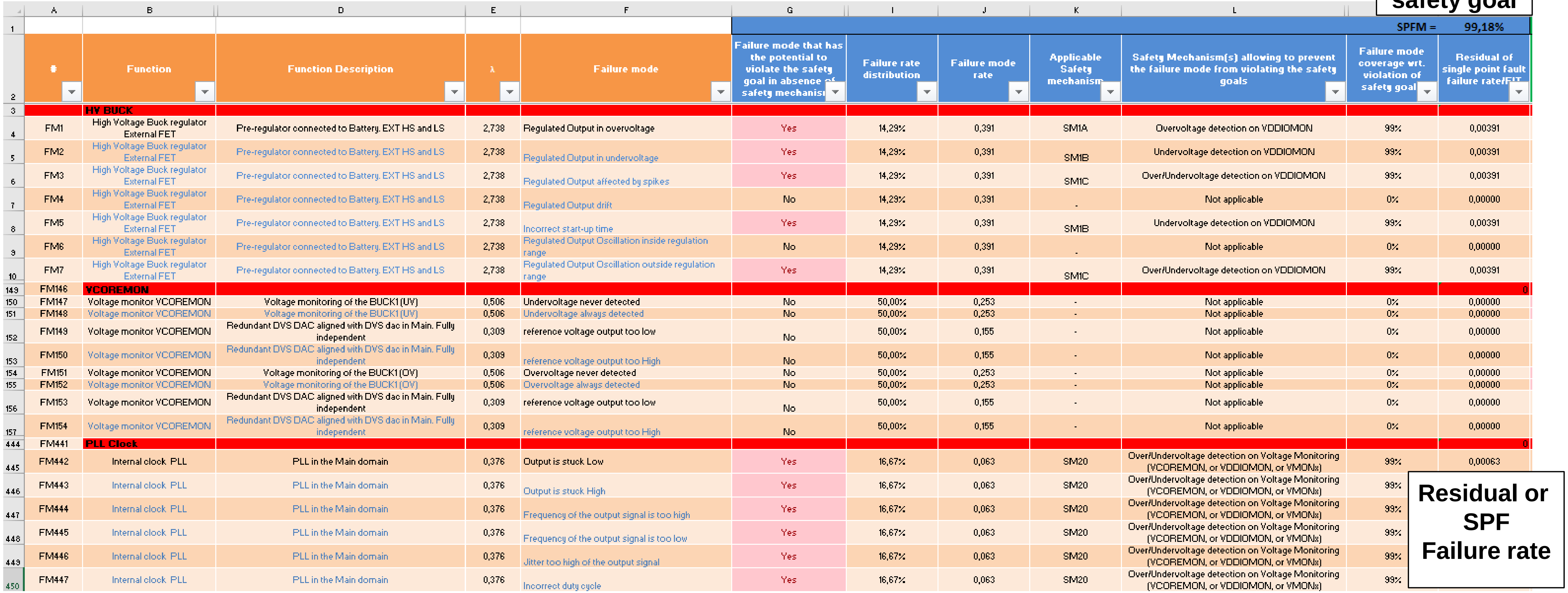


Safety mechanism	Diganostic Coverage numbers
Assumed LBIST	
for stuck-at	90%
for bridging	90%
for open	70%
Average coverage	85%
Assumed MBIST	90%
SRAM	
ECC data and address random data coverage(SECDED)	69%
ECC data and address random address coverage(SECDED)	75%
ECC data and address random data coverage(SEDDED)	99%
Flash EEPROM	
ECC multiple data random failure coverage (SECDED)	71,48%
ECC multiple data random failure coverage (SEDDED)	99,61%

