Making Autonomous Cars Safe

Joern Stohmann, Frederico Ferlini

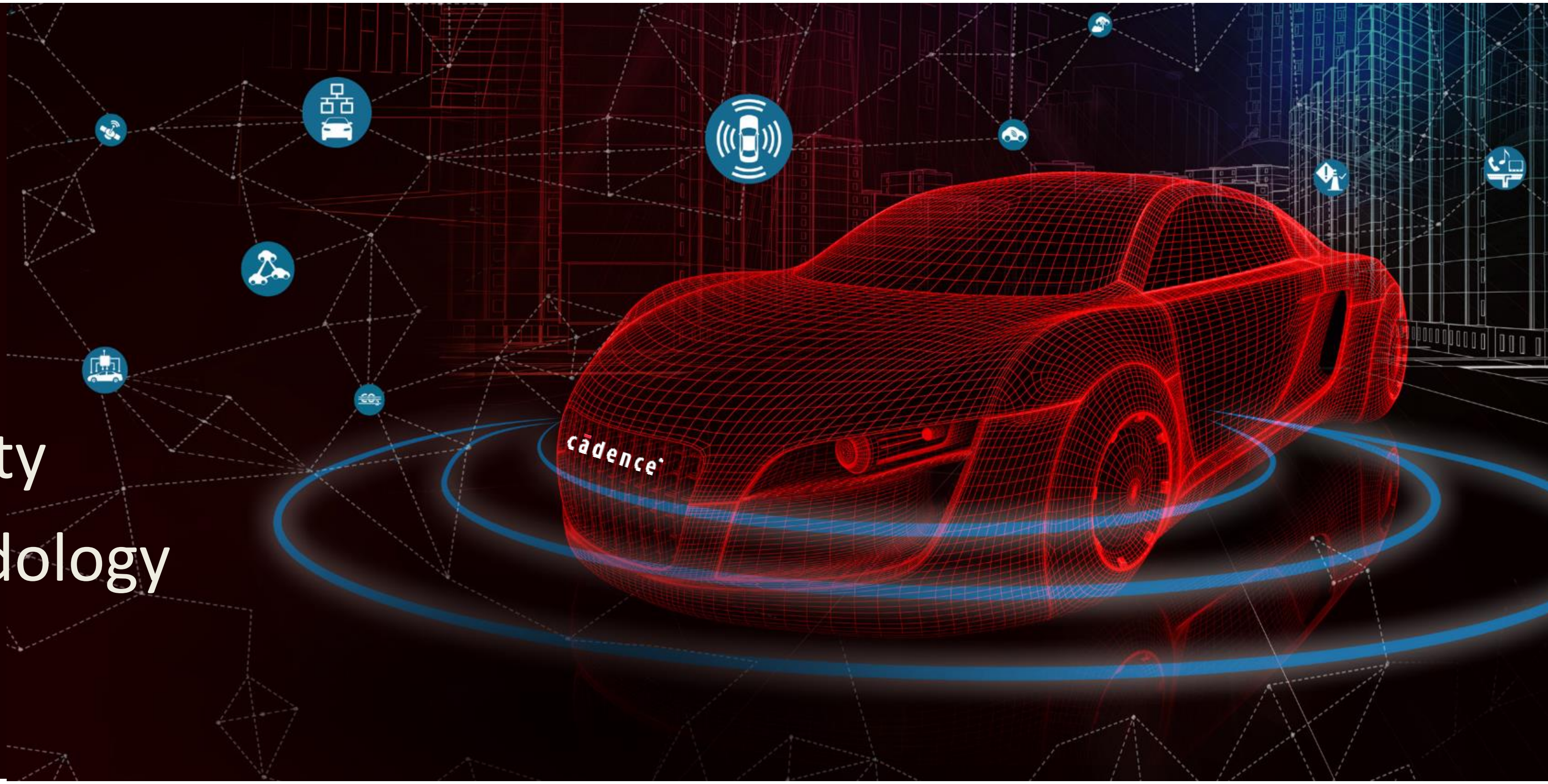
cadence®

Accellera Systems Initiative

2017 Design and Verification™ DVCon Conference and Exhibition Europe

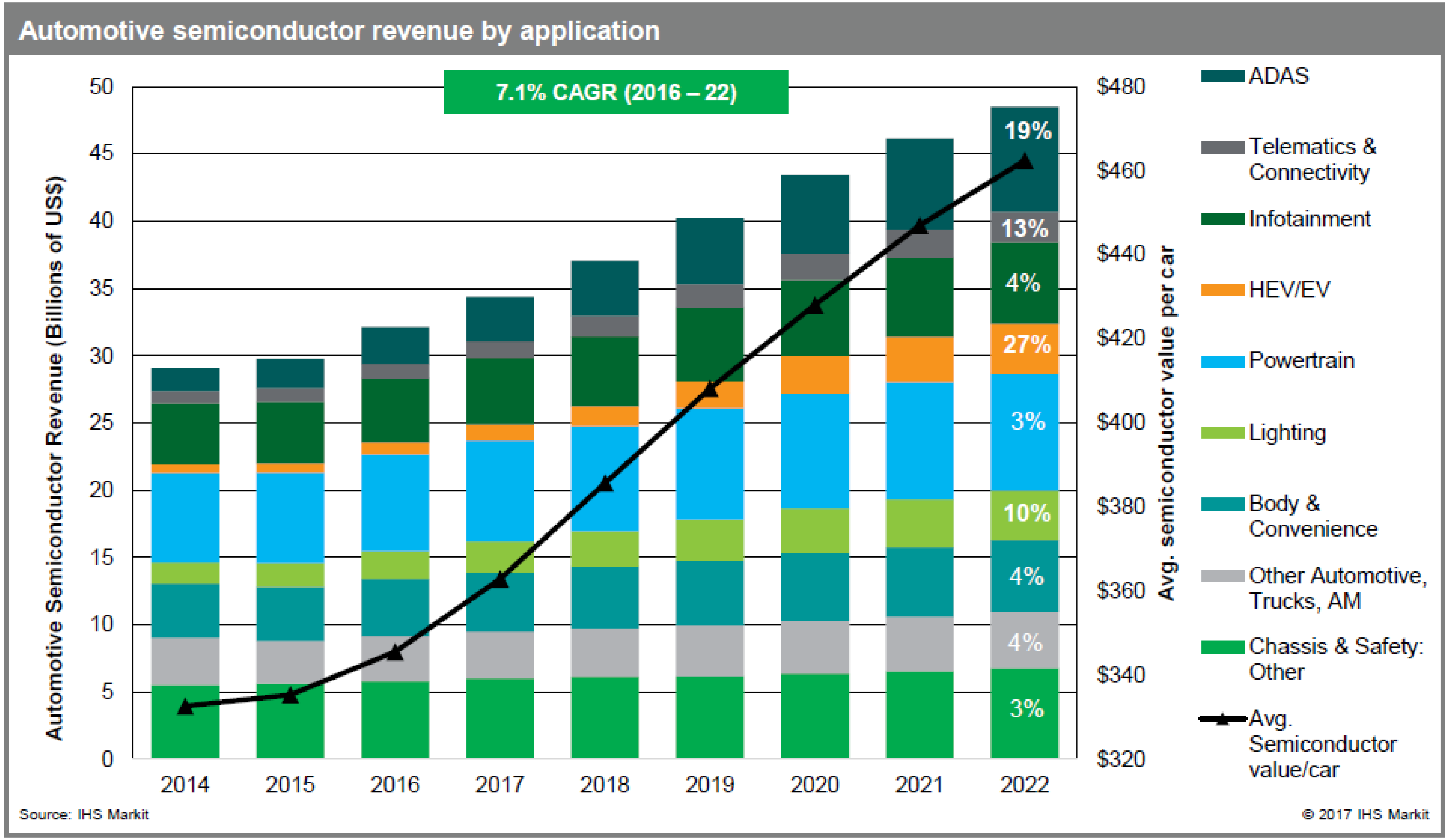
Agenda

- Automotive Market
- Complex Challenges
- ISO 26262 and Basic Safety
- Functional Safety Methodology



The Automotive Market

Automotive Semiconductor Growth



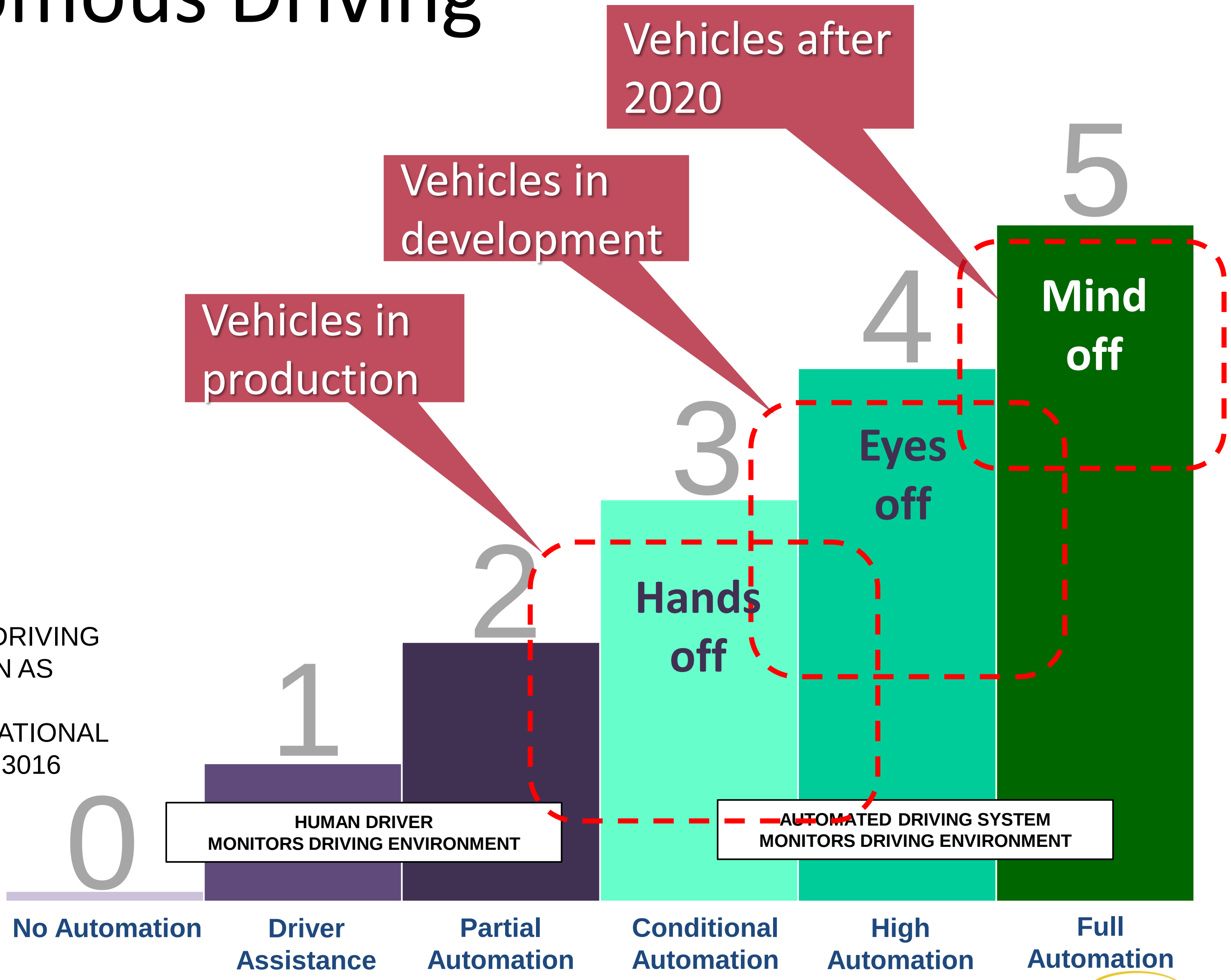
Forces Shaping the Automotive Industry

"Automotive Revolution – Perspective towards 2030" – a **2016 McKinsey Report identified 4 areas that deemed particularly important in shaping the auto industry thru 2030**

Vehicle electrification	Increased Connectivity	Growth of Autonomous Driving	Shared Mobility Services
Advances to solve • High battery costs • Proliferation of charging infrastructure	Advances to • 5G deployment • Telematics services • V2I; V2V	ADAS deployment • Cost effective Level 3 and Level 4 by 2020~2025	Proliferation of • Ride sharing services • Car sharing services

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



LEVELS OF DRIVING AUTOMATION AS DEFINED IN SAE INTERNATIONAL STANDARD J3016

Automotive Opportunities and Focus Areas

ADAS			Infotainment			Automotive SoC Sign-off		
Camera	Radar	Lidar	Audio	Voice	ANC,…	Safety	Security	Reliability
Sensor Fusion			Basic ADAS Features			ISO26262, AEC-Q100,…		

High-performance computing
- Scalability
- High resolution
- Low power
- Vision + CNN
- Memory bandwidth
- Safety and Security is a must!

