

Making ISO26262 Functional Safety Verification a Natural Extension of Functional Verification

Andrew Betts, Verification Engineer, Arm

Ann Keffer, Product Management Director,
Functional Safety, Cadence Design Systems

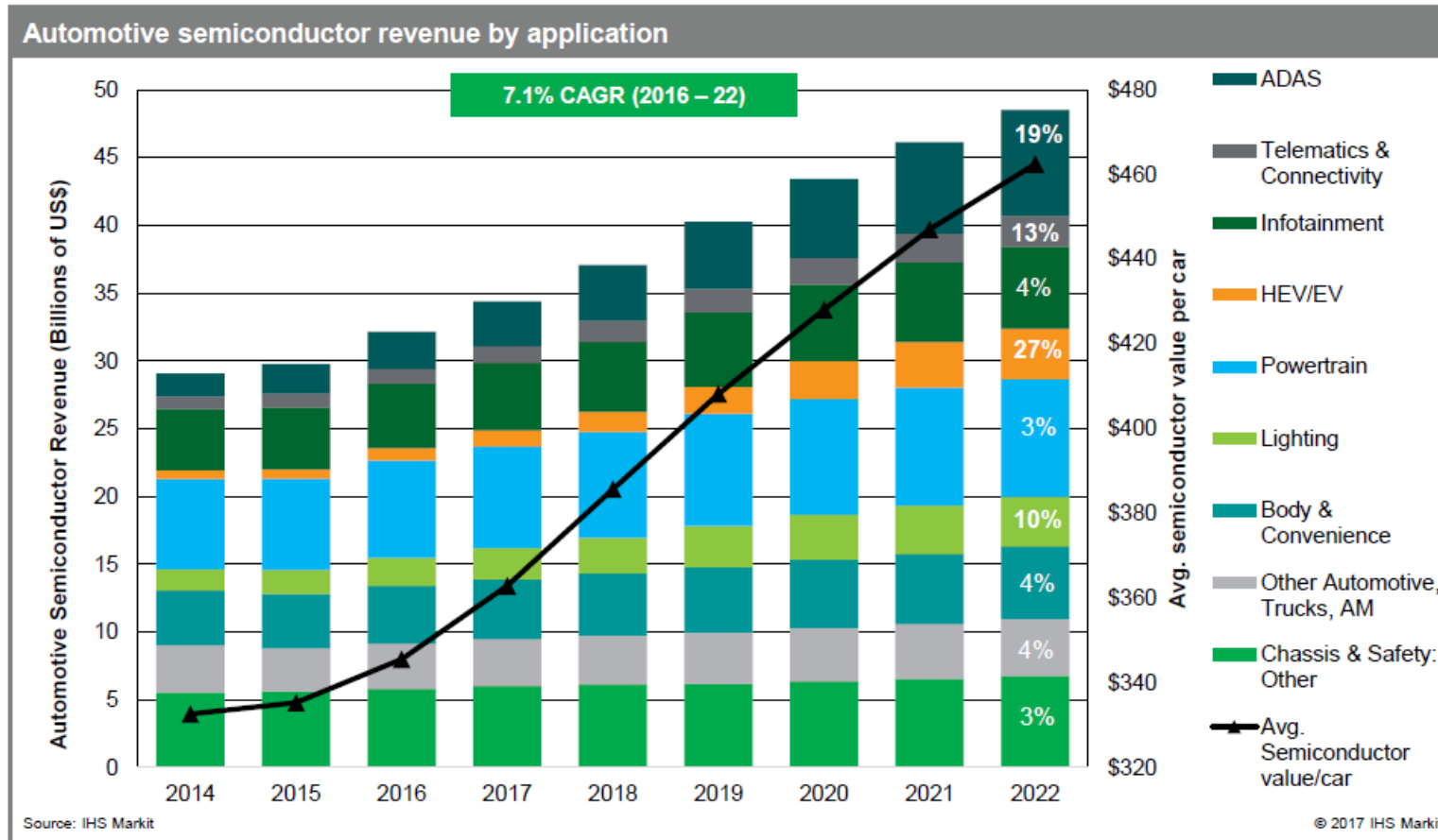
 cadence[®]

 arm

Agenda

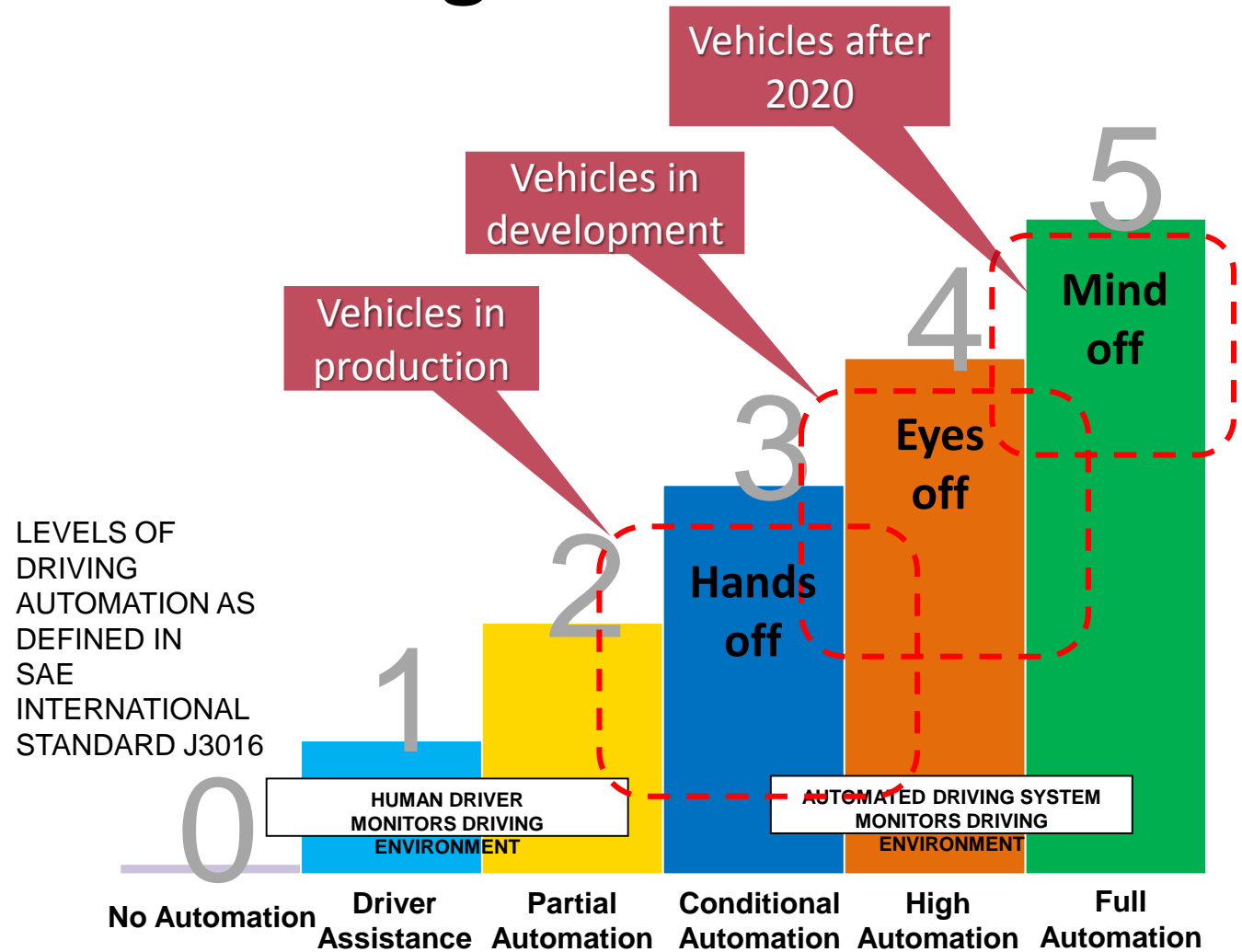
- Market landscape
- Introduction into functional safety
- Why the FMEDA is important
- Functional verification and Safety verification
- Arm[®] processor design description
- Arm Safety Package
- FMEDA Methodology
- Importance of safety campaigns for Arm's STL
- Validation of the FMEDA
- Arm's safety flow
- Q&A
- Demo

Automotive Semiconductor Growth

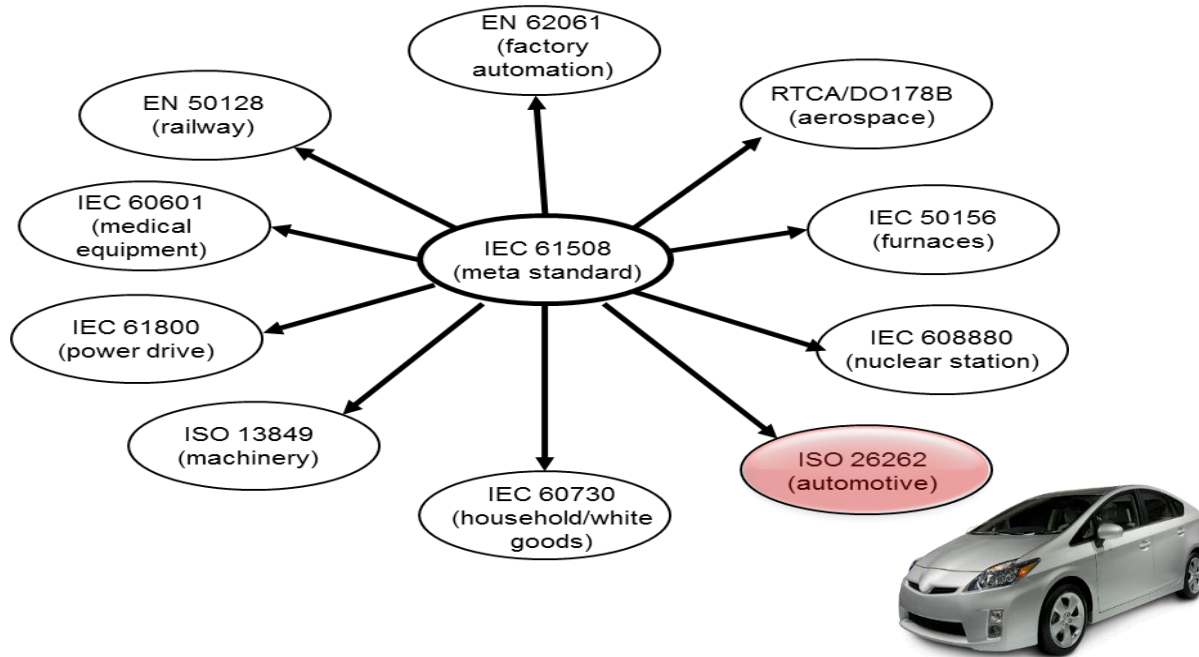


Autonomous Driving

- Amount of electronics is growing fast
- (ADAS) based on complex SoCs to enable high-performance computing
- Safety critical ADAS applications have stringent requirements on
 - Functional safety
 - Security
 - Reliability