Safety Analysis

Example of FMEDA: SPFM Evaluation

Total SPFM for the safety goal



	A	B	D	E	F	G	I	J	K	L		
1											SPFM =	99,18%
2	#	Function	Function Description	λ	Failure mode	Failure mode that has the potential to violate the safety goal in absence of safety mechanis	Failure rate distribution	Failure mode rate	Applicable Safety mechanism	Safety Mechanism(s) allowing to prevent the failure mode from violating the safety goals	Failure mode coverage wrt. violation of safety goal	Residual of single point fault failure rate/FIT
3		HV BUCK										
4	FM1	High Voltage Buck regulator External FET	Pre-regulator connected to Battery. EXT HS and LS	2,738	Regulated Output in overvoltage	Yes	14,29%	0,391	SM1A	Overvoltage detection on VDDIOMON	99%	0,00391
5	FM2	High Voltage Buck regulator External FET	Pre-regulator connected to Battery. EXT HS and LS	2,738	Regulated Output in undervoltage	Yes	14,29%	0,391	SM1B	Undervoltage detection on VDDIOMON	99%	0,00391
6	FM3	High Voltage Buck regulator External FET	Pre-regulator connected to Battery. EXT HS and LS	2,738	Regulated Output affected by spikes	Yes	14,29%	0,391	SM1C	Over/Undervoltage detection on VDDIOMON	99%	0,00391
7	FM4	High Voltage Buck regulator External FET	Pre-regulator connected to Battery. EXT HS and LS	2,738	Regulated Output drift	No	14,29%	0,391	-	Not applicable	0%	0,00000
8	FM5	High Voltage Buck regulator External FET	Pre-regulator connected to Battery. EXT HS and LS	2,738	Incorrect start-up time	Yes	14,29%	0,391	SM1B	Undervoltage detection on VDDIOMON	99%	0,00391
9	FM6	High Voltage Buck regulator External FET	Pre-regulator connected to Battery. EXT HS and LS	2,738	Regulated Output Oscillation inside regulation range	No	14,29%	0,391	-	Not applicable	0%	0,00000
10	FM7	High Voltage Buck regulator External FET	Pre-regulator connected to Battery. EXT HS and LS	2,738	Regulated Output Oscillation outside regulation range	Yes	14,29%	0,391	SM1C	Over/Undervoltage detection on VDDIOMON	99%	0,00391
149	FM146	VCOREMON										0
150	FM147	Voltage monitor VCOREMON	Voltage monitoring of the BUCK1 (UV)	0,506	Undervoltage never detected	No	50,00%	0,253	-	Not applicable	0%	0,00000
151	FM148	Voltage monitor VCOREMON	Voltage monitoring of the BUCK1 (UV)	0,506	Undervoltage always detected	No	50,00%	0,253	-	Not applicable	0%	0,00000
152	FM149	Voltage monitor VCOREMON	Redundant DVS DAC aligned with DVS dac in Main. Fully independent	0,309	reference voltage output too low	No	50,00%	0,155	-	Not applicable	0%	0,00000
153	FM150	Voltage monitor VCOREMON	Redundant DVS DAC aligned with DVS dac in Main. Fully independent	0,309	reference voltage output too High	No	50,00%	0,155	-	Not applicable	0%	0,00000
154	FM151	Voltage monitor VCOREMON	Voltage monitoring of the BUCK1 (OV)	0,506	Overvoltage never detected	No	50,00%	0,253	-	Not applicable	0%	0,00000
155	FM152	Voltage monitor VCOREMON	Voltage monitoring of the BUCK1 (OV)	0,506	Overvoltage always detected	No	50,00%	0,253	-	Not applicable	0%	0,00000
156	FM153	Voltage monitor VCOREMON	Redundant DVS DAC aligned with DVS dac in Main. Fully independent	0,309	reference voltage output too low	No	50,00%	0,155	-	Not applicable	0%	0,00000
157	FM154	Voltage monitor VCOREMON	Redundant DVS DAC aligned with DVS dac in Main. Fully independent	0,309	reference voltage output too High	No	50,00%	0,155	-	Not applicable	0%	0,00000
444	FM441	PLL Clock										0
445	FM442	Internal clock PLL	PLL in the Main domain	0,376	Output is stuck Low	Yes	16,67%	0,063	SM20	Over/Undervoltage detection on Voltage Monitoring (VCOREMON, or VDDIOMON, or VMONx)	99%	0,00063
446	FM443	Internal clock PLL	PLL in the Main domain	0,376	Output is stuck High	Yes	16,67%	0,063	SM20	Over/Undervoltage detection on Voltage Monitoring (VCOREMON, or VDDIOMON, or VMONx)	99%	
447	FM444	Internal clock PLL	PLL in the Main domain	0,376	Frequency of the output signal is too high	Yes	16,67%	0,063	SM20	Over/Undervoltage detection on Voltage Monitoring (VCOREMON, or VDDIOMON, or VMONx)	99%	
448	FM445	Internal clock PLL	PLL in the Main domain	0,376	Frequency of the output signal is too low	Yes	16,67%	0,063	SM20	Over/Undervoltage detection on Voltage Monitoring (VCOREMON, or VDDIOMON, or VMONx)	99%	
449	FM446	Internal clock PLL	PLL in the Main domain	0,376	Jitter too high of the output signal	Yes	16,67%	0,063	SM20	Over/Undervoltage detection on Voltage Monitoring (VCOREMON, or VDDIOMON, or VMONx)	99%	
450	FM447	Internal clock PLL	PLL in the Main domain	0,376	Incorrect duty cycle	Yes	16,67%	0,063	SM20	Over/Undervoltage detection on Voltage Monitoring (VCOREMON, or VDDIOMON, or VMONx)	99%	