Highly integrated cockpit
- Scalability
- Connectivity
- In-vehicle networking
- SW app availability
- Comprehensive I/F support
- Basic ADAS features

Qualification of new SoCs
- Safety, Security and Reliability
- FMEDA not sufficient for SoCs
- Integrated FMEDA and safety verification flow
- Interfaces to RM & Tracing tools

Complex Challenges

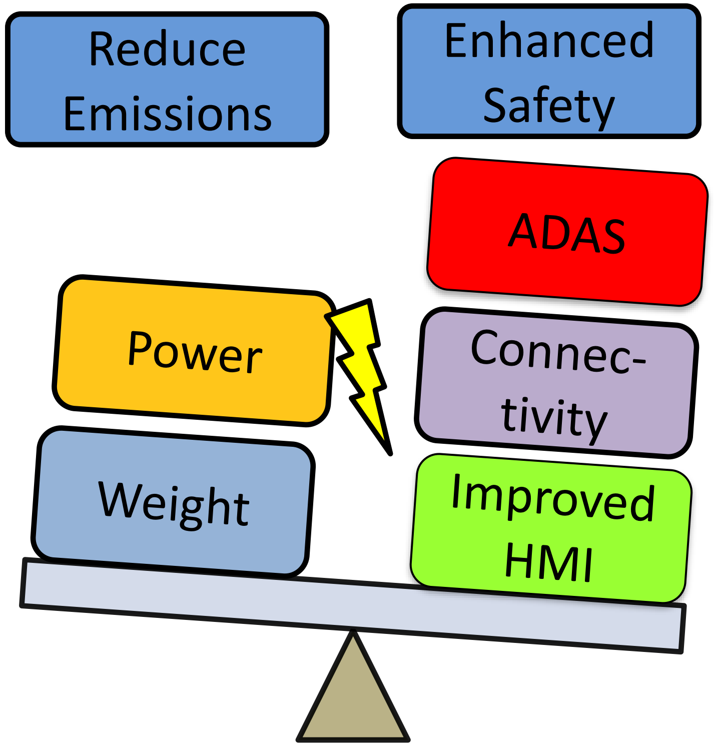
The Megatrends Dilemma

Efficient Electric Vehicles

Source: BMW

Government Regulations

EURO NCAP Program



Safe Autonomous Cars

Source: Volvo

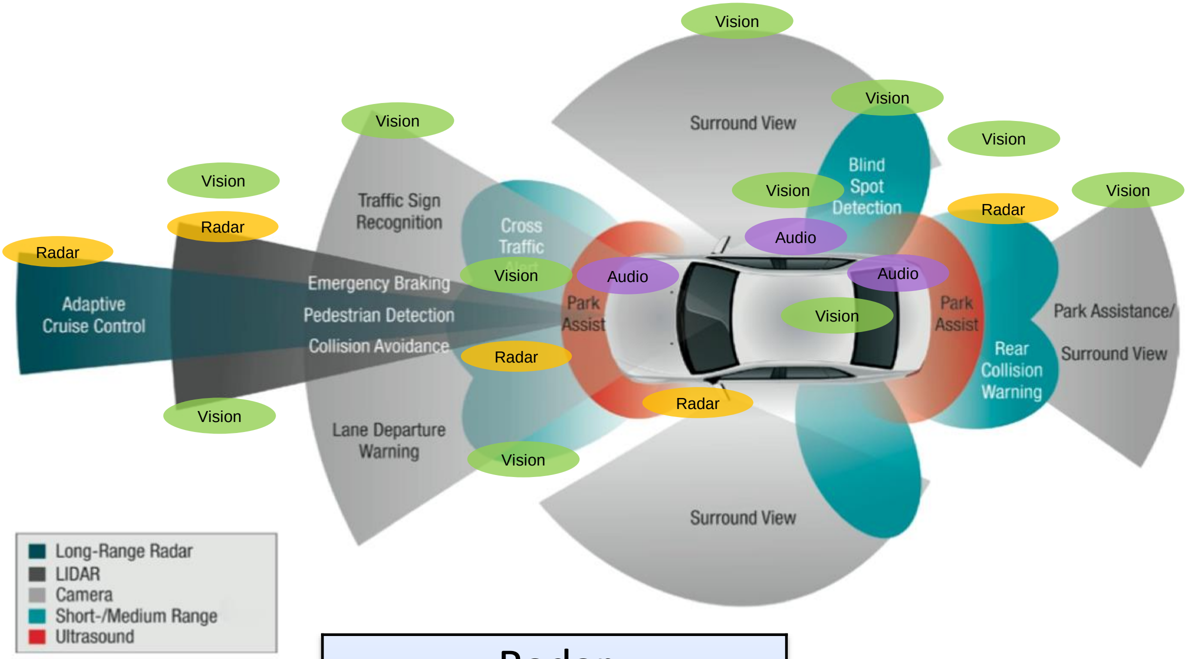
Need low-power, small footprint, high-performance SoCs

Making a Car Autonomous

Audio

Rear Object Detection
Parking Assist/Auto Park
Voice Recognition
Cabin Noise Reduction
Emergency Recognition
Spatial Audio for Warnings

HiFi DSP



Fusion

Radar, LIDAR, Image correlation
System Functional Safety
System Data Control

Fusion DSP

Radar

Front Collision Avoidance Braking
Adaptive Cruise Control
360 degree Hazard Awareness
Rear Collision Detection

ConnX DSP incl. V2X

Active Vision (LiDAR)

Adaptive Cruise Control
Collision Avoidance
Blind Spot Detection

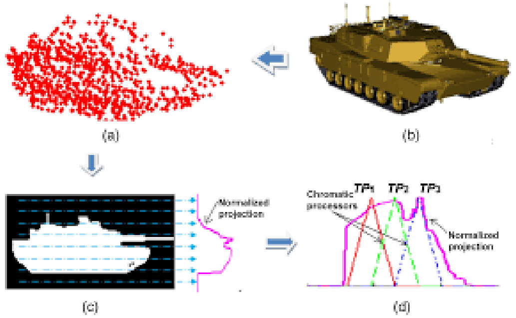
Passive Vision

Rear View Camera
Vision Enhancement
Auto Dimming Headlights
Blind Spot Detection
360 View
Parking Assist
Lane Detection and Following
Sign Recognition
Traffic Signal Recognition
Rain, Snow, /Fog Removal
Pedestrian Tracking /Avoidance
Eye Focus Detection
Driver Monitoring
Vehicle Detection/Avoidance

Vision DSP

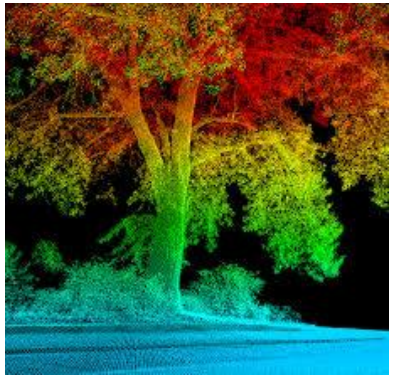
Complicated Convolutional Neural Networks

Radar Point Cloud



~10-100 KB/sec

Lidar Point Cloud



~10-70 MB/sec

Digital Camera

~20-40 MB/sec

Automated and Reliable Object
Recognition
using CNN

Need a high-performance, low-power hardware platform to combine and analyze point clouds and accurately identify objects

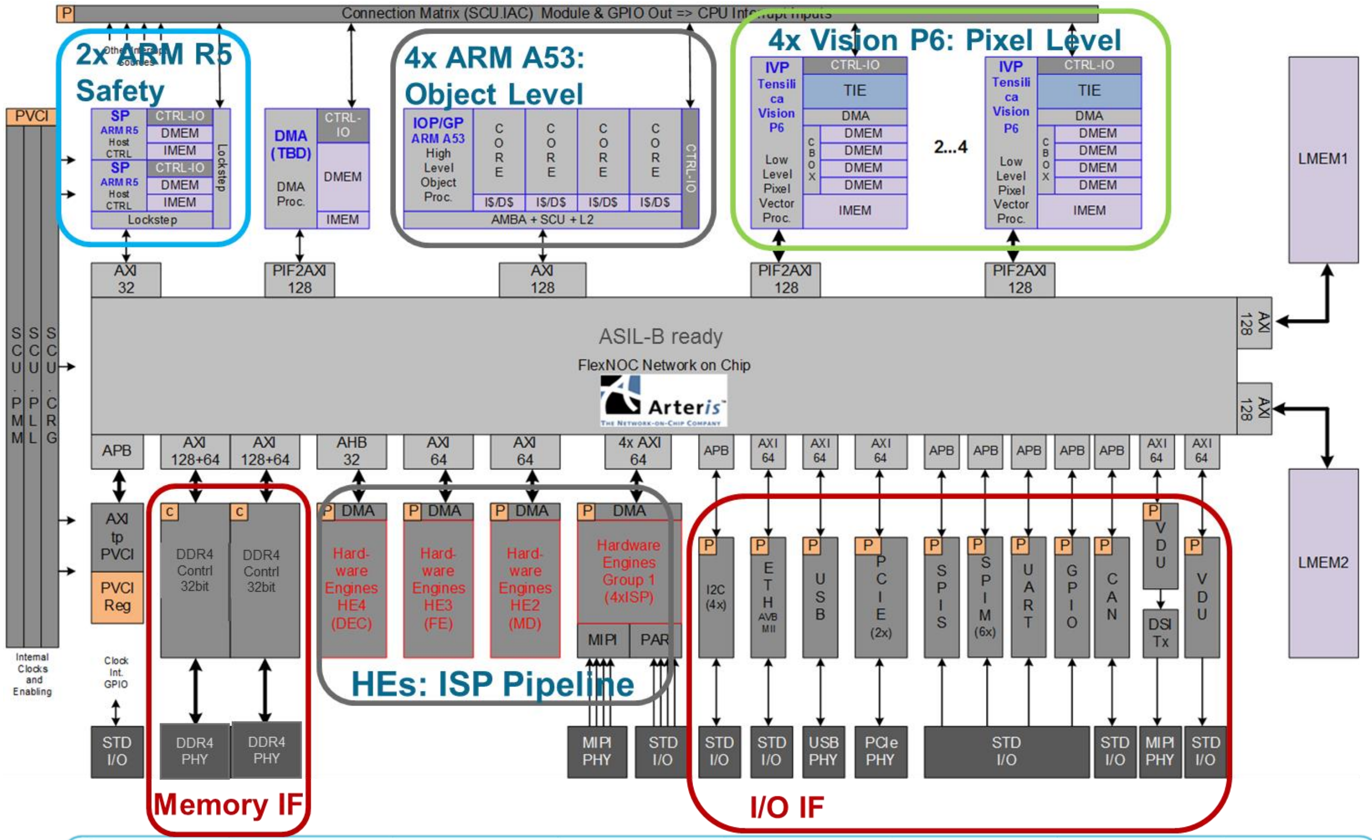
Automotive SoC Verification Challenges

Systematic Failure Verification

- Concurrent SW Development
- Requirements Traceability
- Use Case Verification
- Performance Verification
- Security Verification
- Automotive Protocol Verification
- Mixed Signal Verification
- Functional Safety Verification