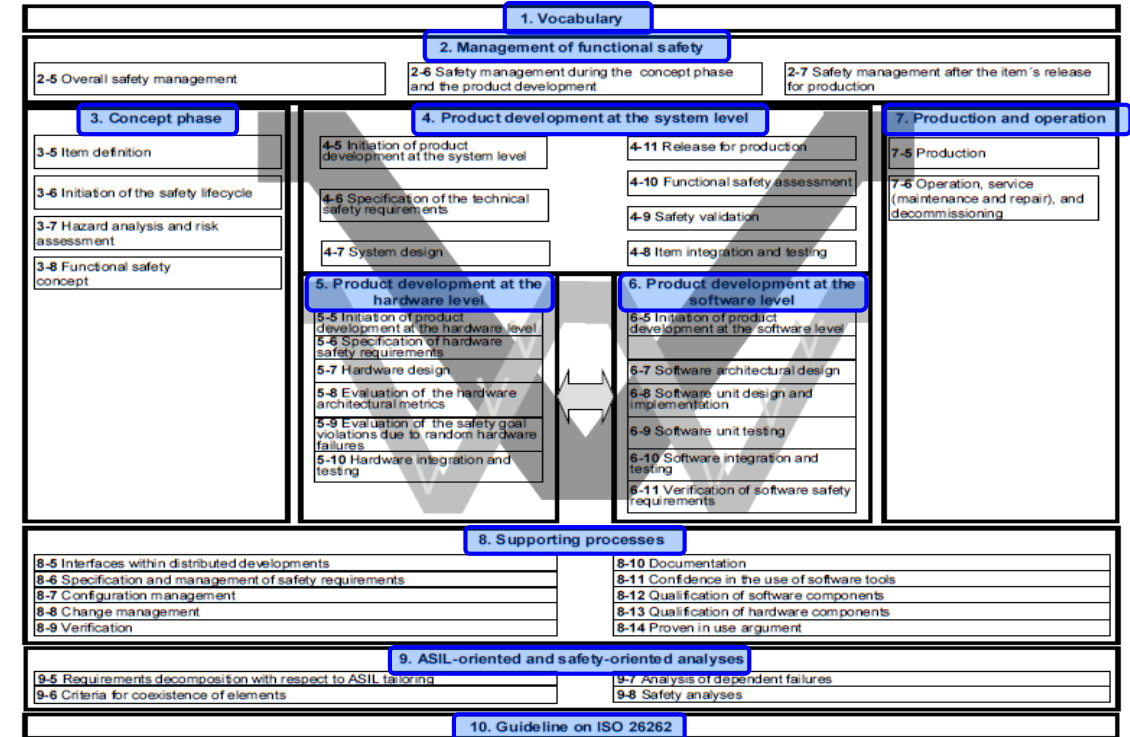


Functional Safety Standards



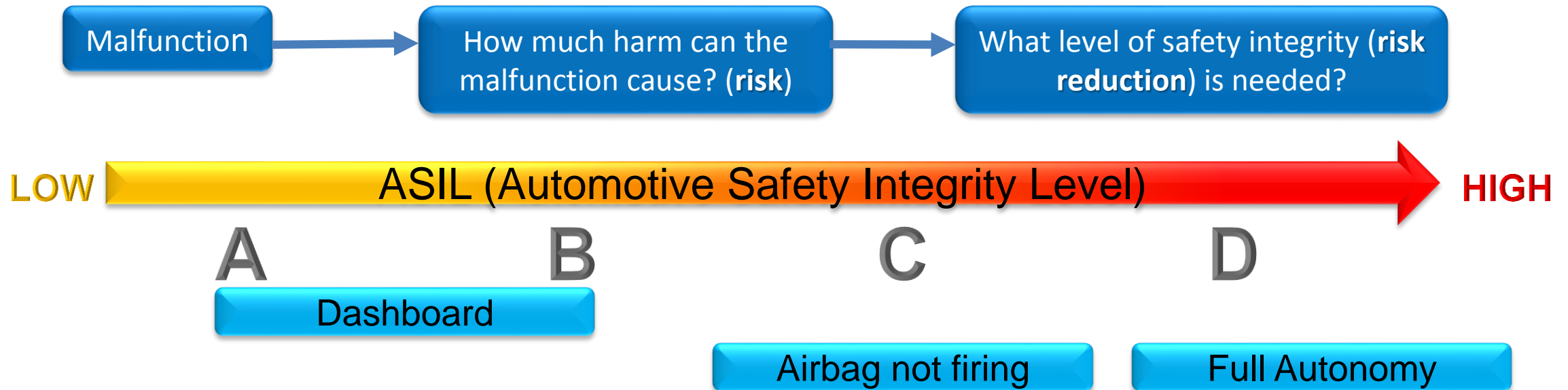
ISO 26262 defines

- Processes to follow
- Hardware/software performance to achieve
- Safety documentation to produce
- Software tools compliance process



Functional Safety Definition—ISO 26262

“Absence of unreasonable **risk** due to **hazards** caused by **malfunctioning** behavior of electrical and/or electronic systems” (ISO 26262)



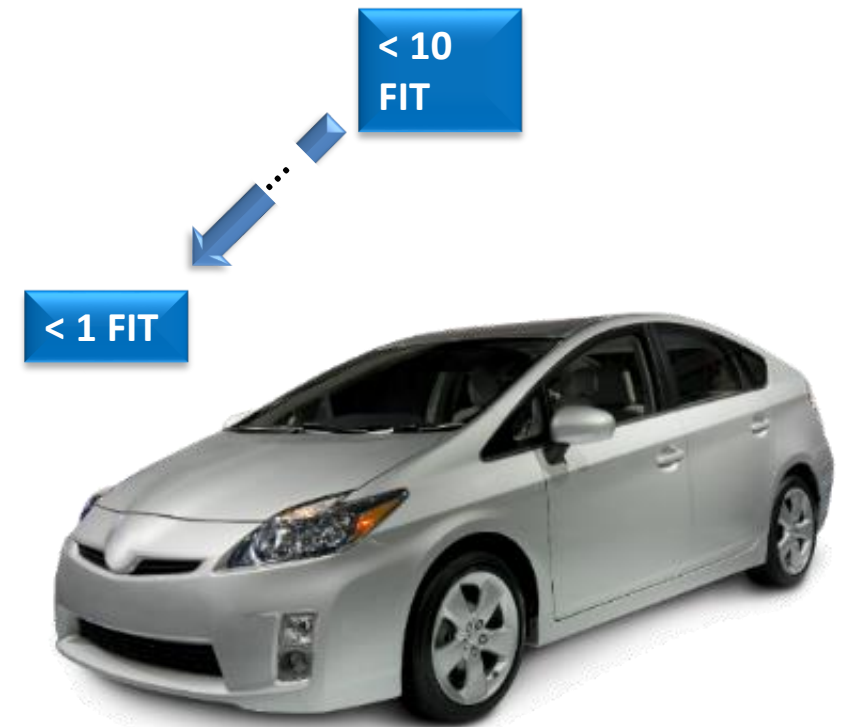
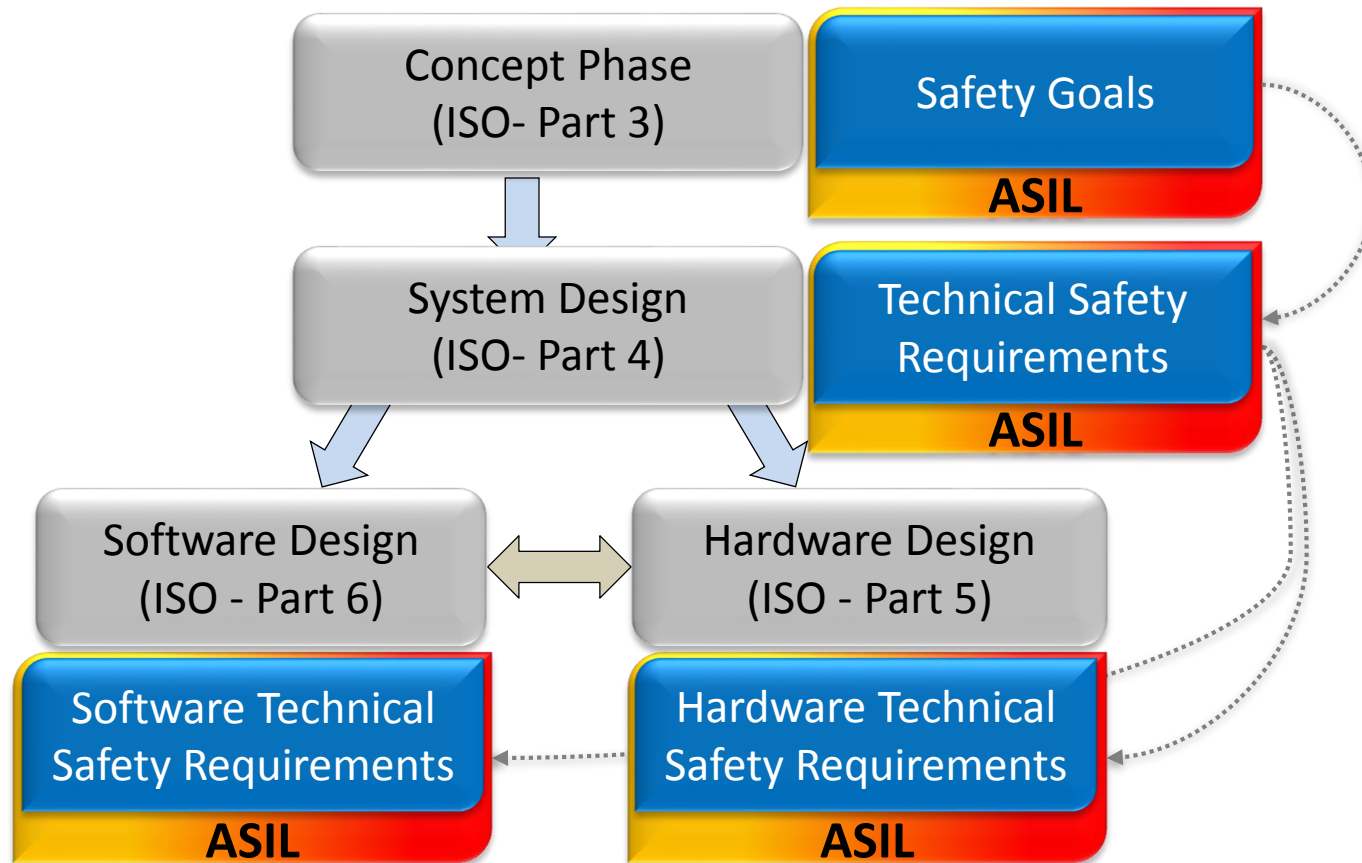
ASIL examples for illustration purposes only

ASIL Determination Example—ISO 26262



Design and Safety Flow

ISO 26262



Failures Relevant to Functional Safety

ISO26262—Functional Safety Principles

Systematic Failures

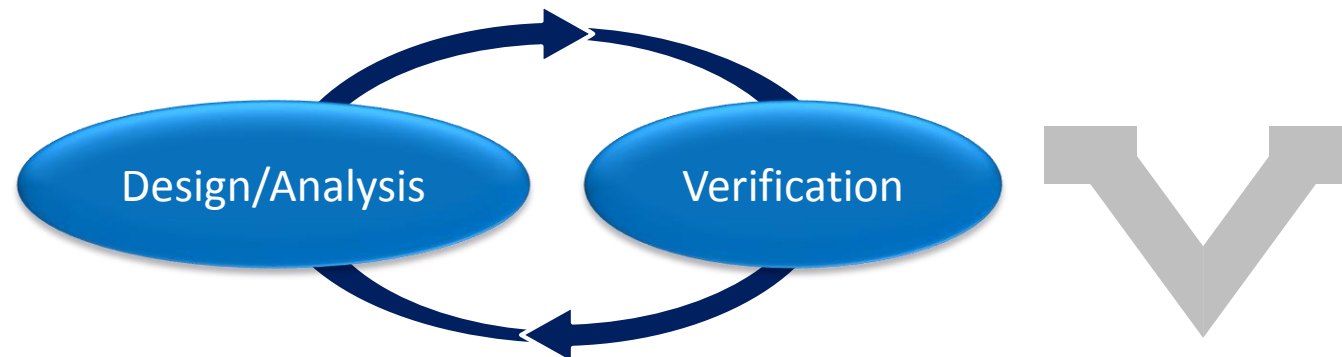
(e.g., software bug)

- Addressed by processes (planning, traceability, documentation, specs)
- Strictness of processes are dependent on the ASIL level

Random Failures

(e.g., component malfunction, noise injection)

- Considers permanent failure and transient effects
- Includes **safety mechanisms** design and integration to handle faults
- Demonstrated by calculations of Reliability/verification of failure rates
- Failure rates and diagnostic coverage requirement depend on ASIL

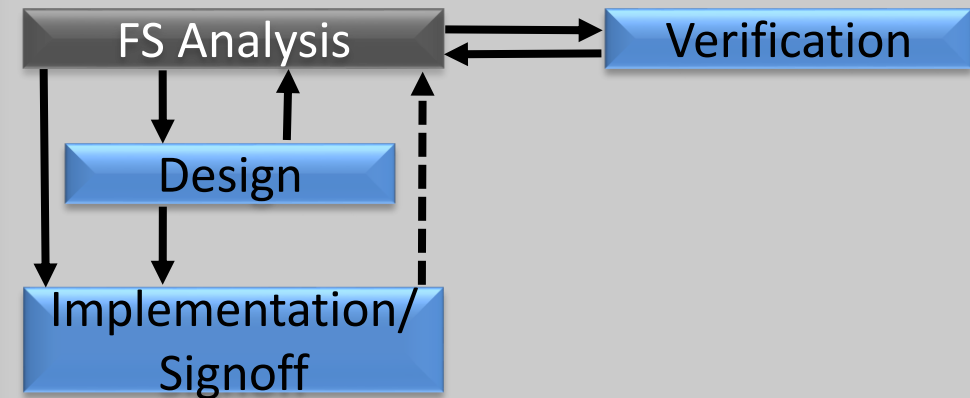


What is Functional Safety Analysis?

