FMEDA-Driven Safety Verification

DVCon China

Xinwei Wu
September 2023

cadence®

Outline

- Automotive Trends and ISO 26262
- FMEDA Creation and Safety Analysis
- Safety Verification
- Summary

Automotive Market and Key Trends

- Still strong Automotive Semiconductor Growth
  - CAGR of 11.1%, 2021-2027 (Source: YOLE Intelligence, 10/2022)
  - Main drivers are SW-defined vehicles, Autonomous Driving, EVs
- Drive towards leading-edge technology nodes
  - 3D-IC design, Chiplets
  - 5nm, 3nm gate-all-around (GAA)
- Industry Responding to Supply Chain Disruption
  - OEM and Tier-1s initiating SoC designs
  - Traditional semiconductor companies entering the automotive market
  - Startup companies developing autonomous driving platforms and sensors

Autonomous Driving

Digital Cockpits & Connectivity

4G → 5G, V2X

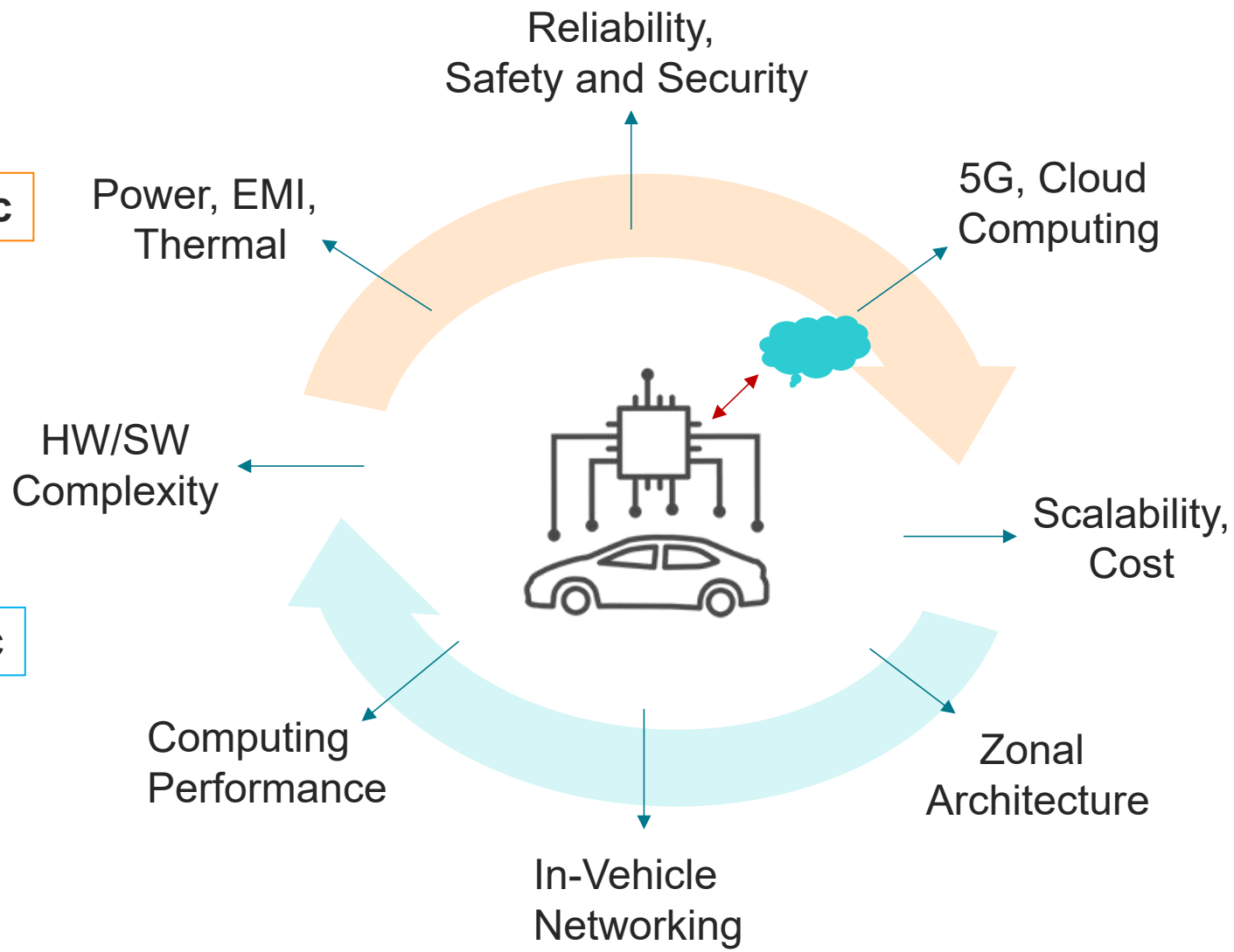
Electrification Hybrid & EVs

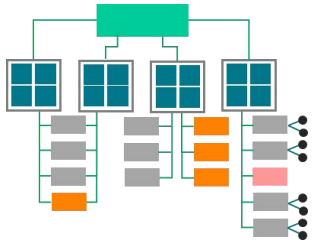
Semi (8.1%) → Auto Semi (11.1%) → AD (19%) → EVs (22%) → Lidar (71%)