Random Failure Verification

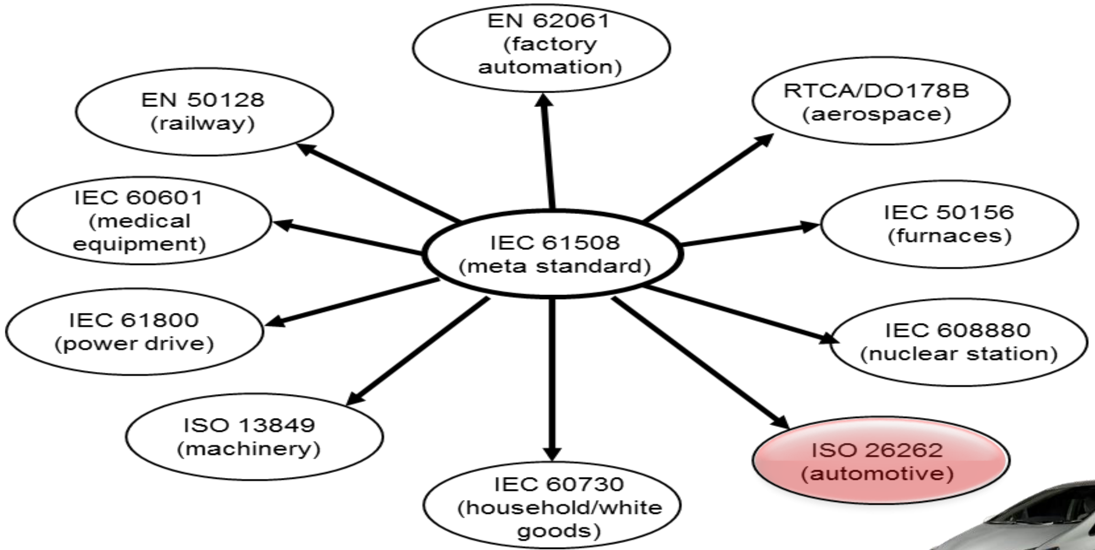
ADAS SoC Example

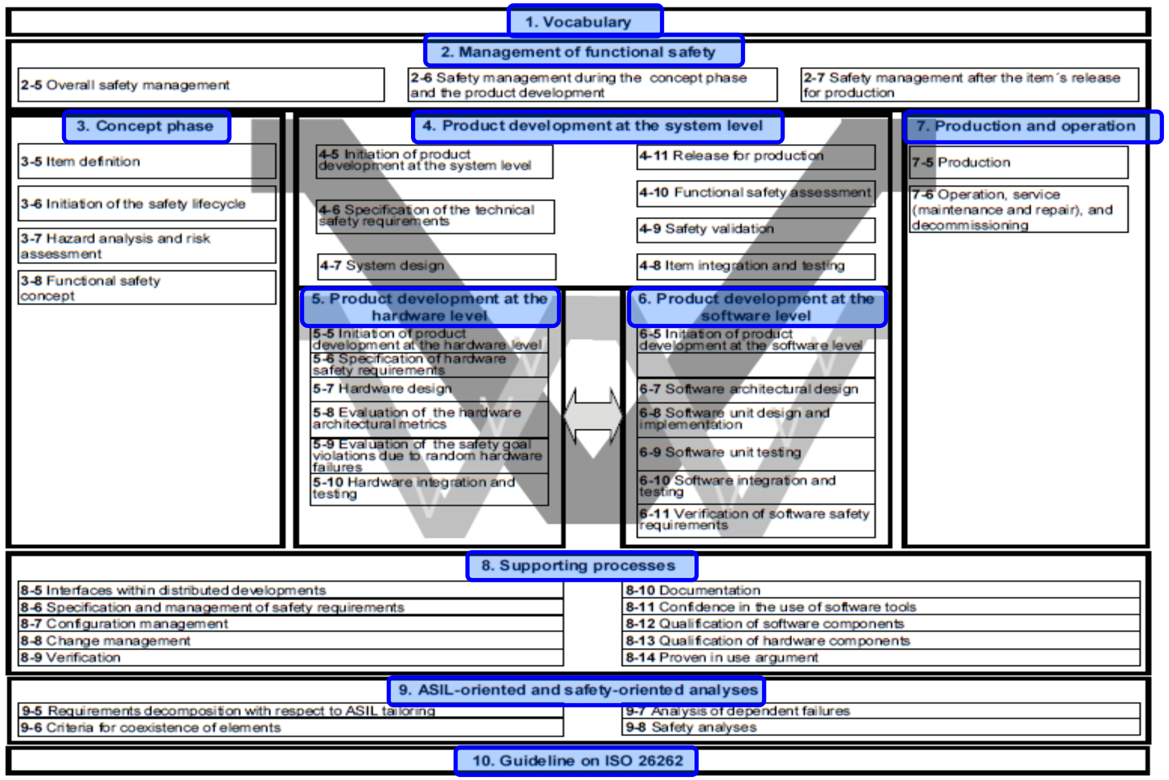


Multiple verification and validation platforms

ISO 26262 and Safety Basics

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)

Malfunction → How much harm can the malfunction cause? (**risk**) → What level of safety integrity (**risk reduction**) is needed?

LOW — ASIL (Automotive Safety Integrity Level) → HIGH

A B C D

Dashboard

Airbag not firing

Braking

ASIL examples for illustration purposes only

ASIL determination example—ISO 26262

For illustration purposes only

Malfunction	ABS system failure
Hazard Analysis	What unintended situations (hazards) could happen? → Loss of stability on split-μ surface
Risk Analysis	• **How likely** is the hazard to happen? (Exposure) → oil spill, gravel, water potholes, …. • **How harmful** is the hazard? (Severity) → Car may spin out of control and crash • **How controllable** is the system if the hazard occur? (Controllability) → dashboard, driver
ASIL Determination	What level of safety (risk reduction) does the system need? • How likely can the malfunction be? → **FIT (Failure in Time)** • How often does the system need to catch it and get to a safe situation? → **DC (Diagnostic coverage)**

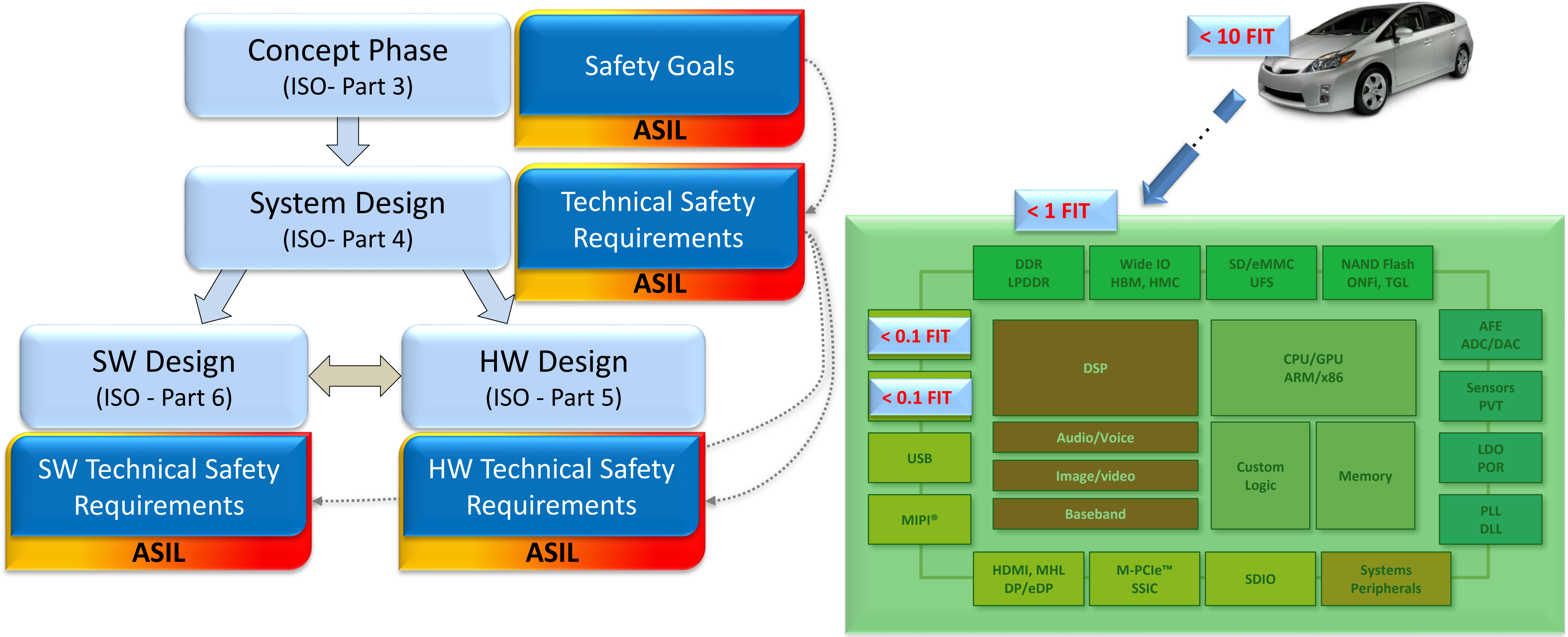
Safety Goal	Prevent ABS failure

LOW ASIL (Automotive Safety Integrity Level) HIGH

A B C D

↓ FIT (Failure In Time), ↑ Diagnostic Coverage (DC)