- Define Failure Modes (FM)
- Determine Safety Mechanisms (SM)
- Validate Single Point Failure Metric (SPFM) and Latent Failure Metric (LFM)

How to improve your HW metric (to achieve the target ASIL):

- Better component
- Better/Additional Safety Mechanism



Defining Functional Safety

Structured Approach to Measure the ASIL HW Metrics

Safety is the freedom from unacceptable risk of physical injury or damage due to unplanned or undesired events



ASIL	Failure Rate	Single Point Failure Mode (SPFM)	Latent Failure Mode (LFM)
A	< 1000 FIT	Not relevant	Not Relevant
B	< 100 FIT	≥ 90%	≥ 60%
C	< 100 FIT	≥ 97%	≥ 80%
D	< 10 FIT	≥ 99%	≥ 90%

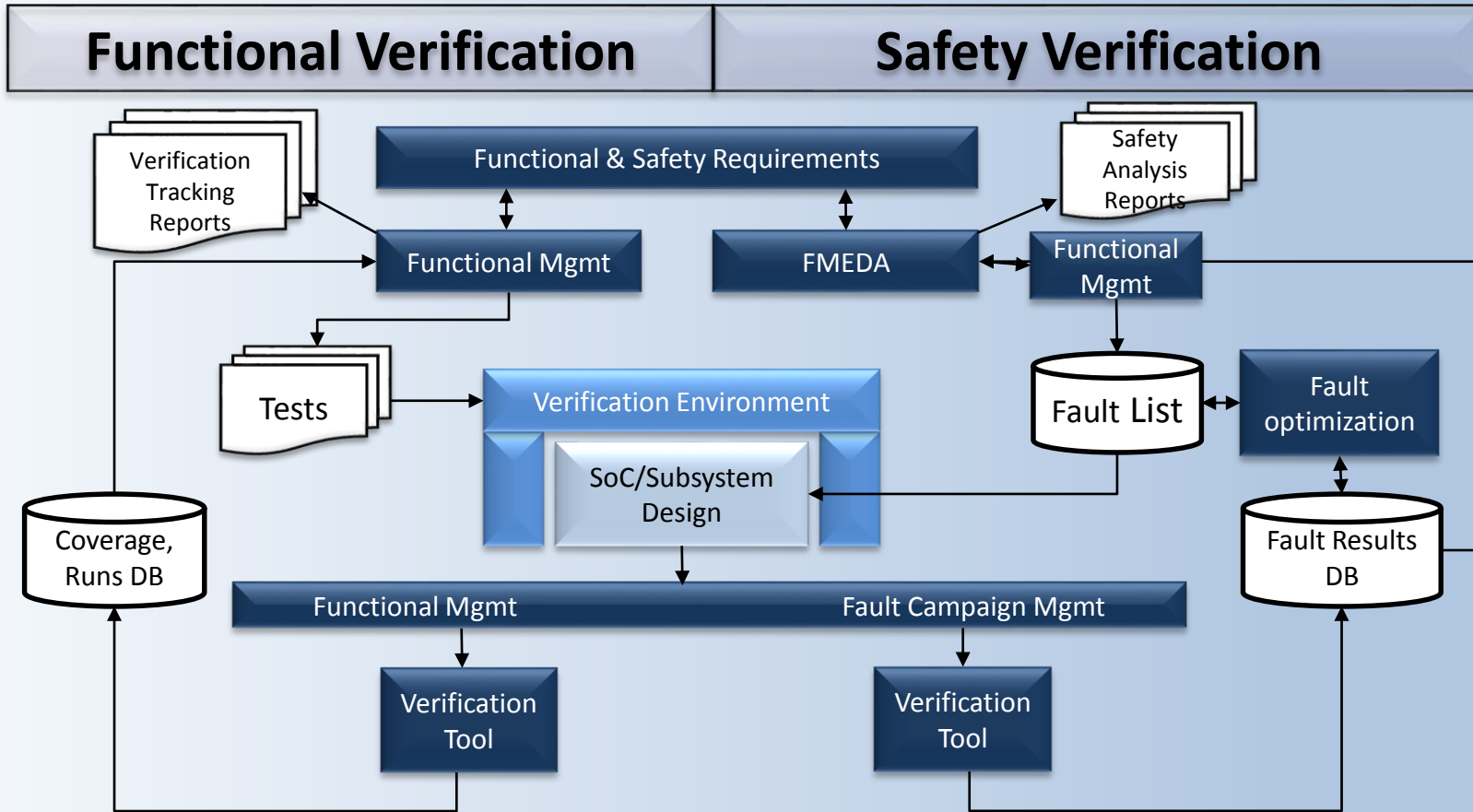
Importance of Failure Mode Effects and Diagnostic Analysis (FMEDA)

- The FMEDA is safety analysis required by ISO26262
 - Other analysis are FMEA, FTA, DFA,....
- FMEDA is needed to:
 - Verify the number of Safety Mechanisms and their claimed diagnostic coverage properties are enough to reach the required ASIL level calculating the architectural safety metrics: SPFM, LFM
 - Validates the Safety Architecture (collection of safety mechanisms) and calculates the performance of the system (SPFM, LFM)

FMEDA – Capture and Analyze Safety Goals

Settings				SPLMp		59.97%		SPFMt		52.76%									
P FIT/Gates	1,20E-05	NAND2	1	LFM		not calculated													
T FIT/Gates	1,64E-03	FLIP FLOP	8																
ID	Part	Sub-Part	Failure Mode	#Gates	#Flops	λ_p	Sp %	λ_{pd}	λ_{ps}	$\lambda_{pd} \%$	λ_t	St %	λ_{td}	λ_{ts}	$\lambda_{td} \%$	DCp	SMp	DCt	SMt
1	CPU	Bus_ITF	Wrong data transaction caused by a fault in the AHB interface	836	23	0,010	0,26	0,007447	0,00262	100,00%	0,039099	40%	0,023459	0,015639	100,00%	30%	E2E	30%	E2E

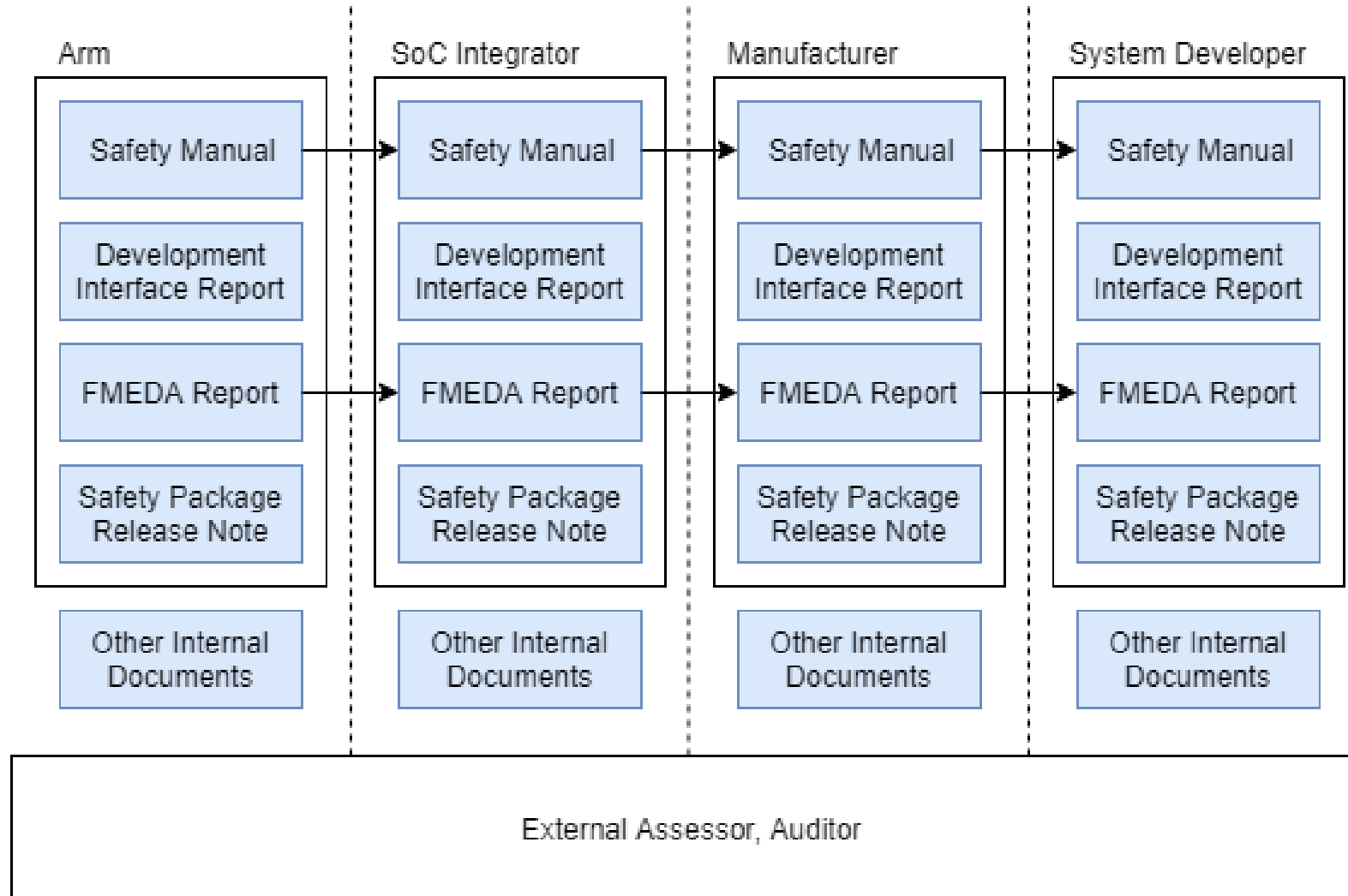
Safety Verification Flow



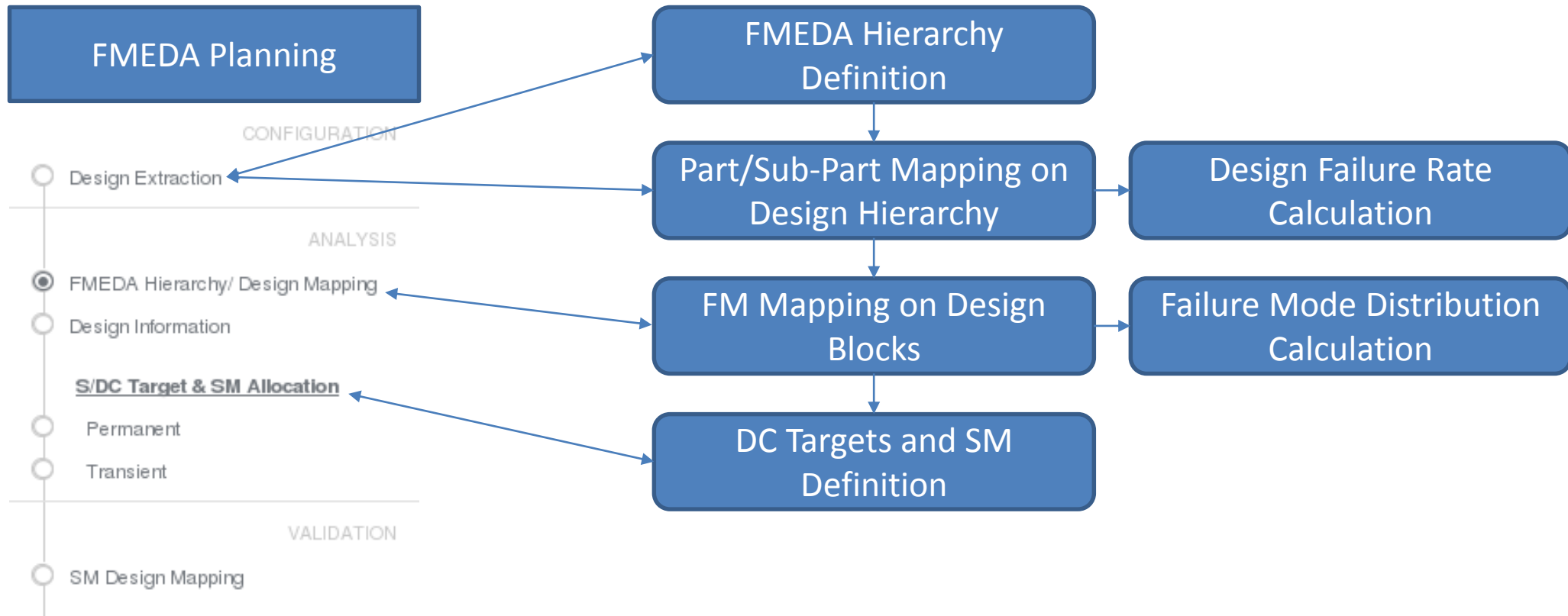
Arm Functional Safety Design Description

- Functional Safety is critical to many Arm products, especially those targeting automotive segment
- Arm has many safety packages already:
 - Arm Cortex®-A53, A57, A72, A75, A76, A35, A32, A34, A55, R5F, R52, M3, M4, M0+, M7, M33, M23
- Arm's safety analysis is for a Safety Element out of Context (SEooC)

Arm Safety Documentation Package



FMEDA Methodology



FMEDA Analytics

Firefox - Mozilla Firefox - @euvclo40

File Edit View History Bookmarks Tools Help

https://euvclo40:8889/web/ 90% Search

FMEDA_DEMO / Configuration

Project Setup

Architectural FMEDA

Not created

Step: -

Detailed FMEDA

Not created

Step: -

Project Name: FMEDA_DEMO

Safety Requirements

ASIL Requirement: A B C D

Transient Enable: ☒

Target Metrics

SPFM P: 90% - SPFM T: 90% - LFM: 60% - PMHF: 100

Technology Information

Tech Na...	Type	P...	Pe...	Tr...	Tra...	Tr...	Tra...	R...	Unit
DigLib	Digital	1.0...	FIT/...	1.6...	FIT/...	1.6...	FIT/FF	0.72	µm2