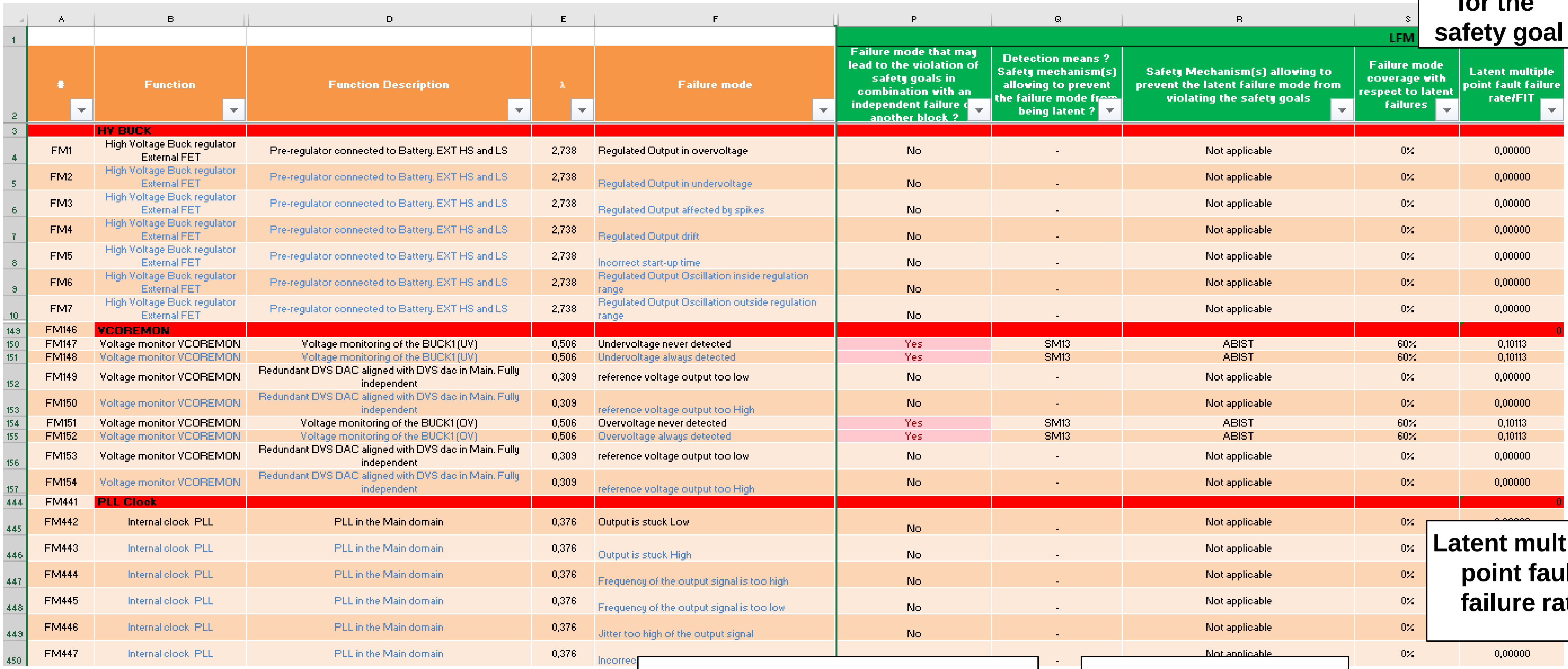
Residual or SPF Failure rate

Violation of the safety goal in absence of SM

Applicable Safety Mechanism and DC

Safety Analysis

Example of FMEDA: LFM Evaluation



	A	B	D	E	F	P	Q	R	S	
1										LFM
2	#	Function	Function Description	λ	Failure mode	Failure mode that may lead to the violation of safety goals in combination with an independent failure o another block ?	Detection means ? Safety mechanism(s) allowing to prevent the failure mode from being latent ?	Safety Mechanism(s) allowing to prevent the latent failure mode from violating the safety goals	Failure mode coverage with respect to latent failures	Latent multiple point fault failure rate/FIT
3		HV BUCK								
4	FM1	High Voltage Buck regulator External FET	Pre-regulator connected to Battery. EXT HS and LS	2,738	Regulated Output in overvoltage	No	-	Not applicable	0%	0,00000
5	FM2	High Voltage Buck regulator External FET	Pre-regulator connected to Battery. EXT HS and LS	2,738	Regulated Output in undervoltage	No	-	Not applicable	0%	0,00000
6	FM3	High Voltage Buck regulator External FET	Pre-regulator connected to Battery. EXT HS and LS	2,738	Regulated Output affected by spikes	No	-	Not applicable	0%	0,00000
7	FM4	High Voltage Buck regulator External FET	Pre-regulator connected to Battery. EXT HS and LS	2,738	Regulated Output drift	No	-	Not applicable	0%	0,00000
8	FM5	High Voltage Buck regulator External FET	Pre-regulator connected to Battery. EXT HS and LS	2,738	Incorrect start-up time	No	-	Not applicable	0%	0,00000
9	FM6	High Voltage Buck regulator External FET	Pre-regulator connected to Battery. EXT HS and LS	2,738	Regulated Output Oscillation inside regulation range	No	-	Not applicable	0%	0,00000
10	FM7	High Voltage Buck regulator External FET	Pre-regulator connected to Battery. EXT HS and LS	2,738	Regulated Output Oscillation outside regulation range	No	-	Not applicable	0%	0,00000
149	FM146	VCOREMON								0