ISO 26262—Design and safety flow

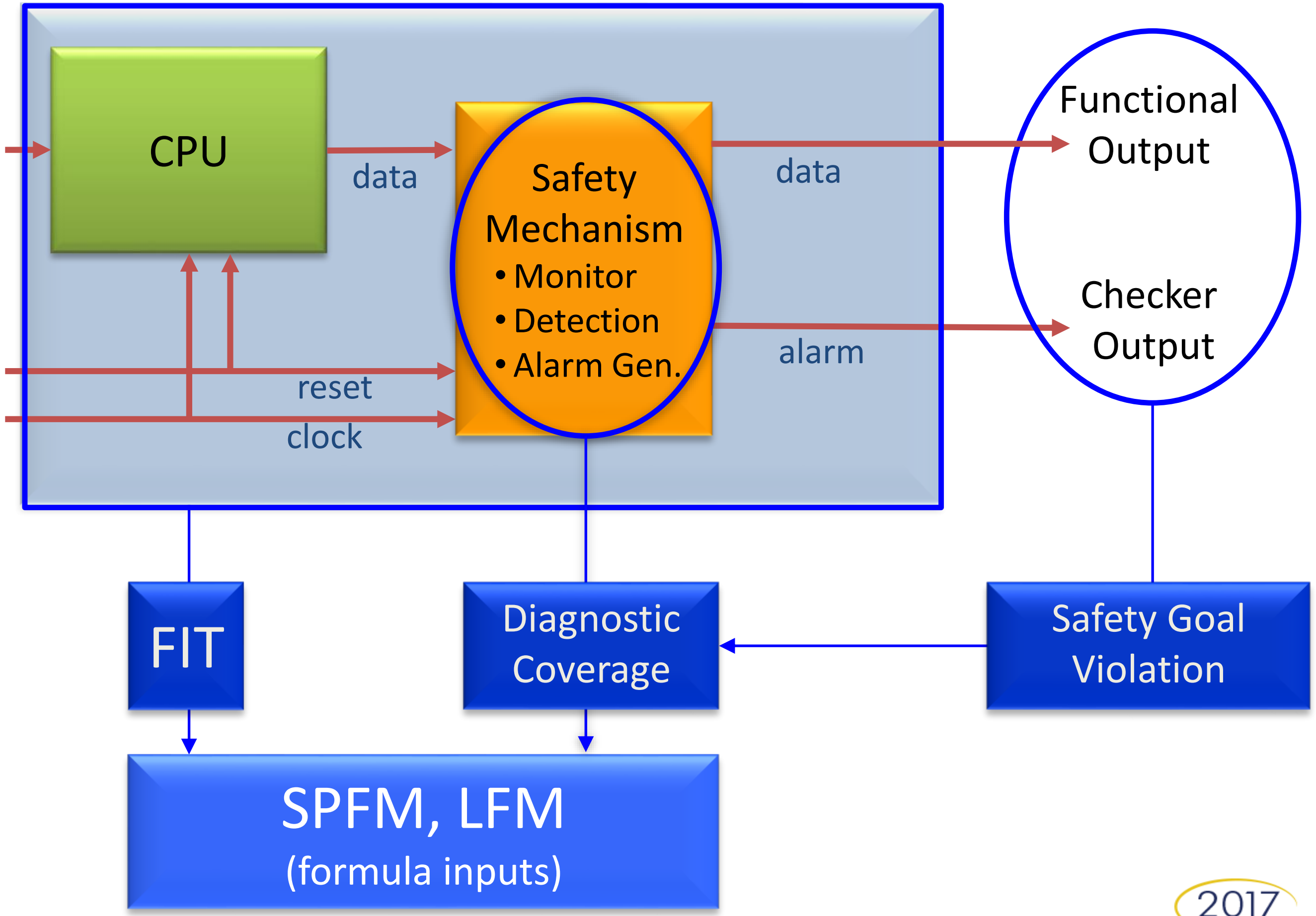


FIT gets distributed from the item to each of the elements

ASIL Hardware Metrics

ASIL	Failure Rate	SPFM	LFM
A	< 1000 FIT	Not relevant	Not Relevant
B	< 100 FIT	> 90%	> 60%
C	< 100 FIT	> 97%	> 80%
D	< 10 FIT	> 99%	> 90%

- FIT Failure In Time (1 Failure / 10^9 hours)
- SPFM Single Point Fault Metric
- LFM Latent Fault Metric



ISO26262—Functional Safety principles

Systematic Failures

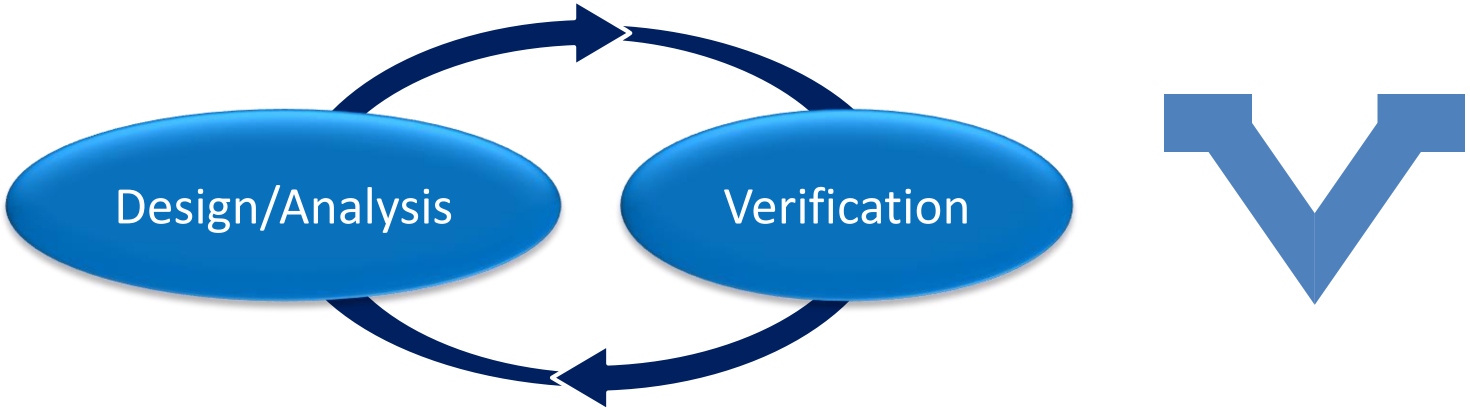
(e.g., software bug)

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

Random Failures

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

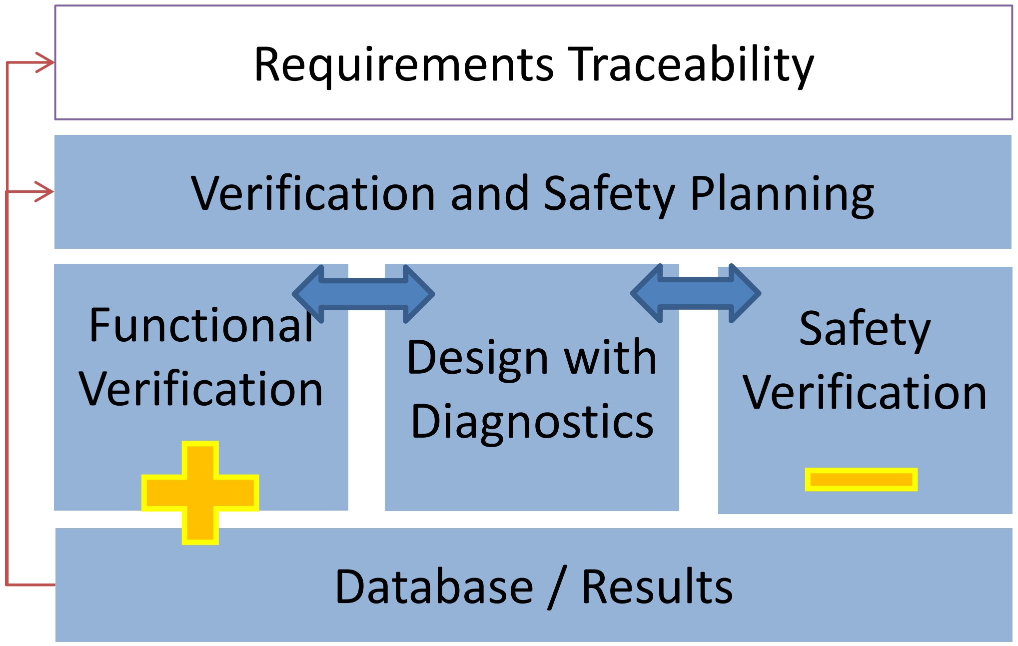
- Considers permanent failure and transient effects
- Includes **safety mechanisms** design and integration to handle faults
- Demonstrated by calculations of Reliability/verification of failure rates
- Failure rates and diagnostic coverage requirement depend on ASIL



ISO 26262 covers random and systematic errors

Functional Safety Methodology

Build a Holistic Solution



- Integrate Safety Mechanisms to reduce the FIT
- Positive testing (functional verification)
  - Verify proper functionality prior to safety verification
- Negative testing (assess diagnostic capability):
  - Targeted tests to confirm failure mode assumptions
  - Statistical tests to ensure design function integrity
  - Transient faults testing to provide evidence safety mechanisms integrity

Build Chips for Safe Autonomous Automobiles

Current Need

- A dedicated functional safety verification methodology and process for these safety-critical IPs and SoCs
- Safety analysis in semiconductor such as fault injection, fault metrics, base failure rate estimation, interfaces within distributed developments, handling of Hardware Intellectual Property (IP)

Methodology

- Holistic methodology which combines analytical methodologies such as FMEDA with dynamic fault simulation and formal analysis based methodologies to significantly reduce the safety verification effort and achieve faster product certification

Metrics

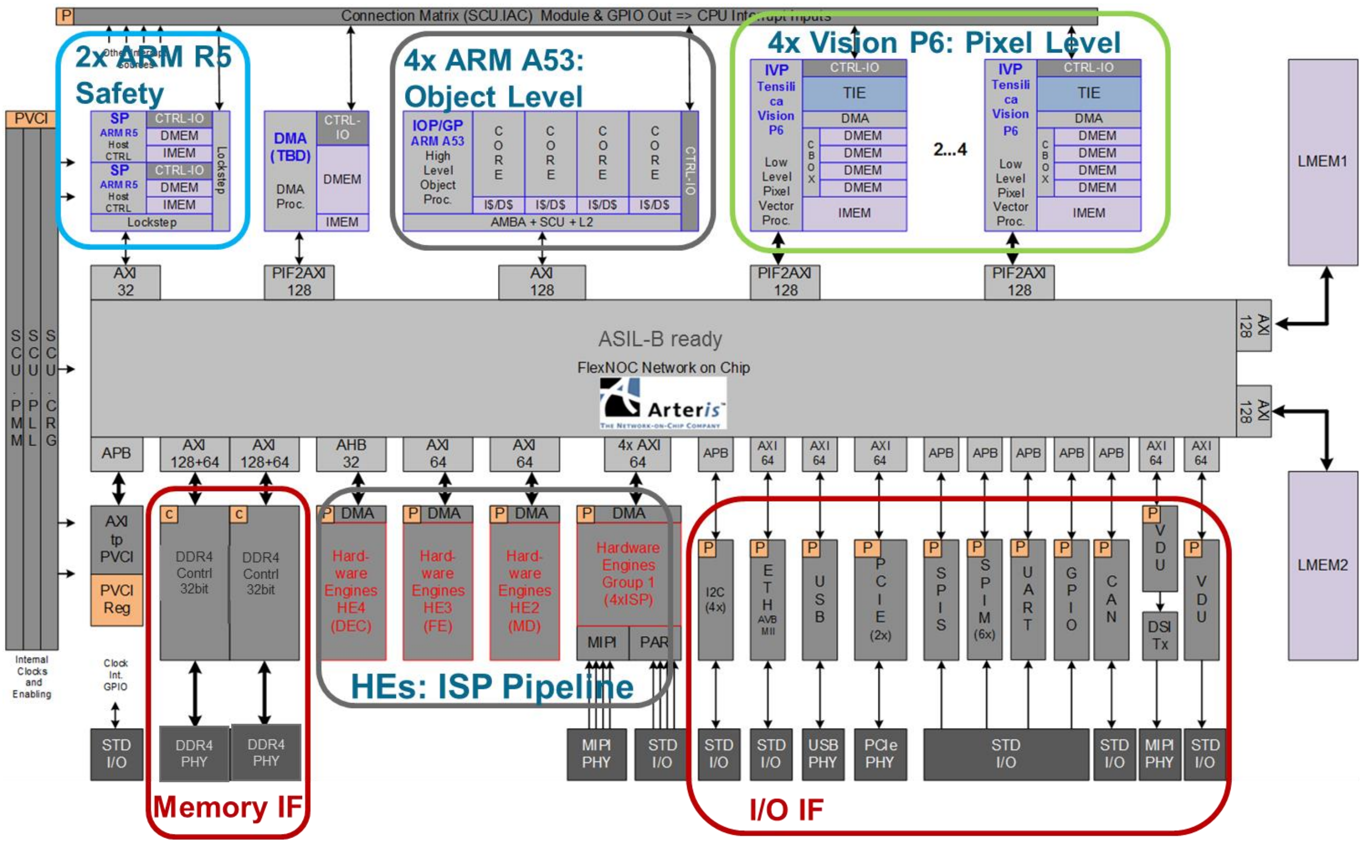
- ISO26262 recommends single point fault metric (SPFM) and Latent Fault Metric (LFM) for the component (IP and SoCs)
- Will be measured for each of the identified Safety Goals associated with the safety critical modules within the IPs and/or SoCs.