New Technology

Delete Project

cadence

FMEDA Methodology

Project Setup

Project Name: FMEDA_DEMO

Safety Requirements

ASIL Requirement: A B C D

Transient Enable: ☒

Target Metrics

SPFM P: 90% - SPFM T: 90% - LFM: 60% - PMHF: 100

Technology Information

Tech Na...	Type	P...	Pe...	Tr...	Tra...	Tr...	Tra...	R...	Unit
DigLib	Digital	1.0...	FIT/...	1.6...	FIT/...	1.6...	FIT/FF	0.72	µm2

New Technology

Delete Project

Design Mapping

FMEDA Hierarchy / Design Mapping

Upload Mapping

CDNS-Design-Mapping-Template-v1.0-OpenRISC-01072018.xlsx

Name	Subpart Descri...	Technology...	Mapping	FM #
▶ FETCH			or120... or1200_ge...	
▶ DECODER			or1200_ctrl...	
▶ EXCEPT			or1200_except...	
▶ CORE REGS			or... or... o... or...	
▶ WR-BACK LOGIC			or120... or1200_op...	
▼ FPU			or1200_fpu...	
FPU Arith	Floating point std...	DigLib	or1200_fpu.fpu_arth...	10 / 11
FPU Fcmp	Floating point co...	DigLib	or1200_fpu.fpu_fcmp...	1 / 1
FPU Int Flot	Integer and foati...	DigLib	or1200_fpu.fpu_intflo...	1 / 1
▶ ALUMAC			or120... or1200_m...	
▶ LOAD-STORE			or1200_isu...	
▶ FREEZE			or1200_freeze...	

cadence 9 Parts / 17 Sub-Parts / 37 Failure Modes SPFMp:- SPFMt:- LFM:- PMHFp:- PMHFt:- PMHFFtm:- Fault Campaigns: 0 / 0 / 37

S/CD Target and SM Allocation

FM Saf

Not secure | https://sjfqos005:8889/web/vmgr/fmeda/index.html#/project/FMEDA_DEMO/Detailed/DetailedSDcTargetAndSmAllocation/Permanent

Cadence Research Costumer

ACM CDN_MAPS IT FTP CCMSutil 15.2 iBeta Wiki - A/V My Home - 2017 SVG Tr Other Bookmarks Jabber Q3Meeting17 JabRef ncls Other bookmarks

ferlini

FMEDA_DEMO / Detailed FMEDA

SM Allocation ☒ A Values ☒ SM Definitions

CONFIGURATION

Design Extraction

ANALYSIS

FMEDA Hierarchy/ Design Mapping

Design Information

S/DC Target & SM Allocation

Permanent

Transient

VALIDATION

SM Design Mapping

FMEDA Plan

Permanent

Fault Injection Campaign Configuration

Planning

Execution Configuration

Execution

Transient

Fault Injection Campaign Configuration

Planning

Execution Configuration

Execution

RESULT

FMEDA

Safety Mechanisms

S/DC Target & SM Allocation - Permanent

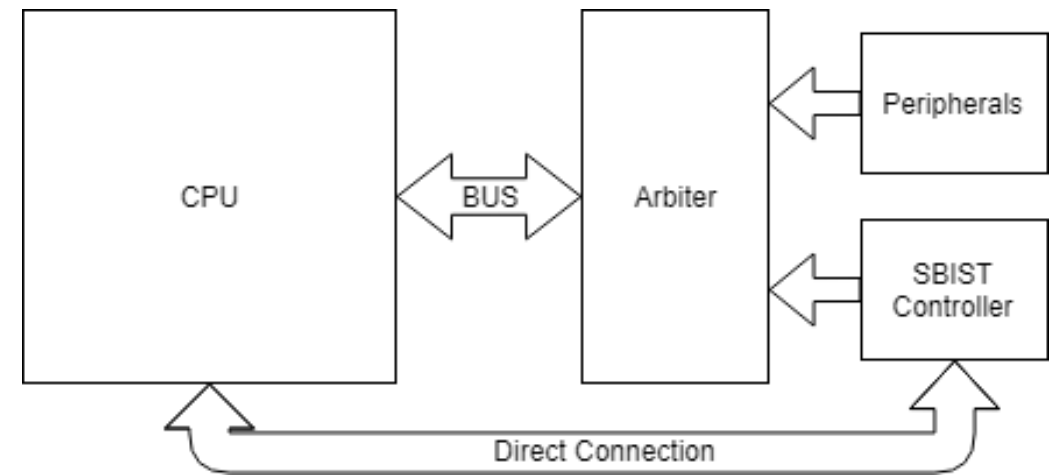
FM ID	Part	Subpart	Failure Mode	Ap	Sp% Target	Sp% Annotated	Apd	Ap%	DCp% Target	DCp% Annotated	SM Permanent	Apr
FM_1	FETCH	Instruction Fetch	Incorrect Instruction Flow caused by a fault the bran...	1.34e-3	0%	4.97% (+4.97%)	1.27e-3	1.33%	99%	100% (+1%)	SM_3	
FM_2	FETCH	GenPC	Incorrect Instruction Flow caused by a fault in the fe...	1.13e-3	0%		1.13e-3	1.12%	0%		Select	1.13e
FM_3	FETCH	GenPC	Incorrect fetch address generation caused by a fault...	1.23e-4	0%		1.23e-4	0.12%	0%		Select	1.23e
FM_4	DECODER	DecodCtrl	Incorrect Instruction Flow caused by a fault in the d...	2.57e-3	0%		2.57e-3	2.55%	0%		Select	2.57e
FM_5	DECODER	DecodCtrl	Incorrect Instruction sequence caused by a fault in t...	3.10e-4	0%		3.10e-4	0.31%	0%		Select	3.10e
FM_6	EXCEPT	Except	Un-intended execution/not executed interrupt request	4.37e-3	0%		4.37e-3	4.35%	0%		Select	4.37e
FM_7	CORE REGS	Special Regs	Processor deadlock caused by system register corr...	1.60e-3	0%		1.60e-3	1.6%	0%		Select	1.60e
FM_8	CORE REGS	Special Regs	Processor memory protection error caused by fault i...	4.92e-5	0%		4.92e-5	0.05%	0%		Select	4.92e
FM_9	CORE REGS	Register File	Corrupt data or value caused by a fault in the regist...	3.58e-2	0%	9.25% (+9.25%)	0.03	35.67%	99%		SM_2	0.03
FM_10	WR-BACK LO...	Write-back mux	Wrong address write back in cache caused by fault I...	9.75e-4	0%		9.75e-4		0%		Select	9.75e
FM_11	WR-BACK LO...	Operand Muxes	Wrong data write back in cache caused by fault into ...	1.37e-3	0%		1.37e-3		0%		Select	1.37e
FM_12	FPU	FPU top logic	Incorrect result caused by fault in the FPU state ma...	8.52e-4	0%		8.52e-4	0.85%	70%		Select	2.56e
FM_13	FPU	FPU Arithmetic	Incorrect result caused by fault in the FPU-Arith stat...	2.19e-3	0%		2.19e-3	2.18%	70%		Select	6.57e
FM_14	FPU	FPU Arithmetic	FPU Adder produces incorrect data due to fault into ...	1.30e-3	0%		1.30e-3	1.29%	70%		Select	3.89e
FM_15	FPU	FPU Arithmetic	FPU Incorrect division data due to fault into the FPU...	2.63e-3	0%		2.63e-3	2.62%	70%		Select	7.90e
FM_16	FPU	FPU Arithmetic	FPU Incorrect multiplication data due to fault into th...	3.22e-3	0%		3.22e-3	3.2%	70%		Select	9.65e
FM_17	FPU	FPU Arithmetic	FPU Incorrect post-division data due to fault into the...	4.23e-3	0%		4.23e-3	4.21%	70%		Select	1.27e
FM_18	FPU	FPU Arithmetic	FPU Incorrect post-normalization multiplication data...	5.97e-3	0%		5.97e-3	5.94%	70%		Select	1.79e
FM_19	FPU	FPU Arithmetic	FPU post-normalized Adder/Subtractor produces incor...	2.18e-3	0%		2.18e-3	2.17%	70%		Select	6.53e
FM_20	FPU	FPU Arithmetic	FPU Incorrect pre-division data due to fault into the...	1.47e-3	0%		1.47e-3	1.47%	70%		Select	4.42e
FM_21	FPU	FPU Arithmetic	FPU Incorrect multiplication data due to fault into th...	2.52e-4	0%		2.52e-4	0.25%	70%		Select	7.56e
FM_22	FPU	FPU Arithmetic	FPU Adder produces incorrect data due to fault into ...	1.89e-3	0%		1.89e-3	1.88%	70%		Select	5.67e
FM_23	FPU	FPU Fcmp	FPU Incorrect comparing result due to fault into the...	3.73e-4	0%		3.73e-4	0.37%	50%		SM_1	1.87e
FM_24	FPU	FPU Int Float	FPU Incorrect floating integer data result due to faul...	6.23e-3	0%		6.23e-3	6.2%	40%		SM_1	3.74e
FM_25	ALUMAC	Arith. Logic	Incorrect result caused by fault in the ALU state ma...	1.43e-3	0%		1.43e-3	1.42%	0%		Select	1.43e
FM_26	ALUMAC	Arith. Logic	Incorrect Instruction Result caused by a fault in the...	3.42e-4	0%		3.42e-4	0.34%	0%		Select	3.42e
FM_27	ALUMAC	Arith. Logic	Incorrect Instruction Result caused by a fault in the l...	1.32e-4	0%		1.32e-4	0.13%	0%		Select	1.32e
FM_28	ALUMAC	Arith. Logic	Incorrect Instruction Result caused by a fault in the...	1.06e-3	0%		1.06e-3	1.06%	0%		Select	1.06e
FM_29	ALUMAC	Multiplier Accumulator	Incorrect result caused by fault in the MAC state ma...	4.52e-3	0%		4.52e-3	4.5%	0%		Select	4.52e
FM_30	ALUMAC	Multiplier Accumulator	Incorrect Instruction Result caused by a fault in the...	2.40e-3	0%		2.40e-3	2.38%	0%		Select	2.40e
FM_31	ALUMAC	Multiplier Accumulator	Incorrect Instruction Result caused by a fault in the...	9.60e-3	0%		9.60e-3	9.55%	0%		Select	9.60e
FM_32	LOAD-STORE	Load Store	Wrong address addressing load/store data caused ...	5.11e-4	0%		5.11e-4	0.51%	0%		Select	5.11e
FM_33	LOAD-STORE	Load Store	Data corruption during memory to register transfer d...	2.69e-4	0%		2.69e-4	0.27%	0%		Select	2.69e

9 Parts / 16 Sub-Parts / 35 Failure Modes | SPFMp: 25.53% SPFM: DISABLED LFM: 100% | PMHFP: 0.07 PMHF: DISABLED PMHFm: 0 | Fault Campaigns: 2 / 2 / 35

STL and Safety Mechanisms

The Importance of Fault Injection Campaigns on the STL

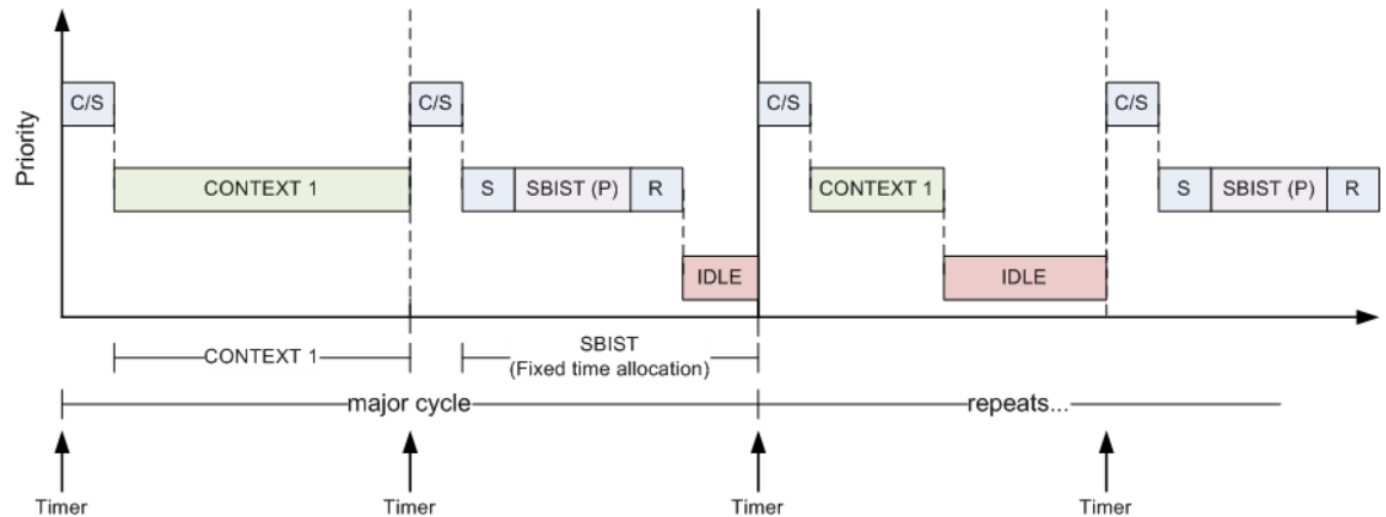
- Software Test Library (STL)
 - It is intended to be run on a safety critical processor, and attempt to detect any errors
 - This can allow the system to fail safely
 - The design of the processor is created with the STL in mind
 - Optimisations enable software to test certain parts and be deterministic



STL and Safety Mechanisms

The Importance of Fault Injection Campaigns on the STL (continued)

- STL is very low level
 - Written in C and assembly
 - Contains a number of functions for testing the “health” of the processor
- Requirements are strict on size and execution time
 - They can be “online” as well as “offline”
- Fault injection used to measure the effectiveness of STL



Example: FMEDA

FMEDA reports are done for the processor with the STL, and also for the SBIST controller.