150	FM147	Voltage monitor VCOREMON	Voltage monitoring of the BUCK1 (UV)	0,506	Undervoltage never detected	Yes	SM13	ABIST	60%	0,10113
151	FM148	Voltage monitor VCOREMON	Voltage monitoring of the BUCK1 (UV)	0,506	Undervoltage always detected	Yes	SM13	ABIST	60%	0,10113
152	FM149	Voltage monitor VCOREMON	Redundant DVS DAC aligned with DVS dac in Main. Fully independent	0,309	reference voltage output too low	No	-	Not applicable	0%	0,00000
153	FM150	Voltage monitor VCOREMON	Redundant DVS DAC aligned with DVS dac in Main. Fully independent	0,309	reference voltage output too High	No	-	Not applicable	0%	0,00000
154	FM151	Voltage monitor VCOREMON	Voltage monitoring of the BUCK1 (OV)	0,506	Overvoltage never detected	Yes	SM13	ABIST	60%	0,10113
155	FM152	Voltage monitor VCOREMON	Voltage monitoring of the BUCK1 (OV)	0,506	Overvoltage always detected	Yes	SM13	ABIST	60%	0,10113
156	FM153	Voltage monitor VCOREMON	Redundant DVS DAC aligned with DVS dac in Main. Fully independent	0,309	reference voltage output too low	No	-	Not applicable	0%	0,00000
157	FM154	Voltage monitor VCOREMON	Redundant DVS DAC aligned with DVS dac in Main. Fully independent	0,309	reference voltage output too High	No	-	Not applicable	0%	0,00000
444	FM441	PLL Clock								0
445	FM442	Internal clock PLL	PLL in the Main domain	0,376	Output is stuck Low	No	-	Not applicable	0%	
446	FM443	Internal clock PLL	PLL in the Main domain	0,376	Output is stuck High	No	-	Not applicable	0%	
447	FM444	Internal clock PLL	PLL in the Main domain	0,376	Frequency of the output signal is too high	No	-	Not applicable	0%	
448	FM445	Internal clock PLL	PLL in the Main domain	0,376	Frequency of the output signal is too low	No	-	Not applicable	0%	
449	FM446	Internal clock PLL	PLL in the Main domain	0,376	Jitter too high of the output signal	No	-	Not applicable	0%	
450	FM447	Internal clock PLL	PLL in the Main domain	0,376	Incorrec		-	Not applicable	0%	0,00000