Safety Verification Challenges and More

- Failure Mode Definition
- Safety Mechanism Design
- Fault Campaign Planning
- Safety Requirement Traceability
- Fault Set (+Optimization) Execution
- Verification Environment Re-use
- Multiple Engines Support
- Link to FMEDA (Metrics Calculation)

Tool Confidence Level (TCL)

ADAS SoC Example



Safety Certified IPs

FMEDA – capture and analyse safety goals

SoC Part

IP Subpart

Failure Mode

Failure Rate

Safe Fraction

Failure Mode Distribution

Diag. Cov.

HW Safety Mechanism

SETTINGS				
P	FIT/gates	1,20E-05	NAND2	1
T	FIT/gates	1,64E-03	FLIP FLOP	8

SPFMp	59,97%	SPFMt	52,76%
LFM	not calculated		

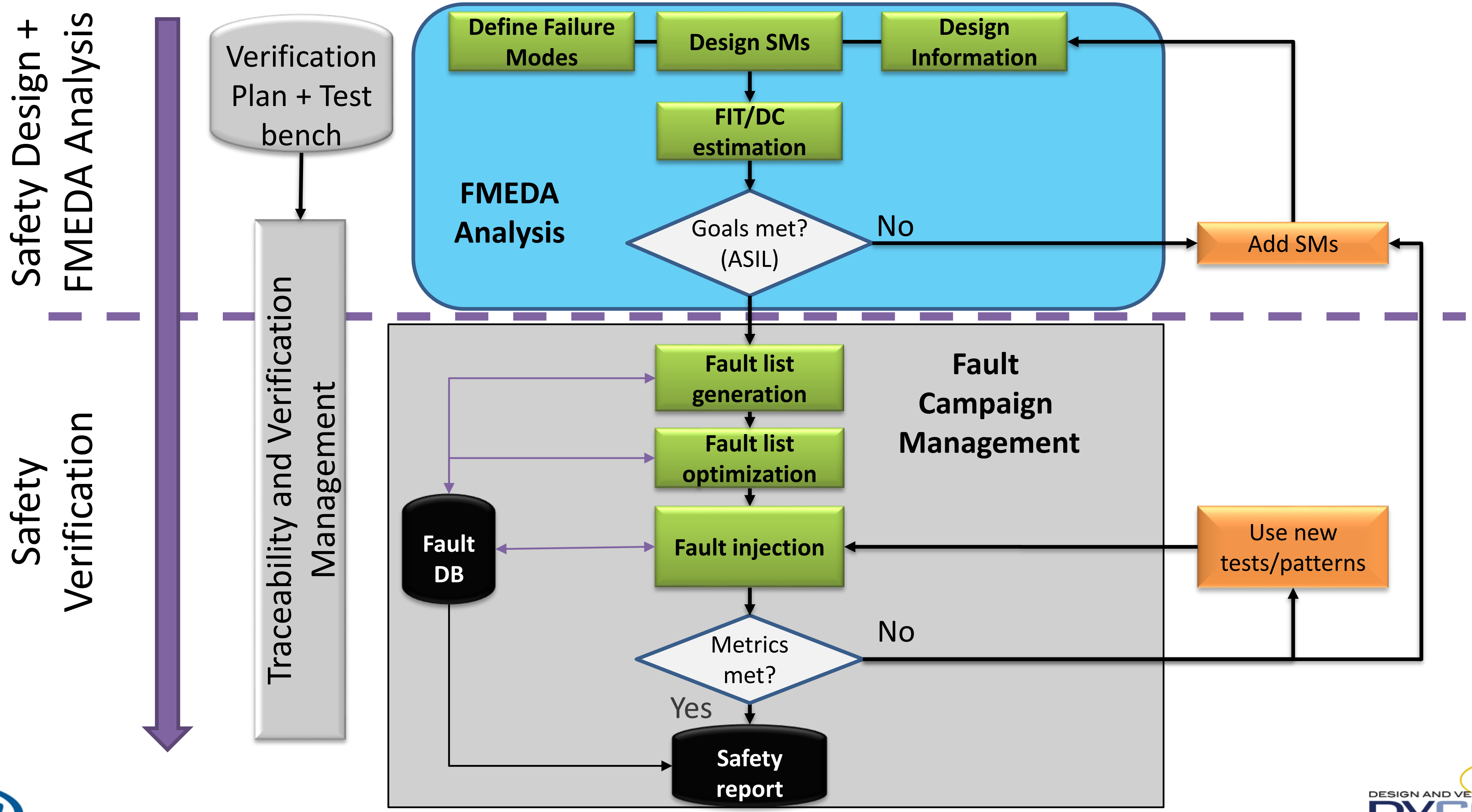
						PERMANENT					TRANSIENT								
ID	PART	SUBPART	Failure Mode	#Gates	#Flops	λp	Sp %	λpd	λps	λpd %	λt	St %	λtd	λts	λtd %	DCp	SMp	DCt	SMt
1	CPU	BUS_ITF	Wrong Data Transaction caused by a fault in the AHB interface	836	23	0,010	0,26	0,007447	0,00262	100,00%	0,039099	40%	0,023459	0,015639	100,00%	30%	E2E	30%	E2E
2		DECODER	Incorrect Instruction Flow caused by a fault the decode logic	326	9	0,004	0,01	0,003885	0,00004	100,00%	0,015298	15%	0,013003	0,002295	100,00%	60%	CTRL FLOW, WD	60%	CTRL FLOW, WD
3		VIC	Un-intended execution/not executed interrupt request	141	4	0,002	0,26	0,001256	0,00044	100,00%	0,006793	40%	0,004076	0,002717	100,00%	60%	INT MONITOR	60%	INT MONITOR
4		ALU	Corrupt data or value caused by a fault in the register bank shadow	7465	206	0,018	0,01	0,017841	0,00018	20,13%	0,069709	15%	0,059252	0,010456	19,81%	60%	PARITY	60%	PARITY
5			Incorrect Instruction Result caused by a fault in the multiplier			0,009	0,01	0,008998	0,00009	10,15%	0,035685	15%	0,030332	0,005353	10,14%	90%	HW REDUNDANT RANGE CHK	90%	HW REDUNDANT RANGE CHK
6			Incorrect Instruction Result caused by a fault in the adder			0,002	0,01	0,002229	0,00002	2,51%	0,008508	15%	0,007232	0,001276	2,42%	90%		90%	
7			Incorrect Instruction Result caused by a fault in the divider			0,002	0,01	0,001256	0,00035	1,42%	0,006779	15%	0,005763	0,001017	1,93%	90%		90%	
8			Corrupt data or value caused by a fault in the register bank			0,030	0,01	0,029329	0,00030	33,09%	0,115579	15%	0,098242	0,017337	32,85%	95%	STL	0%	-
9			Incorrect Instruction Flow caused by a fault the pipeline controller			0,029	0,01	0,028984	0,00029	32,70%	0,115579	15%	0,098242	0,017337	32,85%	40%	CTRL FLOW, WD	40%	CTRL FLOW, WD
10		FETCH	Incorrect Instruction Flow caused by a fault the branch logic (Wrong Branch Prediction)	1606	44	0,001	0,01	0,001025	0,00001	5,35%	0,003422	15%	0,002908	0,015639	0,04574	25%	STL, WD	15%	WD
11			Incorrect Instruction Flow caused by a fault the fetch logic			0,018	0,01	0,018115	0,00018	94,65%	0,071387	15%	0,060679	0,015639	0,95426	19%	STL	0%	-
12																			
13																			
14																			
15																			
16																			
17	BUS																		
				10374	286			0,120364	0,00452				0,403188	0,104706					