Permanent faults								
FM distribution	Failure rate	Fsafe	Fault detection and control mechanism	Diagnostic coverage (Krf)	Residual / single point failure rate	Multiple point failure rate	Diagnostic coverage for latent faults (Klat)	Latent multiple point failure rate
0.000%	3.57E-04	0.000%	STL	89.240%	3.84E-05	3.19E-04	100.00%	0.00E+00

How to Validate an FMEDA

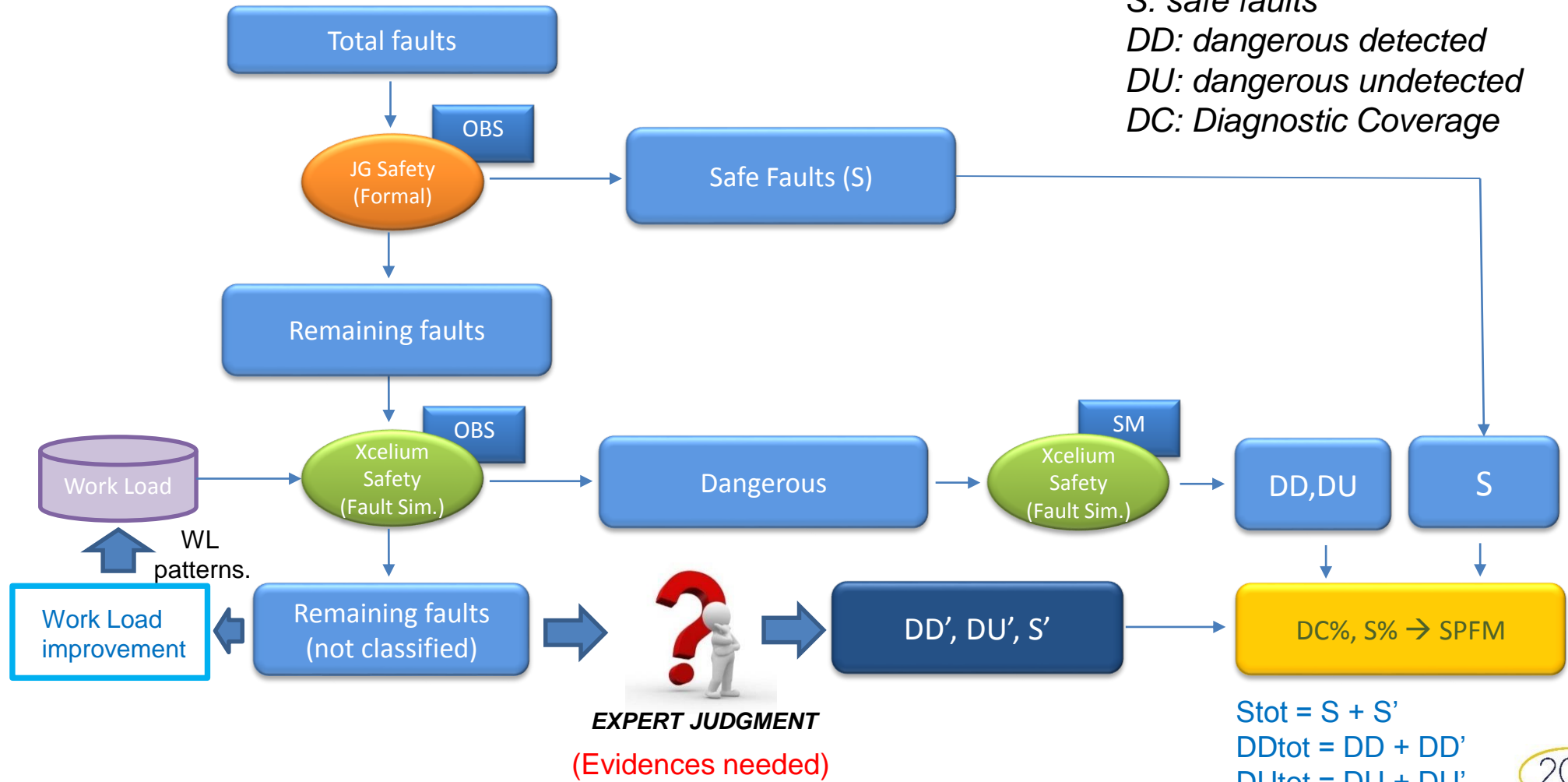
Agenda:

S: safe faults

DD: dangerous detected

DU: dangerous undetected

DC: Diagnostic Coverage

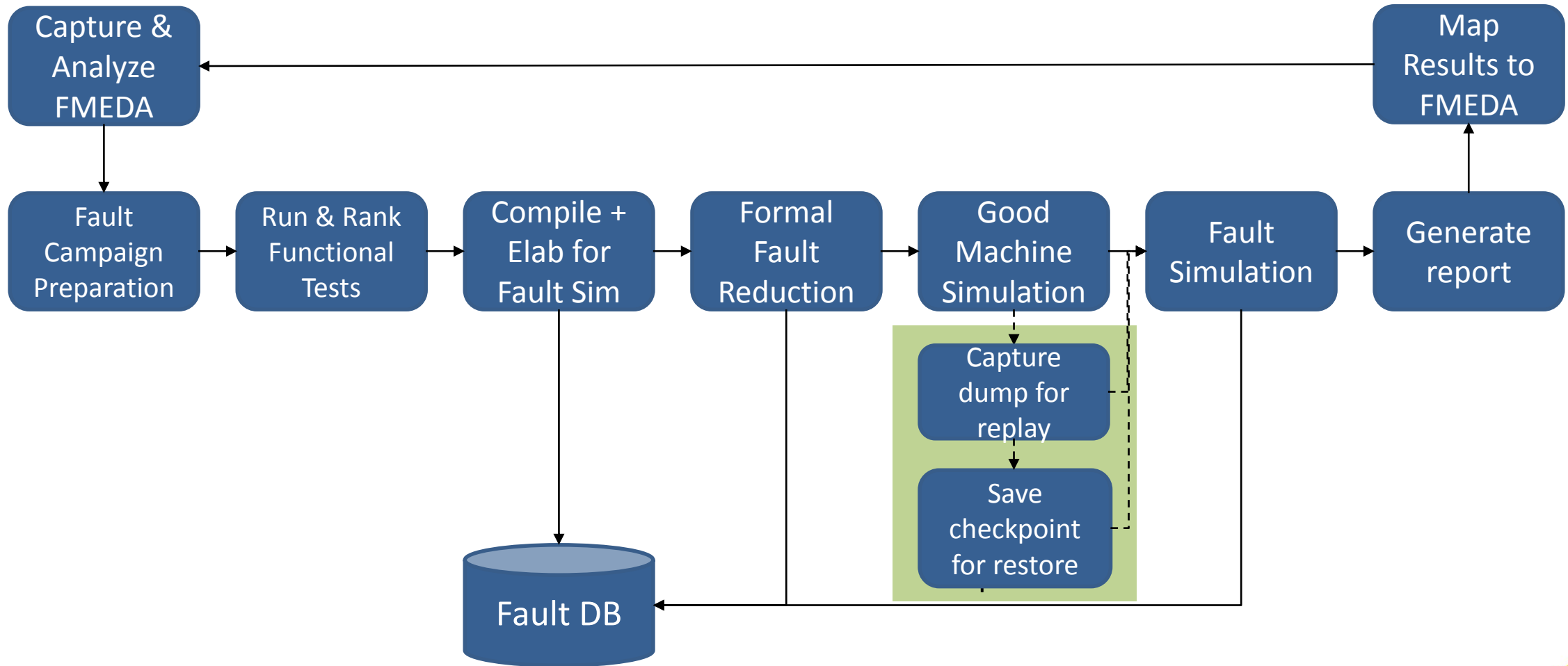


$$Stot = S + S'$$

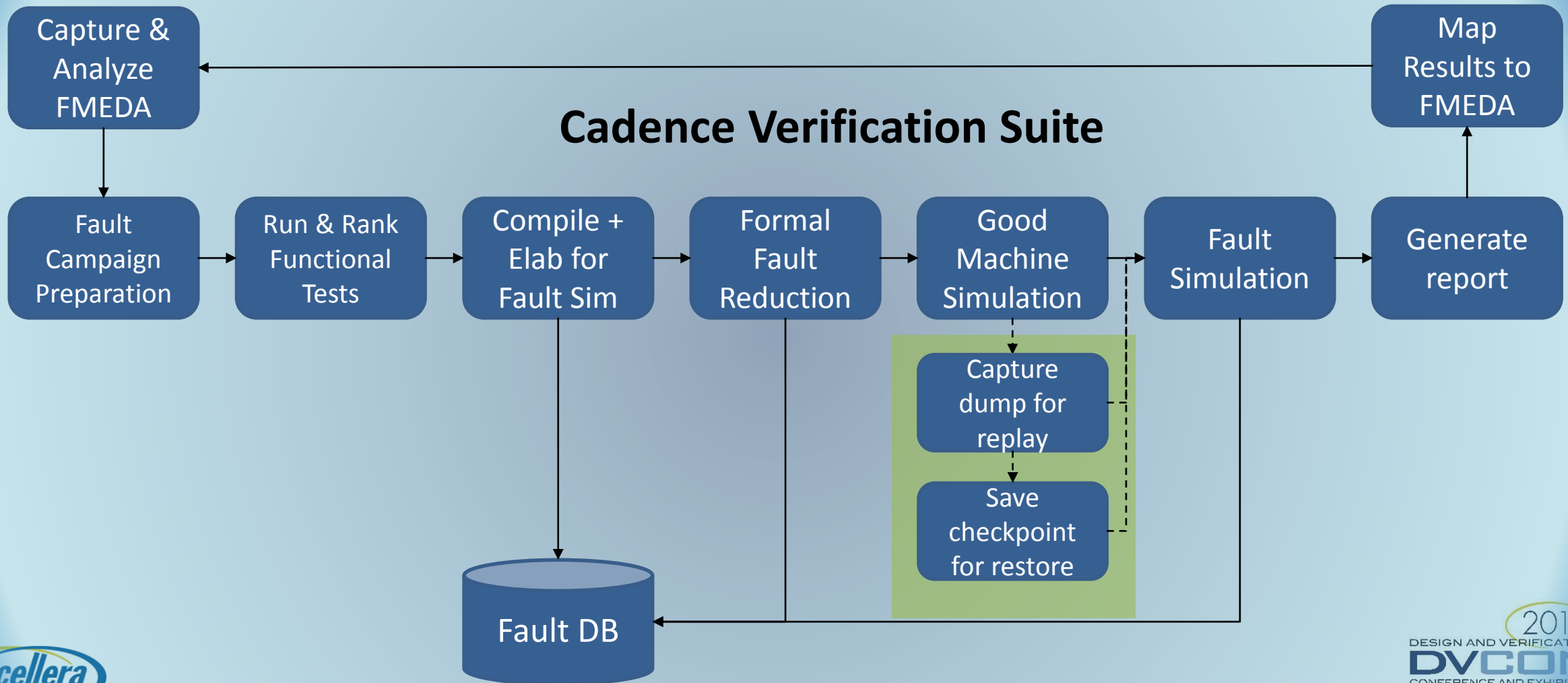
$$DD_{tot} = DD + DD'$$

$$DU_{tot} = DU + DU'$$

Functional Safety Flow



Cadence Functional Safety Flow



Questions?