Total LFM for the safety goal

Latent multiple point fault failure rate

Violation of the safety goal in combination with another fault

Applicable Safety Mechanism and DC

02.

FUNCTIONAL SAFETY CONFIRMATION MEASURE

ISO 26262 Functional Safety Audit/Assessment

Requirement	Confirmation review	Functional safety audit	Functional safety assessment
Subject for evaluation	Work product	Implementation of the processes required for functional safety	Item as described in the item definition in accordance with ISO 26262-3:—, Clause 5
Result	Confirmation review report[a]	Functional safety audit report[a] in accordance with 6.4.8	Functional safety assessment report in accordance with 6.4.9
Responsibility of the persons that perform the confirmation measure	**Evaluation of the compliance of the work product with the corresponding requirements of ISO 26262**	**Evaluation of the implementation of the required processes**	**Evaluation of the achieved functional safety**

Process or technical

Process review

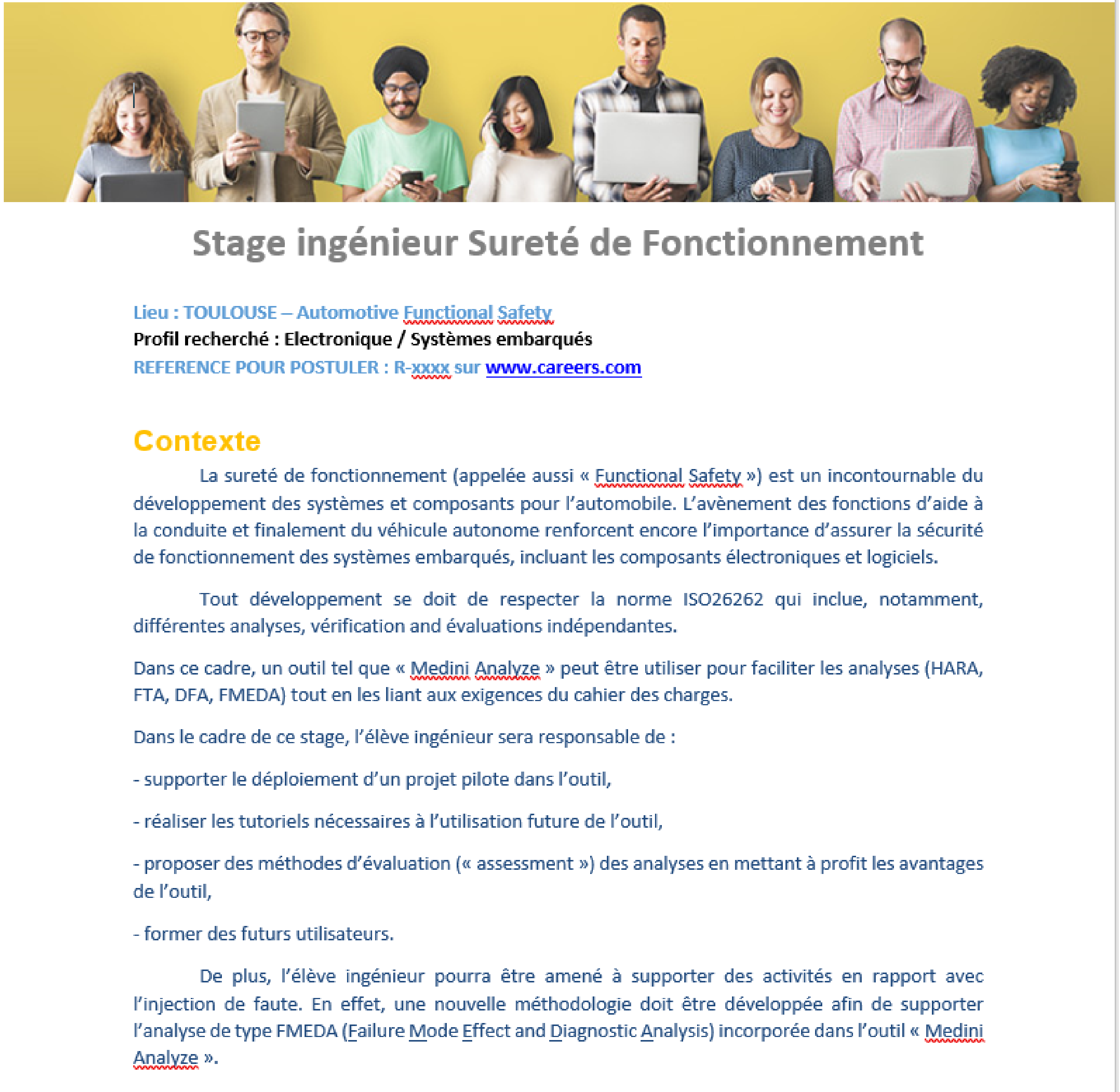
Technical review
Peer review

Table 2 — Procedural requirements for confirmation measures - Extract from ISO26262 - 2

03.

INTERNSHIP

SECURE CONNECTIONS
FOR A SMARTER WORLD



Stage ingénieur Sureté de Fonctionnement

Lieu : TOULOUSE – Automotive Functional Safety
Profil recherché : Electronique / Systèmes embarqués
REFERENCE POUR POSTULER : R-xxxx sur www.careers.com

Contexte