LINK

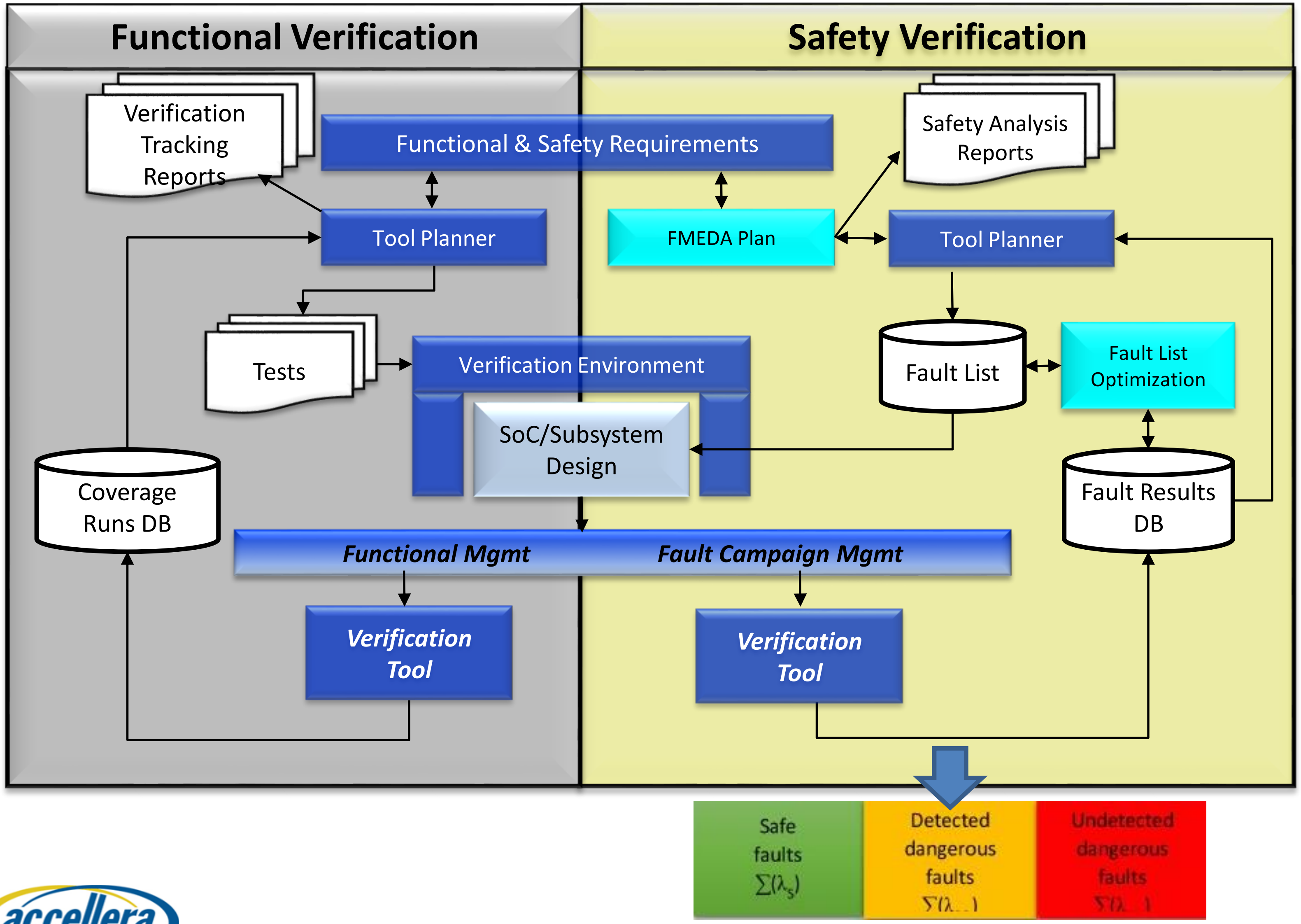
A SM can cover more the one FMs

One FM can be covered by multiple SMs

Typical Functional Safety Workflow

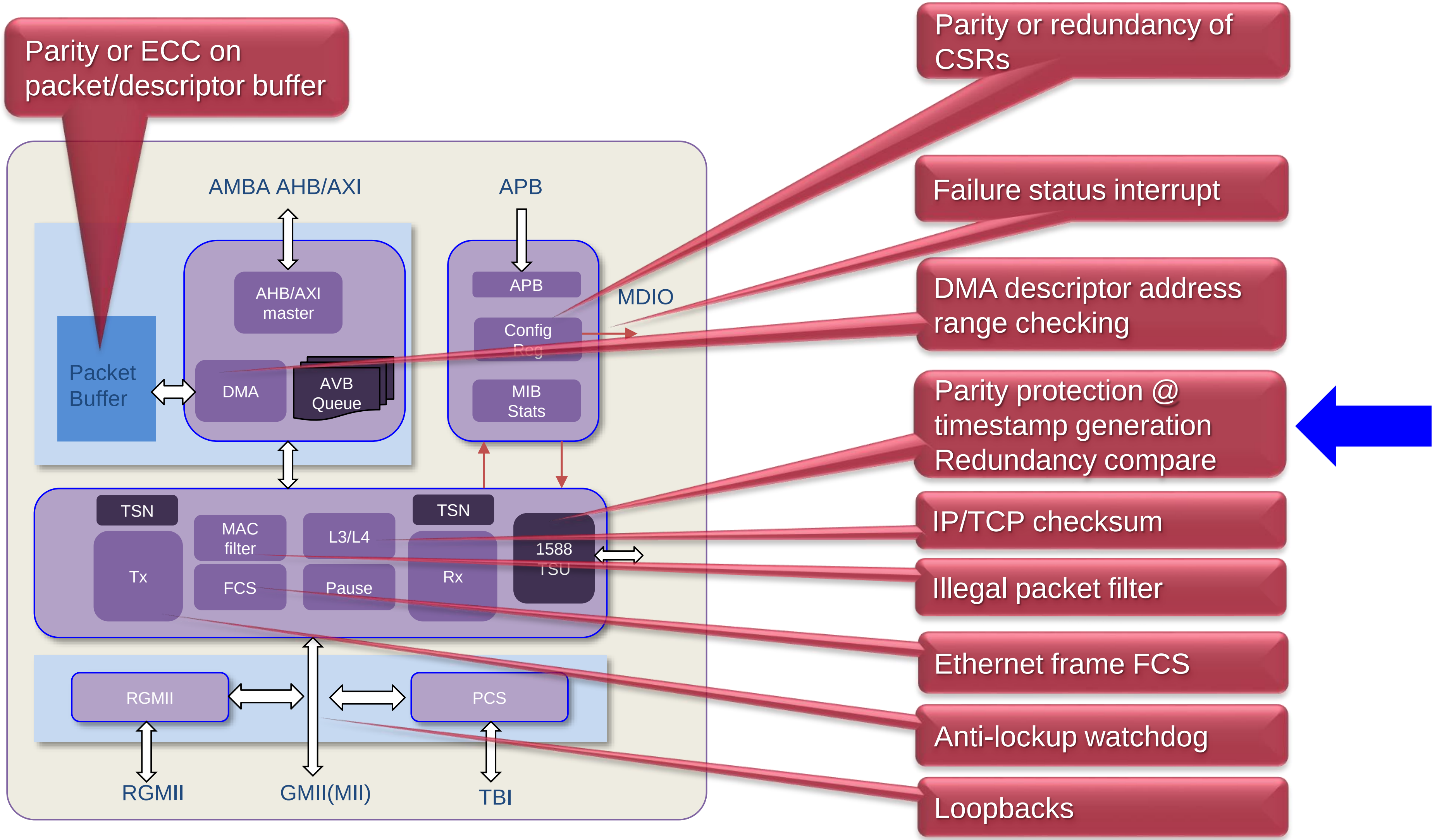


Safety Verification Solution Vision



- Unified functional + safety verification flow and engines
- Integrated fault campaign management across formal, simulation, and emulation
- Common fault results database unifies diagnostic coverage
- Proven requirements traceability, enabling FMEDA integration

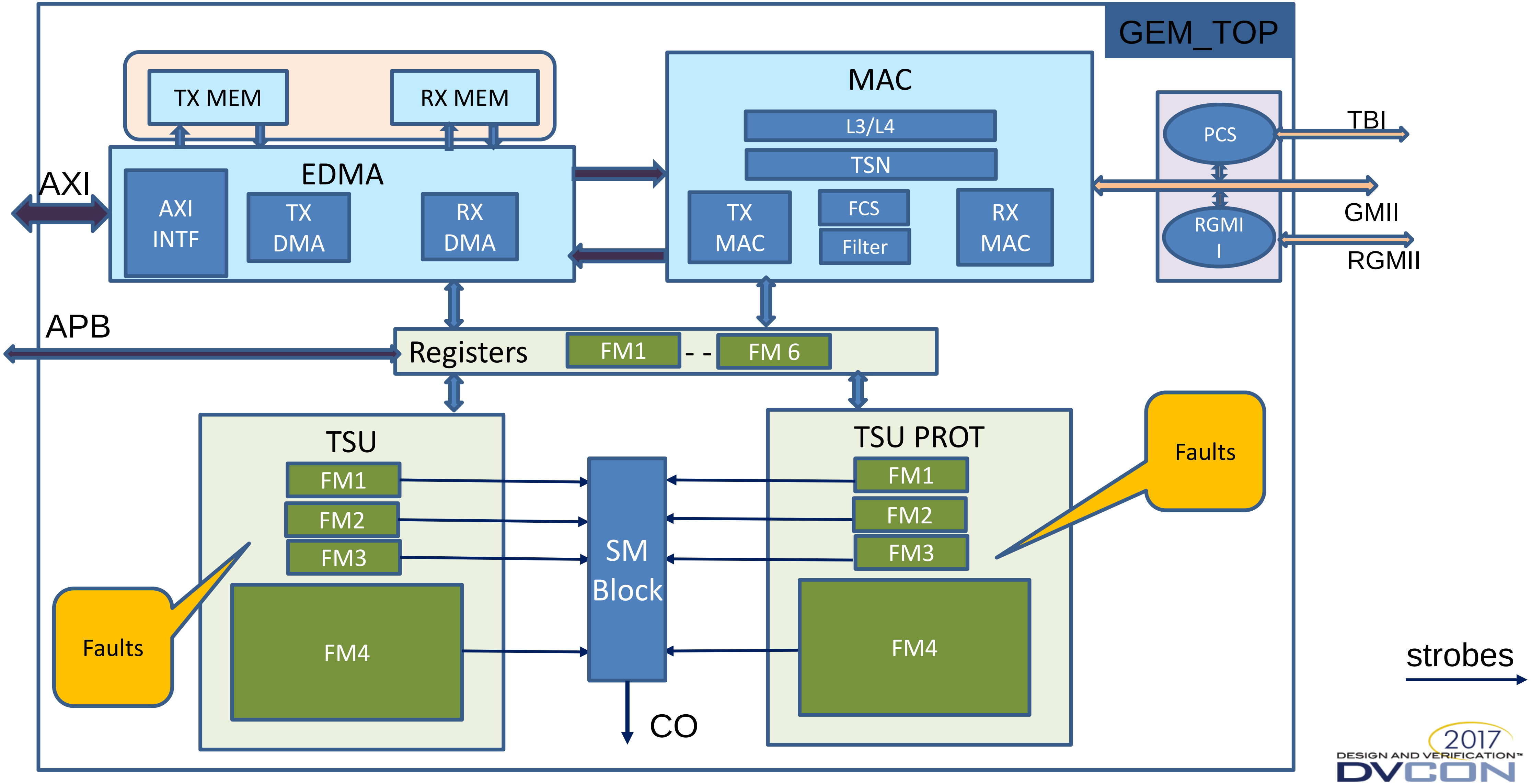
Safety Mechanisms in Ethernet IP



GEM Block – FMEDA Analysis

Block or Subblock	λ [FIT]	Failure Mode	FM Distribution	Effect Description of FM	SM Implemented
TSU	0.0719	Fault in TSU compare pulse	0.9%	TSU compare interrupt is incorrect	Compare logic is duplicated
TSU	0.0719	Fault in TSU seconds increment pulse	0.9%	The TSU seconds interrupt is incorrect	Interrupt logic is duplicated
TSU	0.0719	Fault in generation of the TSU strobe pulse to the registers	0.9%	The timer value may not be captured or captured incorrectly	Strobe Pulse Logic is duplicated
TSU	0.0719	Fault in TSU timer output value	97.3%	TX/RX timestamp is corrupted, output TSU timer value to local system will be invalid, Timer value read back in registers is also invalid.	Timer logic is duplicated
Registers	0.3013	Fault in static configuration outputs from the registers	95%	Unpredictable behavior of IP	Parity generation and detection

Ethernet IP – GEM Block

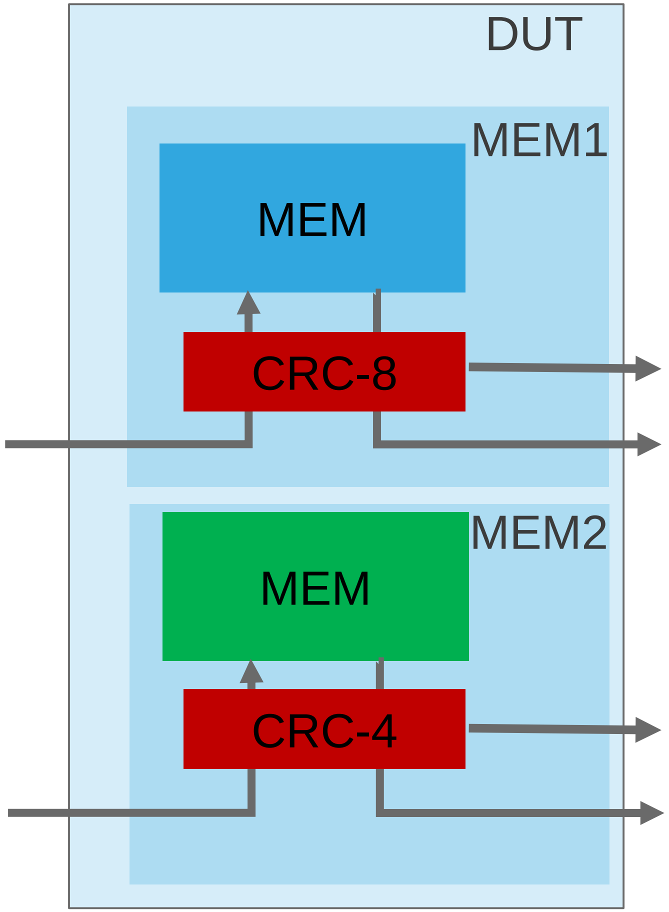


GEM Block – FMEDA Verification

Block or Subblock	λ [FIT]	Failure Mode	FM Distribution	DC Number Estimated	DC Number Achieved
TSU	0.0719	Fault in TSU compare pulse	0.9%	95%	96%
TSU	0.0719	Fault in TSU seconds increment pulse	0.9%	95%	98%
TSU	0.0719	Fault in generation of the TSU strobe pulse to the registers	0.9%	95%	78%
TSU	0.0719	Fault in TSU timer output value	97.3%	95%	100%
Registers	0.3013	Fault in static configuration outputs from the registers	95%	90%	92.5%