Demo

FMEDA Demo

How to Validate an FMEDA – Fault Classification Flow

- Fault classification can't be ideal in practice, not classified faults (NC) can be exposed to user expert judgment to be further classified

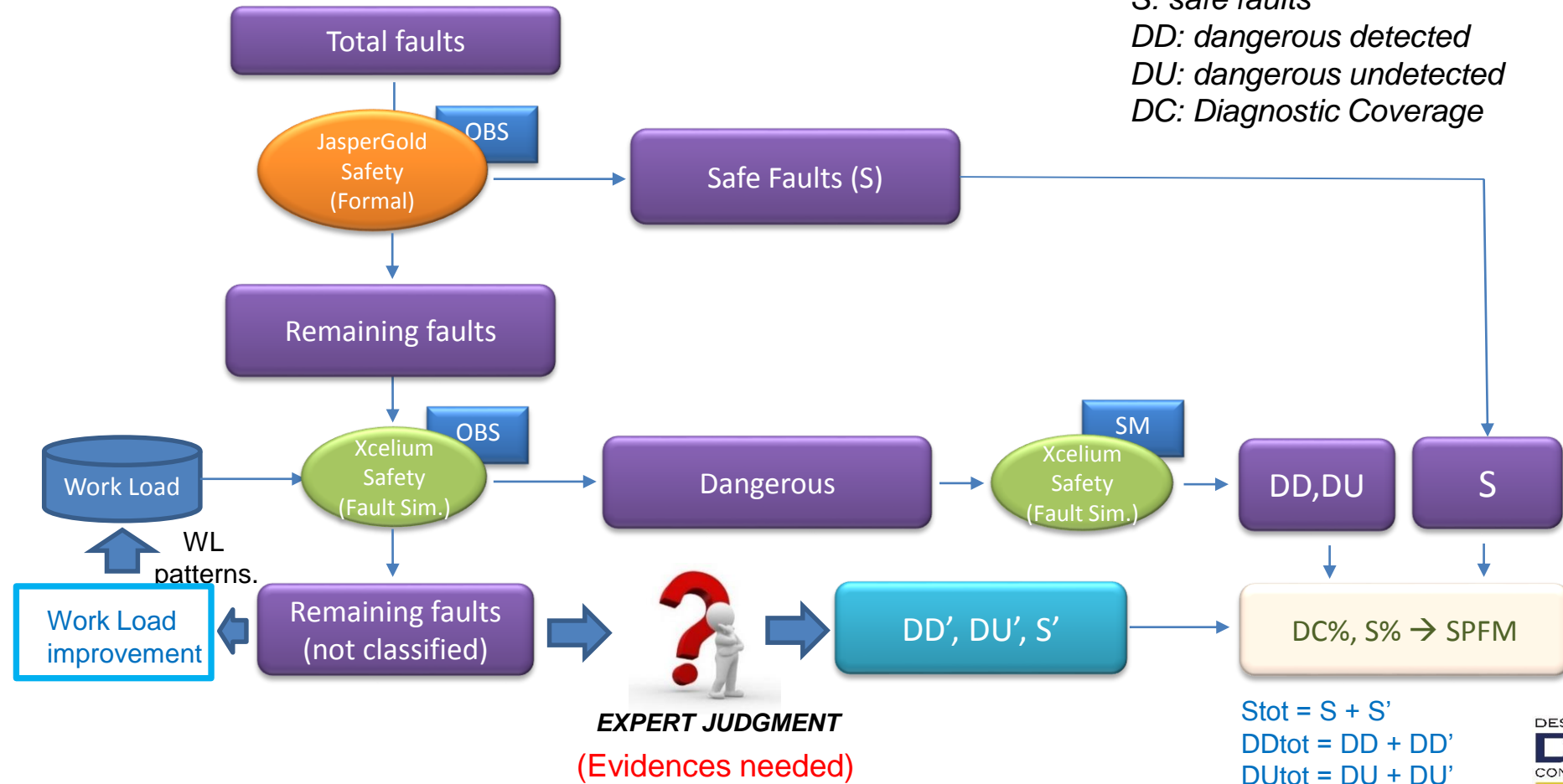
Agenda:

S: safe faults

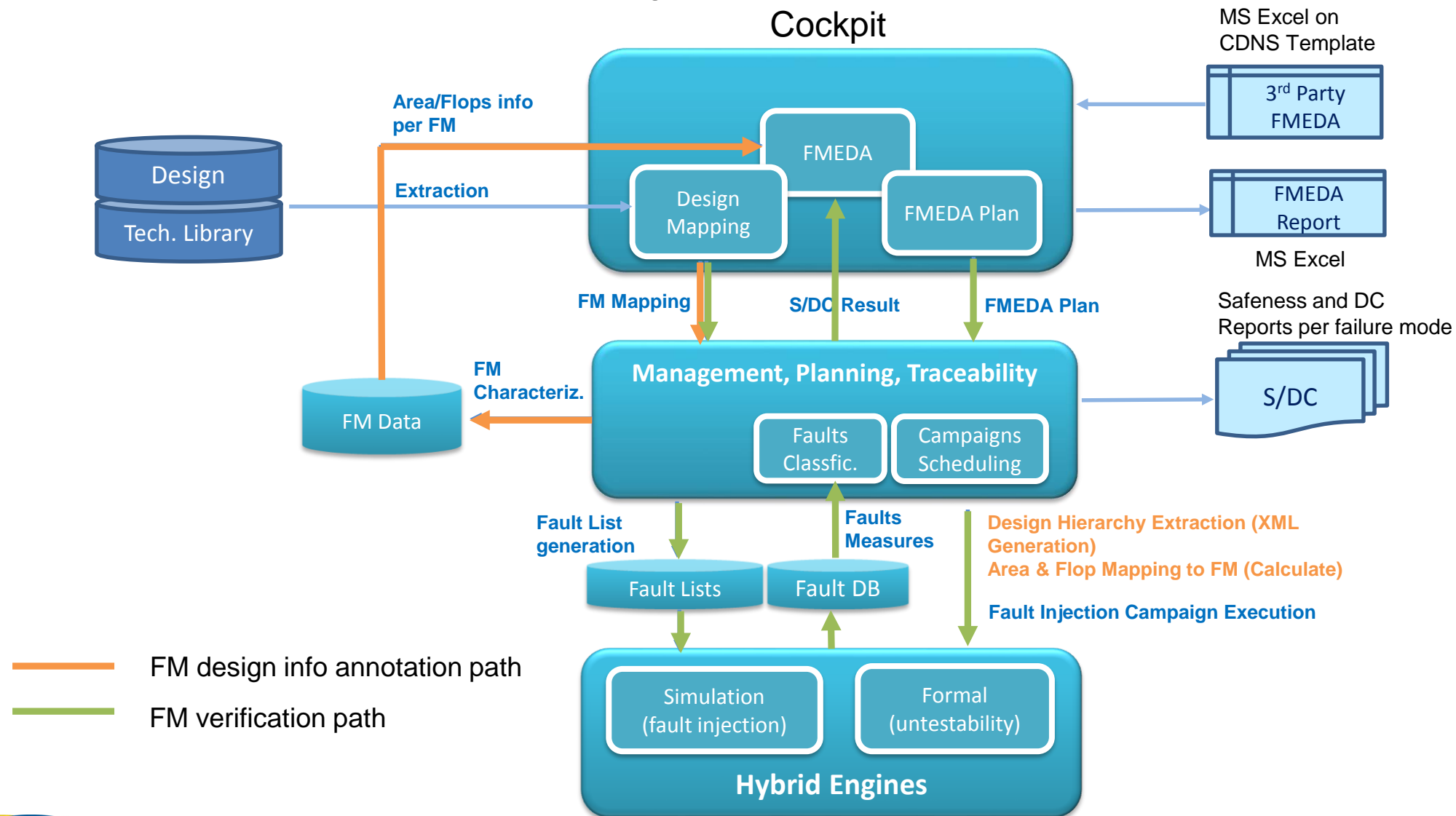
DD: dangerous detected

DU: dangerous undetected

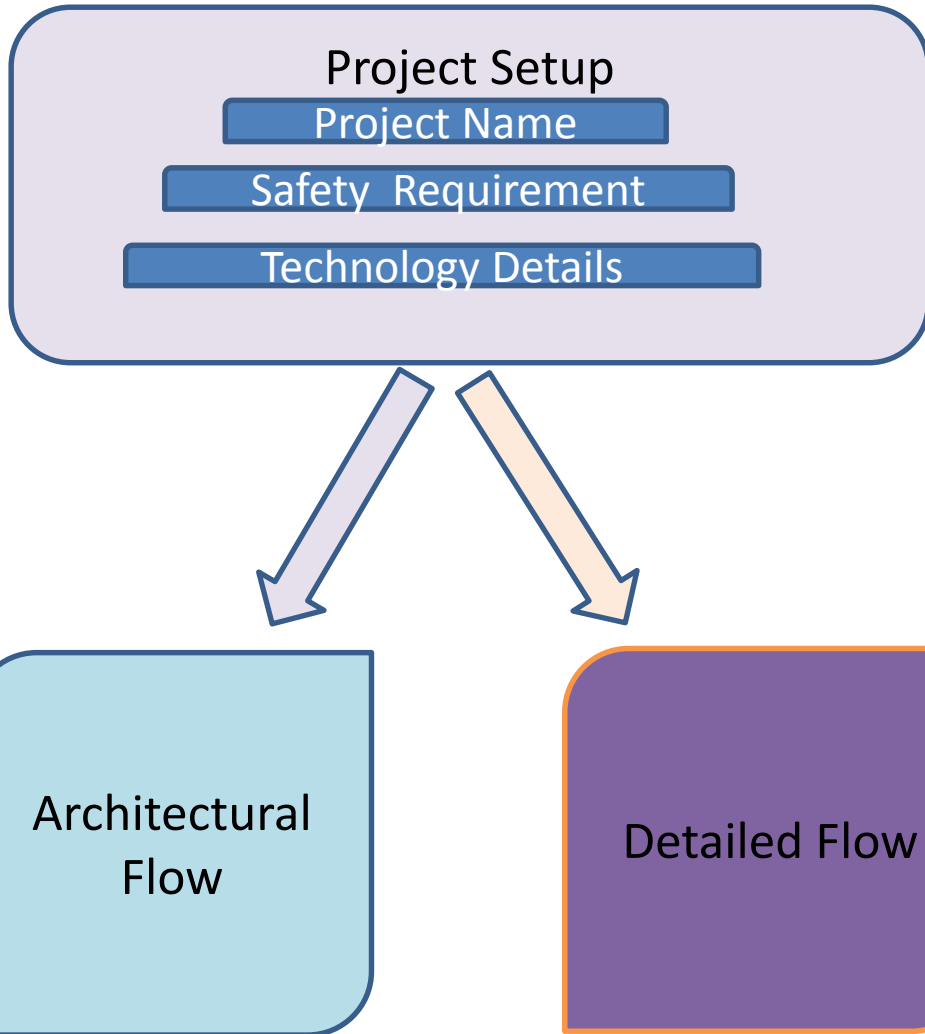
DC: Diagnostic Coverage



FMEDA Solution – Top Level View



Flow support



Architectural FMEDA Flow:

- Rough estimation of the overall metrics
 - Course grained FMEDA
- Metrics evaluation before RTL/design information availability
- Analysis is to address feasibility study
- Analysis aimed to figure out primary SM requirements.

Detailed FMEDA Flow:

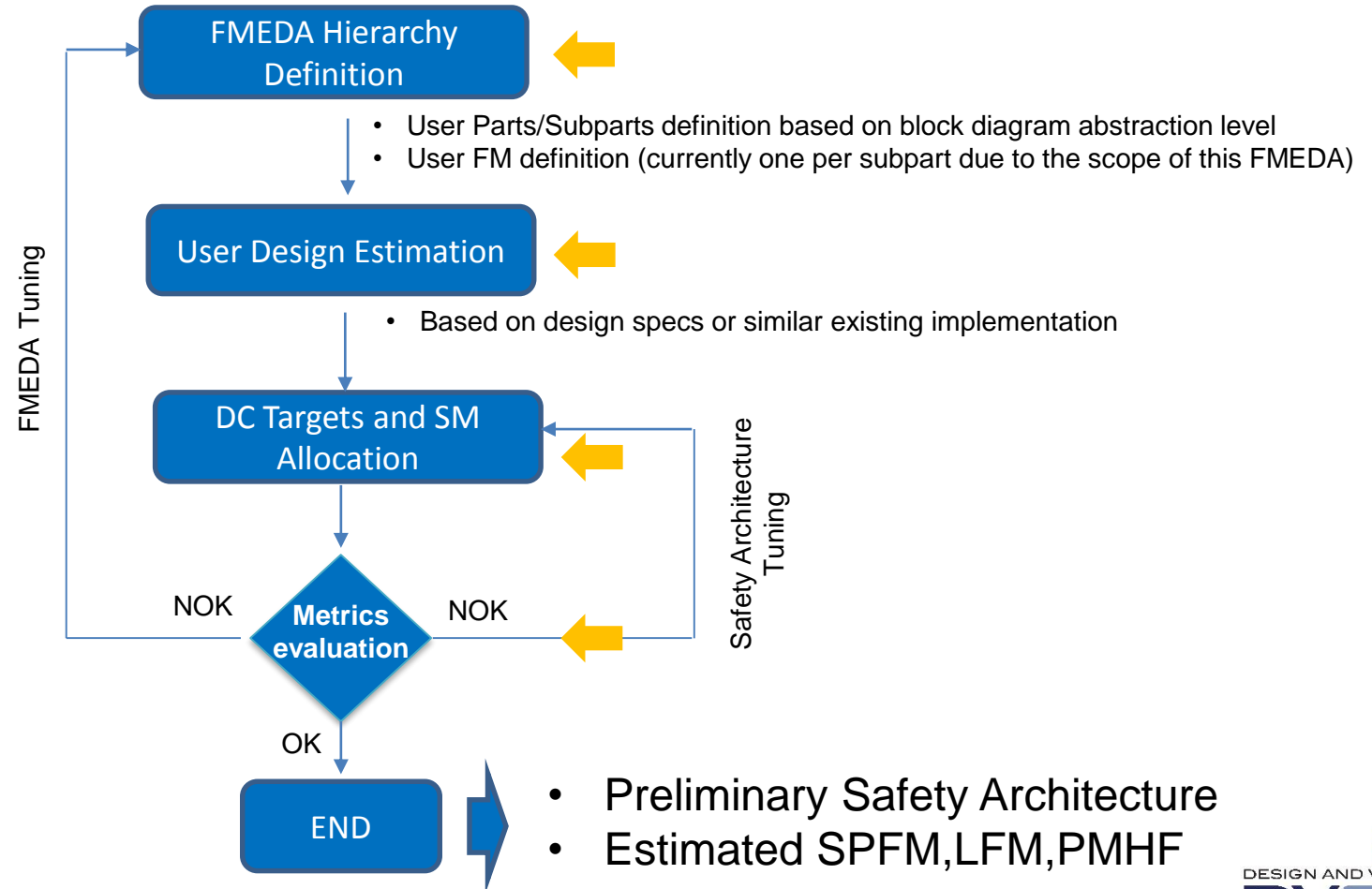
- Accurate estimation of the overall metrics
 - Fine grained FMEDA
- Metrics evaluation using actual design & assumed DC targets
- Evidence to prove the achieved safety goals
 - Data for ASIL certification
- Validation of metrics – Fault Injection, Formal Analysis