La sureté de fonctionnement (appelée aussi « Functional Safety ») est un incontournable du développement des systèmes et composants pour l'automobile. L'avènement des fonctions d'aide à la conduite et finalement du véhicule autonome renforcent encore l'importance d'assurer la sécurité de fonctionnement des systèmes embarqués, incluant les composants électroniques et logiciels.

Tout développement se doit de respecter la norme ISO26262 qui inclue, notamment, différentes analyses, vérification and évaluations indépendantes.

Dans ce cadre, un outil tel que « Medini Analyze » peut être utiliser pour faciliter les analyses (HARA, FTA, DFA, FMEDA) tout en les liant aux exigences du cahier des charges.

Dans le cadre de ce stage, l'élève ingénieur sera responsable de :

- supporter le déploiement d'un projet pilote dans l'outil,

- réaliser les tutoriels nécessaires à l'utilisation future de l'outil,

- proposer des méthodes d'évaluation (« assessment ») des analyses en mettant à profit les avantages de l'outil,

- former des futurs utilisateurs.

De plus, l'élève ingénieur pourra être amené à supporter des activités en rapport avec l'injection de faute. En effet, une nouvelle méthodologie doit être développée afin de supporter l'analyse de type FMEDA (Failure Mode Effect and Diagnostic Analysis) incorporée dans l'outil « Medini Analyze ».

SECURE CONNECTIONS
FOR A SMARTER WORLD

NXP and the NXP logo are trademarks of NXP B.V. All other product or service names are the property of their respective owners. © 2018 NXP B.V.