Demo

Fault Injection Campaign – Example

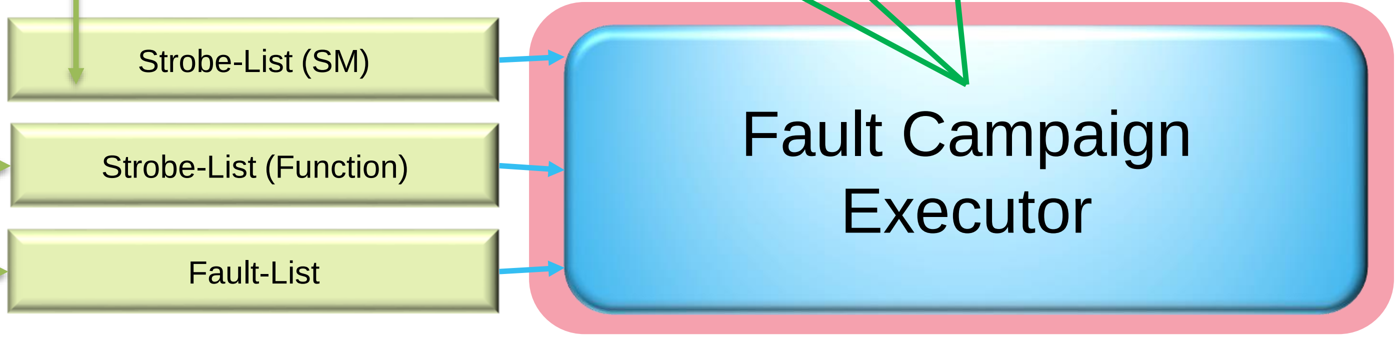


- DUT: 2 memories
  - FS Requirement: **ASIL-D**
    - E.g. HW arch. metrics: SPFM >= 99%, LFM >= 90%
- MEM1
  - Bit-Width: 32 bit
  - FS Analysis: use 8 bit CRC (CRC-8)
- MEM2
  - Bit-Width: 8 bit
  - FS Analysis: use 4 bit CRC (CRC-4)
- Reuse functional verification environment
  - Contains multiple tests
- Goal:

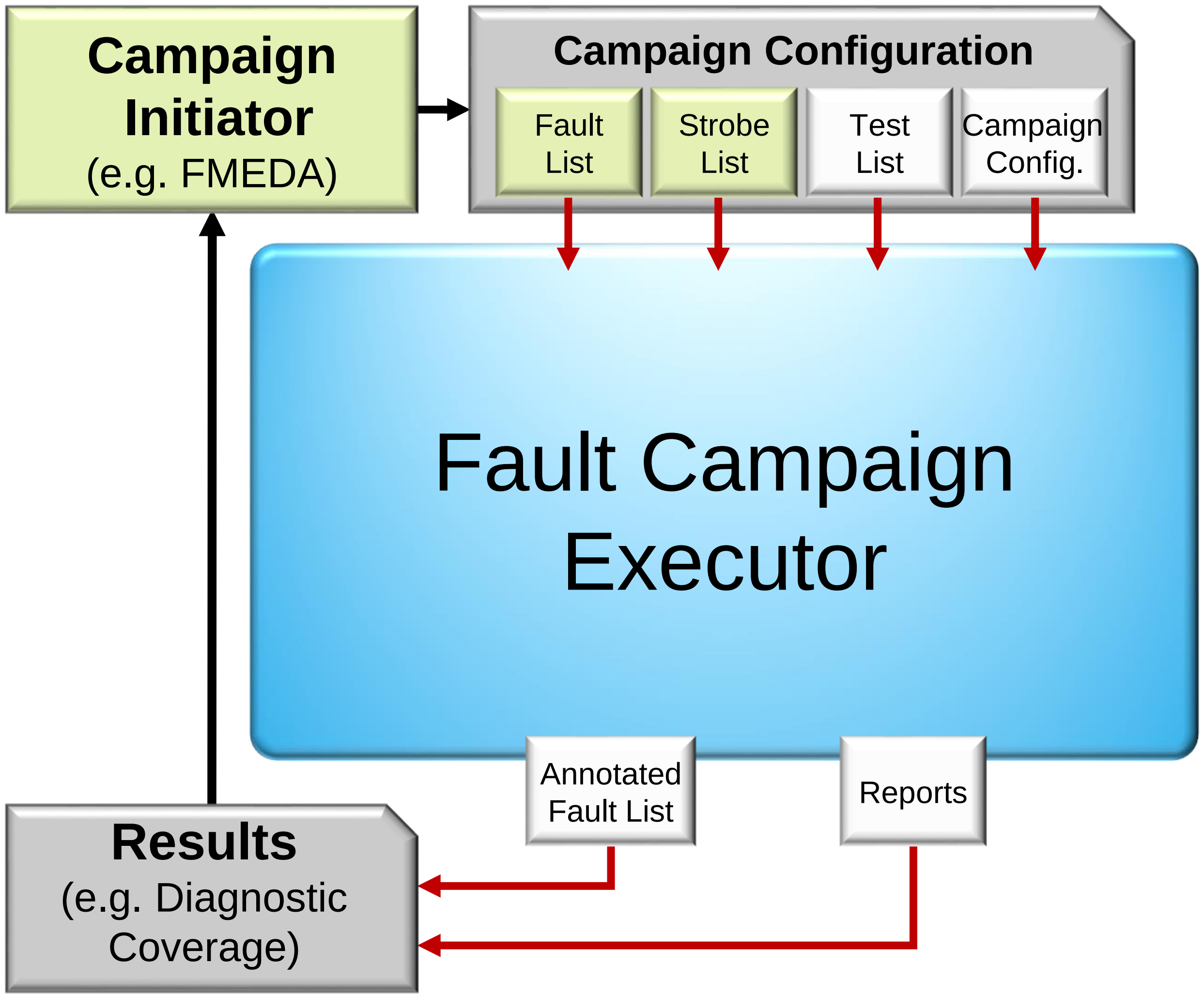
"Calculate DC values for MEM1, MEM2 required for HW architectural metrics calculation."

Mapping FMEDA to Fault Injection Campaign

Part	Sub-part	Safety related	Failure mode	Failure Rate (FIT)	Safe Faults [%]	Safety Mechanism	DC – Residual or Single Point Fault [%]	RES/SPF Failure Rate	DC – Latent [%]	Latent MP Failure Rate
DUT	MEM1	SR	permanent	4.0	0%	SMEM1	99%	0.040	90%	0.396
	MEM2	SR	permanent	1.0	0%	SMEM2	99%	0.010	90%	0.099
								0.050		0.495
							SPFM (Calc)	99.0%	LFM (Calc)	90.0%
							SPFM (Target)	>= 99%	LFM (Target)	>= 90%



Fault Campaign Executor - Interface



Inputs: FMEDA

- Fault List
  - Definition of the faults to be injected
- Strobe List
  - Definition of the observation points

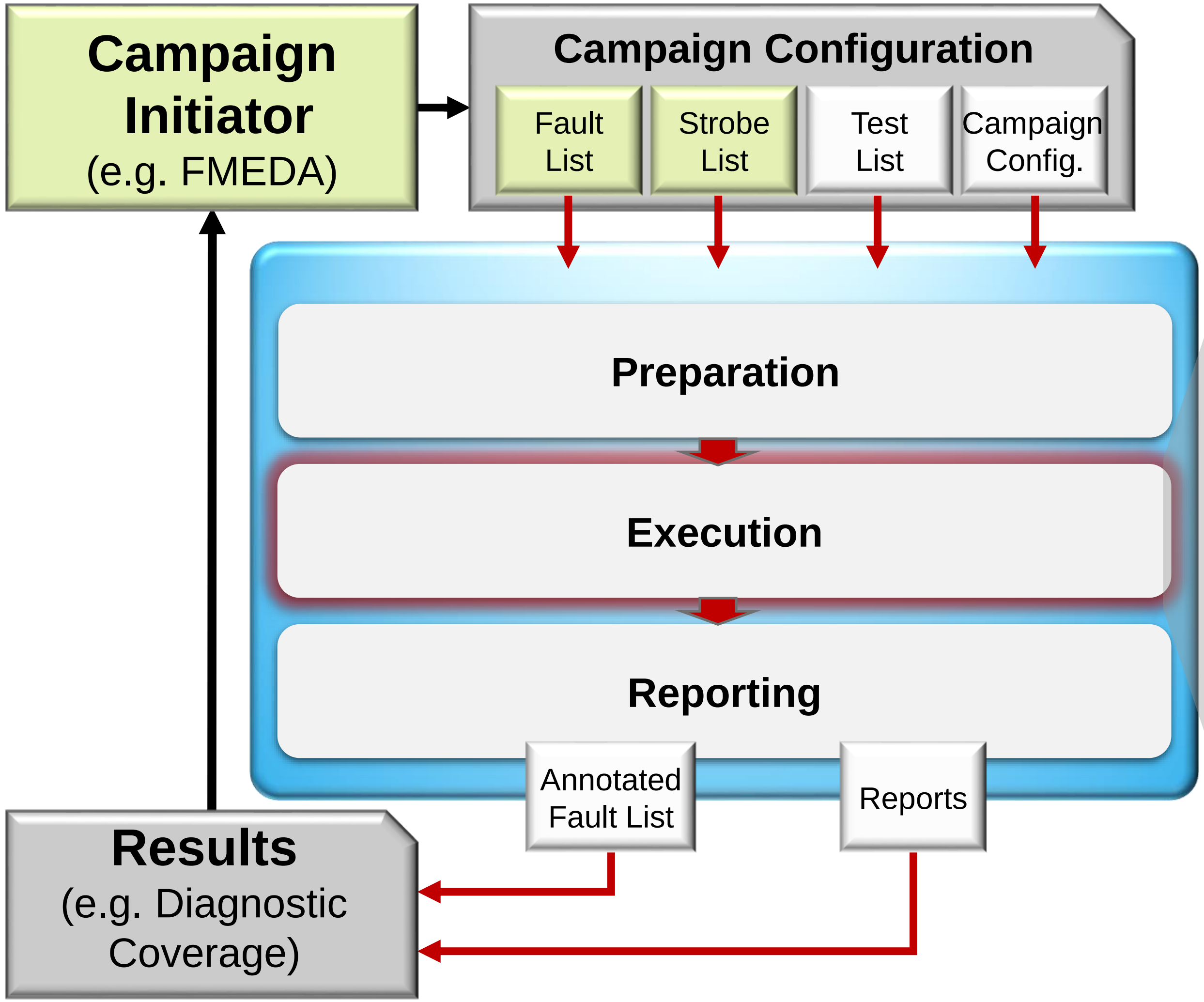
Inputs: Safety Verification Engineer

- Test List
  - Tests to be used during the campaign
- Campaign Configuration
  - Define the campaign parameters