FMEDA Solution

Architectural FMEDA: based on Design Estimation (before RTL availability)

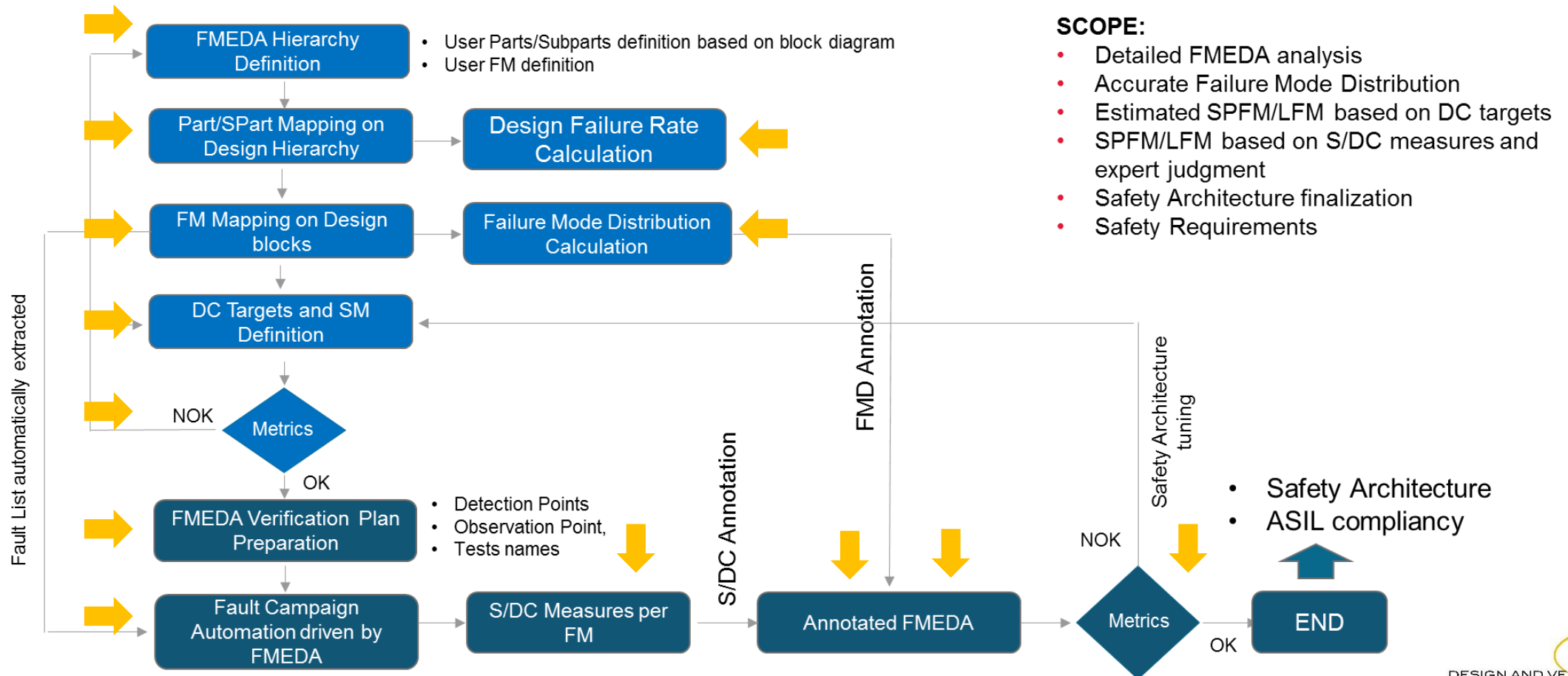
SCOPE:

- Course grained FMEDA analysis
- Preliminary Safety Architecture
- Preliminary Safety Requirements
 - S, DC associated with mapped Safety Mechanism
- Estimated SPFM, LFM, PMHF
 - For Permanent and Transient

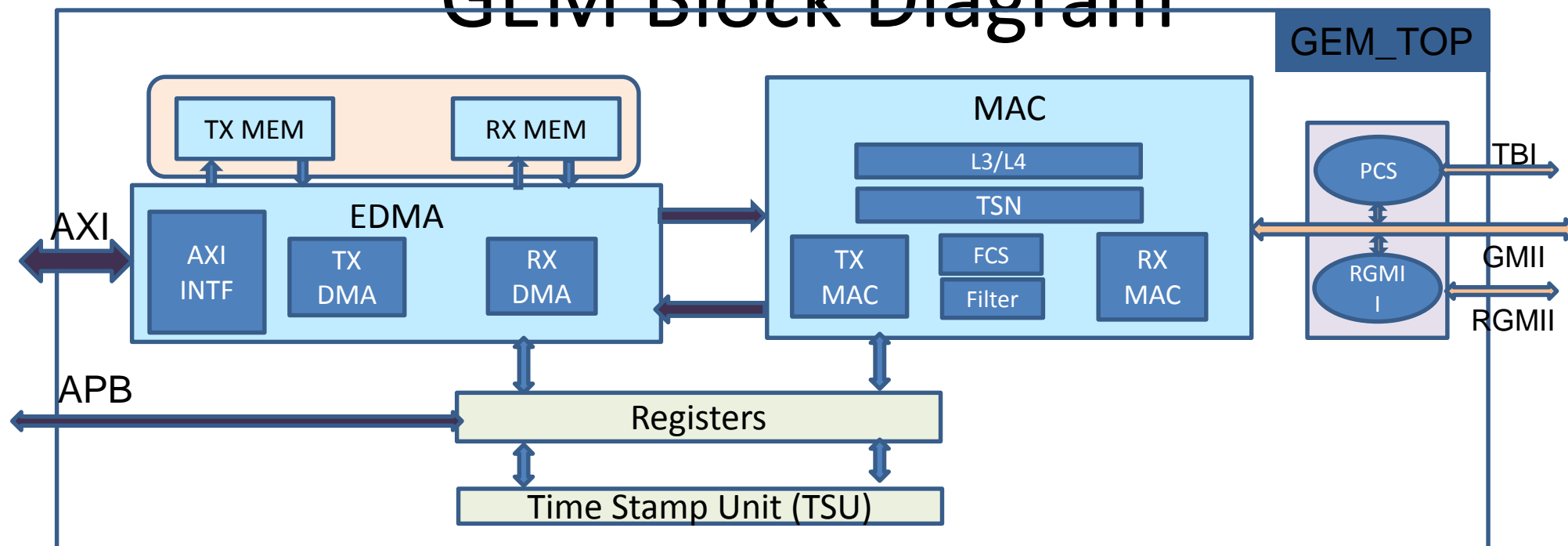


FMEDA Solution

Detailed FMEDA: based on actual design information (after RTL, Netlist availability)



GEM Block Diagram



Ethernet_IP_Demo_1 / Detailed FMEDA

admin

CONFIGURATION

Design Extraction

ANALYSIS

FMEDA Hierarchy/ Design Mapping

Design Information

S/DC Target & SM Allocation

Permanent

Transient

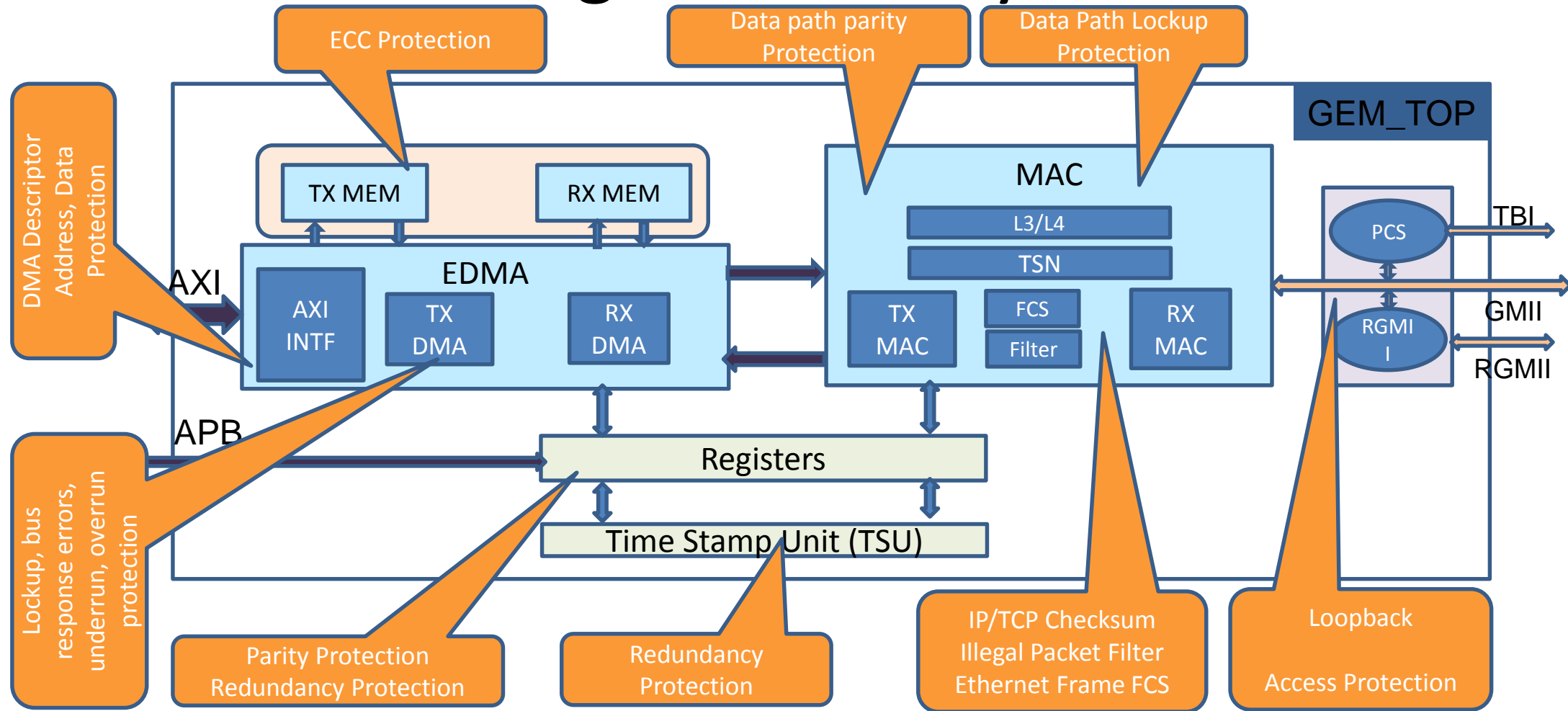
VALIDATION

FMEDA Hierarchy / Design Mapping

Upload Mapping

gen_tsu_i_gem_tsu		gem_gxl_i_gem_ss_i_gem_top.gen_tsu_i_gem_tsu				4/4
ID	Failure Mode	Safety Relevant	Type	Memory Bits	Mapping	
FM_1	The timer value may not be captured or captured incorrectly	✓	Mission		gem_gxl_i_gem_ss_i_gem_top.gen_tsu_i_gem_tsu...	
FM_2	The TSU seconds interrupt is incorrect	✓	Mission		gem_gxl_i_gem_ss_i_gem_top.gen_tsu_i_gem_tsu	
FM_3	TSU compare interrupt is incorrect	✓	Mission		gem_gxl_i_gem_ss_i_gem_top.gen_tsu_i_gem_tsu	
FM_4	TX/RX timestamp is corrupted, output TSU timer value to local s...	✓	Mission		gem_gxl_i_gem_ss_i_gem_top.gen_tsu_i_gem_tsu	