Outputs: Safety Client

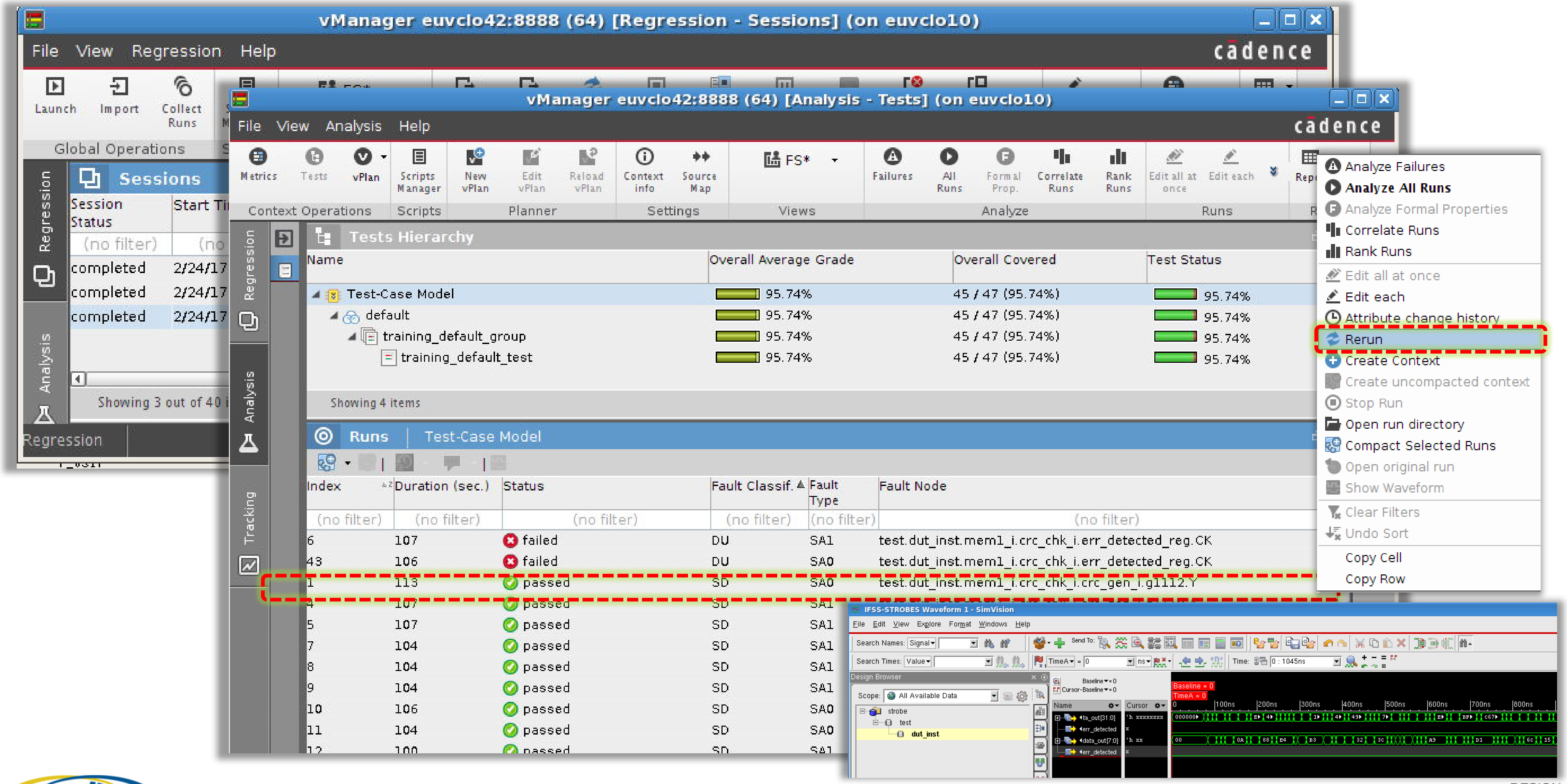
- Annotated Fault List
  - Fault classification is back annotated
- Reports
  - Various kind according to the use case

Fault Campaign Executor – Execution Flow

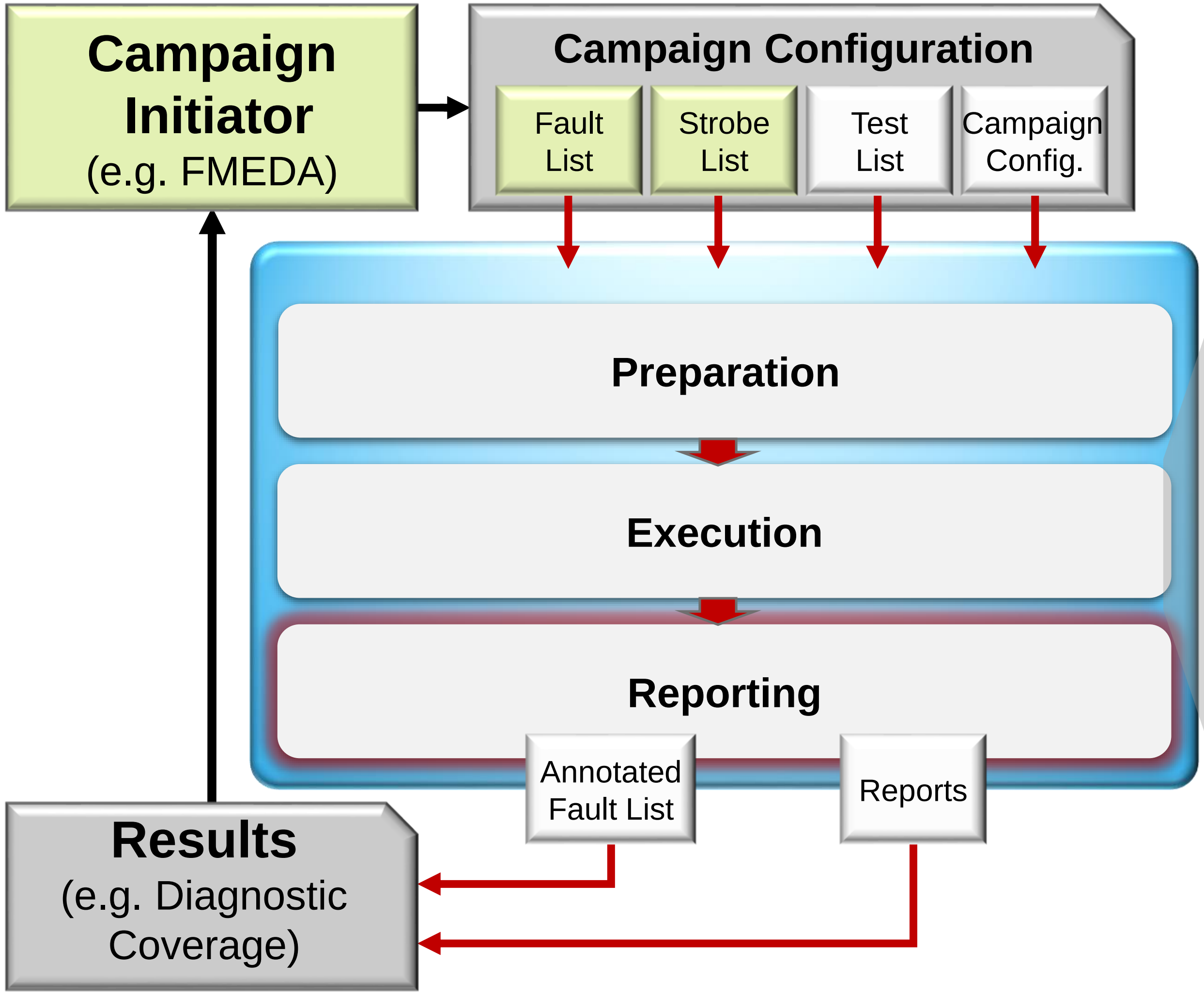


- Test selection & Ranking
  - Execute the user defined list of tests
  - Rank the user defined list of tests
- Good Simulation
  - Fault instrumentation
  - Generate strobe data for each selected test
- Fault Simulation Setup
  - Prepare fault simulation including static and dynamic (formal) fault set optimization
- Fault Simulation Execution
  - Simulate each fault with the selected tests
  - Perform dynamic optimizations

Fault Campaign Executor – GUI Example



Fault Campaign Executor – Reporting



- Comprehensive report generation
  - Campaign Execution Statistics
  - Fault Classification – Hierarchical View
  - Test execution order
  - Fault annotation list

```
-----------------------------------------------------------------------------------------
--- Fault Classification (dual strobe)
-----------------------------------------------------------------------------------------
nr faults UNKNOWN                [UK] :          0 [  0.0%]           0 [  0.0%]
nr faults UNTESTABLE             [UT] :        258 [  9.8%]         258 [ 11.6%]
nr faults       SAFE_UNDETECTED  [SU] :        160 [  6.1%]         121 [  5.4%]
nr faults       SAFE_DETECTED    [SD] :       1388 [ 52.9%]        1090 [ 48.9%]
nr faults DANGEROUS_DETECTED     [DD] :        520 [ 19.8%]         458 [ 20.6%]
nr faults DANGEROUS_UNDETECTED   [DU] :        300 [ 11.4%]         300 [ 13.5%]
nr faults total                       :       2626                 2227
-----------------------------------------------------------------------------------------
--- Results to FMEDA (Diagnostic Coverage)
-----------------------------------------------------------------------------------------
Amount of Safe Faults                 :            [  9.8%]             [ 11.6%]
DC wrt. Residual Faults               :            [ 87.3%]             [ 84.8%]
DC wrt. Latent Faults                 :            [ 92.3%]             [ 92.8%]
-----------------------------------------------------------------------------------------
```

Computed metrics to be back-annotate to FMEDA

FMEDA – estimated and simulated values

Part	Sub-part	Safety related	Failure mode	Failure Rate (FIT)	Safe Faults [%]	Safety Mechanism	DC – Residual or Single Point Fault [%]	RES/SPF Failure Rate	DC – Latent [%]	Latent MP Failure Rate
DUT	MEM1	SR	permanent	4.0	0%	SMEM1	99%	0.040	90%	0.396
	MEM2	SR	permanent	1.0	0%	SMEM2	99%	0.010	90%	0.099
								0.050		0.495
							SPFM (Calc)	99.0%	LFM (Calc)	90.0%
							SPFM (Target)	>= 99%	LFM (Target)	>= 90%

Estimated Values

Part	Sub-part	Safety related	Failure mode	Failure Rate (FIT)	Safe Faults [%]	Safety Mechanism	DC – Residual or Single Point Fault [%]	RES/SPF Failure Rate	DC – Latent [%]	Latent MP Failure Rate
DUT	MEM1	SR	permanent	4.0	10.0%	SMEM1	88.3%	0.421	94.1%	0.188
	MEM2	SR	permanent	1.0	8.7%	SMEM2	100.0%	0.000	93.2%	0.062
								0.421		0.250
							SPFM (Calc)	91.6%	LFM (Calc)	94.5%
							SPFM (Target)	>= 99%	LFM (Target)	>= 90%

Validated Values
(Fault Simulation)

Summary

Summary

- Autonomous cars are coming and ‘Mind-Off’ driving is expected to be real by the mid 2020s
- ADAS SoCs are very large, complicated designs
- ISO 26262 is the automotive standard that defines the processes to follow, the performance level for hardware and software performance and the compliance process
- A systematic analysis technique such as the FMEDA is essential for meeting ISO 26262 metrics
- Safety verification provides quantitative data useful in verifying ASIL metrics have been met

Questions