GEM Block Diagram - Safety mechanism view



FMEDA Template – Instance Mapping Formats

DESIGN MAPPING INFORMATION

Part (Block)	Part Instances mapping	Subpart (Sub-block)	Description	Subpart Instances mapping	Failure Mode	Failure Mode Instances mapping
i_gem_top	gem_gxl.i_gem_ss.i_gem_top	gen_tsu_i_gem_tsu	Time Stamp Unit	gem_gxl.i_gem_ss.i_gem_top.gen_tsu_i_gem_tsu	The timer value may not be captured or captured incorrectly	gem_gxl.i_gem_ss.i_gem_top.gen_tsu_i_gem_tsu...
					The TSU seconds interrupt is incorrect	gem_gxl.i_gem_ss.i_gem_top.gen_tsu_i_gem_tsu
					TSU compare interrupt is incorrect	gem_gxl.i_gem_ss.i_gem_top.gen_tsu_i_gem_tsu
					TX/RX timestamp is corrupted, output TSU timer value to local system will be invalid, Timer value read back in registers is also invalid. May also cause TX lockup for time based scheduling.	gem_gxl.i_gem_ss.i_gem_top.gen_tsu_i_gem_tsu
		i_gem_reg_top.i_gem_registers	Etherent IP Registers	gem_gxl.i_gem_ss.i_gem_top.i_gem_reg_top.i_gem_registers...	Fault in Parity Generators of	gem_gxl.i_gem_ss.i_gem_top.i_gem_reg_top.i_gem_registers.gen_axi_i_gem_parity_gen_dma_config_burst_len; gem_gxl.i_gem_ss.i_gem_top.i_gem_reg_top.i_gem_registers.i_gem_parity_gen_dma_config_byte_1; gem_gxl.i_gem_ss.i_gem_top.i_gem_reg_top.i_gem_registers.i_gem_parity_gen_default; gem_gxl.i_gem_ss.i_gem_top.i_gem_reg_top.i_gem_registers.i_gem_parity_gen_int_mask_disable
						em_ss.i_gem_top.i_gem_reg_top.i_gem_registers...; !gem_gxl.i_gem_ss.i_gem_top.i_gem_reg_top.i_gem_registers.gen_axi_i_gem_parity_gen_dma_config_burst_len; i_gem_ss.i_gem_top.i_gem_reg_top.i_gem_registers.i_gem_parity_gen_dma_config_byte_1; m_gxl.i_gem_ss.i_gem_top.i_gem_reg_top.i_gem_registers.i_gem_parity_gen_default; d.i_gem_ss.i_gem_top.i_gem_reg_top.i_gem_registers.i_gem_parity_gen_int_mask_disable
					Fault in dynamic control outputs from the registers	gem_gxl.i_gem_ss.i_gem_top.i_gem_reg_top.i_gem_registers;

a.b.c.d... -> Include all the submodules instances inside the module 'd'

a.b.c.d -> Include only Submodule 'd'

!a.b.c.d.e... -> Exclude all the submodules instances inside the module 'e'

!a.b.c.d.e -> Exclude only Submodule 'e'

Architectural Flow

Controls visibility

Report

Home / Ethernet_IP_DEMO / Architectural FMEDA

admin

ANALYSIS

FMEDA Hierarchy

Design Estimation

S/DC Target & SM Allocation

Permanent

Transient

RESULT

FMEDA

Safety Mechanisms

FMEDA Result

Design Information ☒ FM Type ☒

Generate Report

ID	Part	Subpart	Technology	Area	#G...	...	#bit	λ_p	Sp...	λ_{pd}	$\lambda_p \%$	DCp %	λ_{pr}	SM ID Perma
FM_ARCH_16	gem_gxl	TX_Data_Memory	MEM_LIB	4505.6			4096	4.92e-2	2%	0.05	2.77%	99%	4.82e-4	SM_11
FM_ARCH_15	gem_gxl	RX_Data_Memory	MEM_LIB	9011.2			8192	9.83e-2	2%	0.1	5.54%	99%	9.63e-4	SM_11
FM_ARCH_14	gem_gxl	TSU_Comparator	Generic_SS_LIB	513	500	64		2.91e-3	2%		0.16%			
FM_ARCH_13	gem_gxl	Register_Parity_Logic	Generic_SS_LIB	1026	1000	0		5.82e-3	2%		0.33%			
FM_ARCH_12	gem_gxl	PHY_Interface	Generic_SS_LIB	5130	5000	100		2.91e-2	2%	0.03	1.64%	90%	2.85e-3	SM_13
FM_ARCH_11	gem_gxl	MISC	Generic_SS_LIB	3078	3000	200		1.75e-2	2%	0.02	0.98%	90%	1.71e-3	SM_12
FM_ARCH_10	gem_gxl	ECC_protection	Generic_SS_LIB	2872.8	2800	50		1.63e-2	2%	0.02	0.92%	95%	7.99e-4	SM_11
FM_ARCH_9	gem_gxl	CSR_Space	Generic_SS_LIB	51300	50000	4500		2.91e-1	2%	0.29	16.41%	95%	0.01	SM_5 ; SM_6
FM_ARCH_8	gem_gxl	TSU	Generic_SS_LIB	12312	12000	300		6.99e-2	2%	0.07	3.94%	98%	1.37e-3	SM_10
FM_ARCH_7	gem_gxl	TX_MAC	Generic_SS_LIB	41040	40000	1500		2.33e-1	2%	0.23	13.13%	97%	6.85e-3	SM_7 ; SM_9 ; SM_12 ; S
FM_ARCH_6	gem_gxl	RX_MAC	Generic_SS_LIB	34884	34000	22		1.98e-1	2%	0.19	11.16%	97%	5.82e-3	SM_8 ; SM_12 ; SM_13 ;
FM_ARCH_5	gem_gxl	AXI_RD_WR	Generic_SS_LIB	61560	60000	4600		3.49e-1	2%	0.34	19.7%	95%	0.02	SM_3 ; SM_4 ; SM_7 ; S
FM_ARCH_4	gem_gxl	DMA_RX_RD	Generic_SS_LIB	30780	30000	1400		1.75e-1	2%	0.17	9.85%	95%	8.56e-3	SM_2 ; SM_4
FM_ARCH_3	gem_gxl	DMA_RX_WR	Generic_SS_LIB	5130	5000	250		2.91e-2	2%	0.03	1.64%	95%	1.43e-3	SM_4
FM_ARCH_2	gem_gxl	DMA_TX_RD	Generic_SS_LIB	14364	14000	1200		8.15e-2	2%	0.08	4.6%	92%	6.39e-3	SM_3
FM_ARCH_1	gem_gxl	DMA_TX_WR	Generic_SS_LIB	22572	22000	1350		1.28e-1	2%	0.13	7.22%	96%	5.02e-3	SM_1 ; SM_3

1 Parts / 16 Sub-Parts / 16 Failure Modes

SPFMp: 95.85% SPFMt: 95.14% LFM: 99.95%

PMHFp: 0.07 PMHft: 6.9 PMHFtm: 8.56e-4

cadence

accelera
SYSTEMS INITIATIVE

DVCON
CONFERENCE AND EXHIBITION
EUROPE

Detailed Flow

CONFIGURATION

Design Extraction

ANALYSIS

FMEDA Hierarchy/ Design Mapping

Design Information

S/DC Target & SM Allocation

Permanent

Transient

VALIDATION

SM Design Mapping

FMEDA Plan

Permanent

Fault Injection Campaign Configuration

Planning

Execution Configuration

Execution

Transient

Fault Injection Campaign Configuration

Planning

Execution Configuration

Execution

RESULT

☒ FMEDA

Safety Mechanisms

Ethernet_IP_DEMO / Detailed FMEDA

admin

FMEDA Result

Filter Options

Design Information ☐ FM Type ☐

Generate Report

ID	Part	Subpart	Failure Mode	Safety Relevant	λ_p	Sp %	λ_{pd}	λ_p %	DCp %	λ_{pr}
FM_1	i_gem_top	gen_tsu_i_gem_tsu	The timer value may not be captured or captured incorrectly	true	8.49e-3	6.49%	7.94e-3	2.16%	100%	0
FM_2	i_gem_top	gen_tsu_i_gem_tsu	The TSU seconds interrupt is incorrect	true	8.44e-3	6.38%	7.90e-3	2.15%	99.76%	1.92e-5
FM_3	i_gem_top	gen_tsu_i_gem_tsu	TSU compare interrupt is incorrect	true	8.44e-3	2%	8.27e-3	2.15%	98%	1.65e-4
FM_4	i_gem_top	gen_tsu_i_gem_tsu	TX/RX timestamp is corrupted, output TSU timer value to local system will be...	true	8.44e-3	2%	8.27e-3	2.15%	98%	1.65e-4
FM_5	i_gem_top	i_gem_reg_top.i_gem_registers	Fault in Parity Generators of Registers	true	4.72e-4	2%	4.62e-4	0.12%	95%	2.31e-5
FM_6	i_gem_top	i_gem_reg_top.i_gem_registers	Fault in static configuration outputs from the registers	true	1.84e-1	2%	0.18	46.83%	95%	9.00e-3
FM_7	i_gem_top	i_gem_reg_top.i_gem_registers	Fault in dynamic control outputs from the registers	true	1.74e-1	2%	0.17	44.43%	95%	8.54e-3

Generate Report in Excel Format

cadence

accelera

SYSTEMS INITIATIVE

1 Parts / 2 Sub-Parts / 7 Failure Modes

SPFMP: 95.43% SPFMT: 96.61% LFM: 100%

PMHFP: 0.02 PMHFT: 1.8 PMHFIm: 0

Fault Campaigns: 2 / 0 / 7

DVCUN

CONFERENCE AND EXHIBITION

EUROPE

Detailed Flow

CONFIGURATION

Design Extraction

ANALYSIS

FMEDA Hierarchy/ Design Mapping

Design Information

S/DC Target & SM Allocation

Permanent

Transient

VALIDATION

SM Design Mapping

FMEDA Plan

Permanent

Fault Injection Campaign Configuration

Planning

Execution Configuration

Execution

Transient

Fault Injection Campaign Configuration

Planning

Execution Configuration

Execution

RESULT

FMEDA

Safety Mechanisms

Ethernet_IP_DEMO / Detailed FMEDA

admin

FMEDA Result

Filter Options

Design Information

FM Type

Generate Report

ID	Part	Subpart	Failure Mode	Safety Relevant	λ_p	Sp %	λ_{pd}	λ_p %	DCp %	λ_{pr}
FM_1	i_gem_top	gen_tsu_i_gem_tsu	The timer value may not be captured or captured incorrectly	true	8.49e-3	6.49%	7.94e-3	2.16%	100%	0
FM_2	i_gem_top	gen_tsu_i_gem_tsu	The TSU seconds interrupt is incorrect	true	8.44e-3	6.38%	7.90e-3	2.15%	99.76%	1.92e-5
FM_3	i_gem_top	gen_tsu_i_gem_tsu	TSU compare interrupt is incorrect	true	8.44e-3	2%	8.27e-3	2.15%	98%	1.65e-4
FM_4	i_gem_top	gen_tsu_i_gem_tsu	TX/RX timestamp is corrupted, output TSU timer value to local system will be...	true	8.44e-3	2%	8.27e-3	2.15%	98%	1.65e-4
FM_5	i_gem_top	i_gem_reg_top.i_gem_registers	Fault in Parity Generators of Registers	true	4.72e-4	2%	4.62e-4	0.12%	95%	2.31e-5
FM_6	i_gem_top	i_gem_reg_top.i_gem_registers	Fault in static configuration outputs from the registers	true	1.84e-1	2%	0.18	46.83%	95%	9.00e-3
FM_7	i_gem_top	i_gem_reg_top.i_gem_registers	Fault in dynamic control outputs from the registers	true	1.74e-1	2%	0.17	44.43%	95%	8.54e-3

Generate Report in Excel Format

1 Parts / 2 Sub-Parts / 7 Failure Modes

SPFMp: 95.43% SPFMT: 96.61% LFM: 100%

PMHFP: 0.02 PMHFT: 1.8 PMHFIm: 0

Fault Campaigns: 2 / 0 / 7

Summary

- Integrated functional + safety verification flow and engines
 - Reduce effort of developing & maintaining different environments
 - Highest performance native fault simulation
- vPlan-based requirements traceability, with FMEDA plan based metrics analysis
 - Use FMEDA user strategy to reduce amount of required fault simulation
 - Integrate design data for accurate analysis
- Automate the functional safety verification tool flow
 - Reduce the human effort whenever possible, automate all possible steps
 - Minimize the Fault Injection Campaign Set-up time
 - Reuse of Functional Verification Environment
- Execution core
 - Optimized flow to improve the TAT and optimized usage of each involved feature
 - Use coverage data to reduce the number of test to be executed
 - Utilization of formal techniques to reduce the fault space
 - Intelligent algorithms to minimize the number of fault to be injected and executed
- Cadence provides the most comprehensive solution for Functional Safety

Thanks