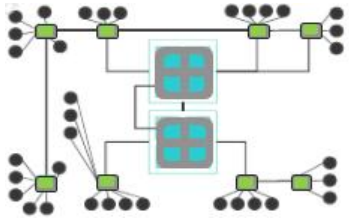
Automotive Challenges

Automotive-specific

Application-specific

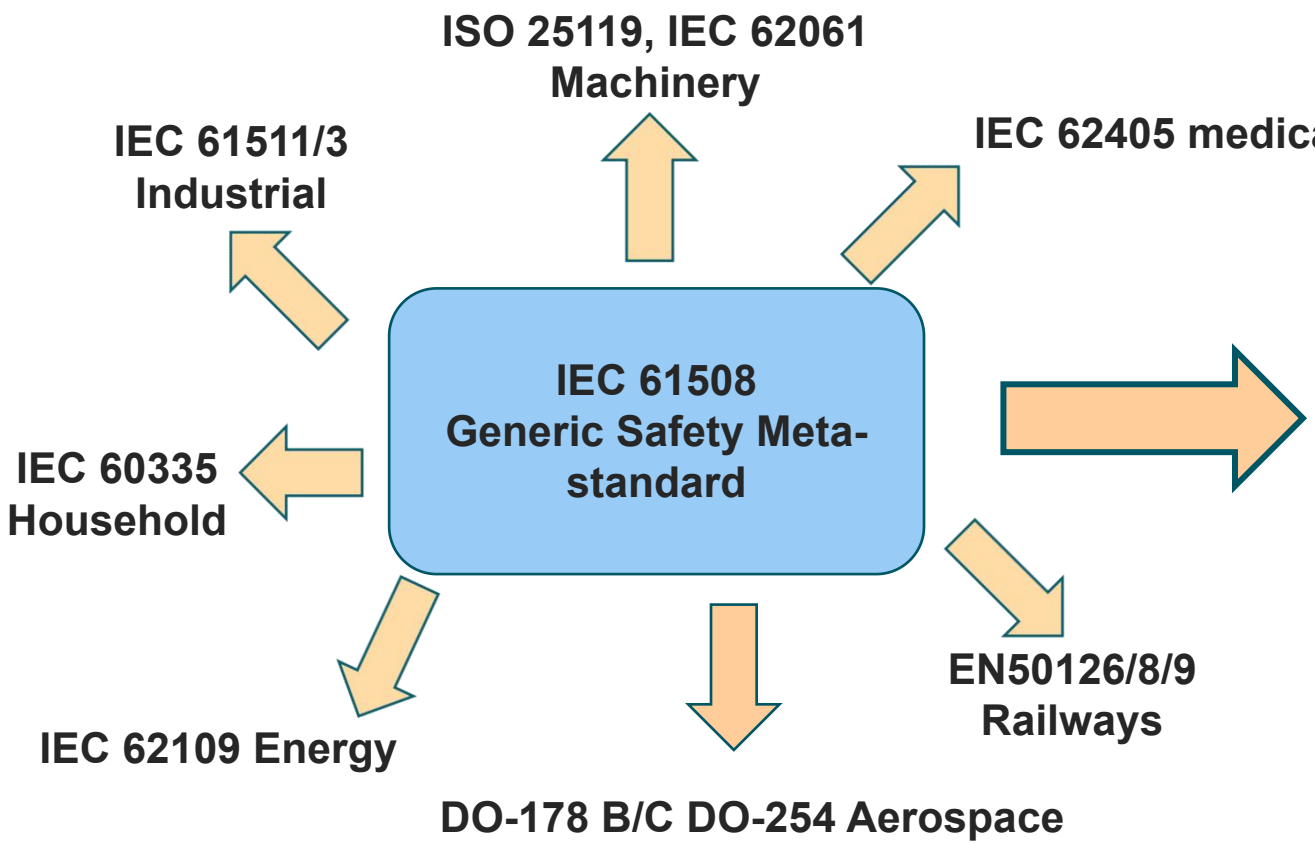


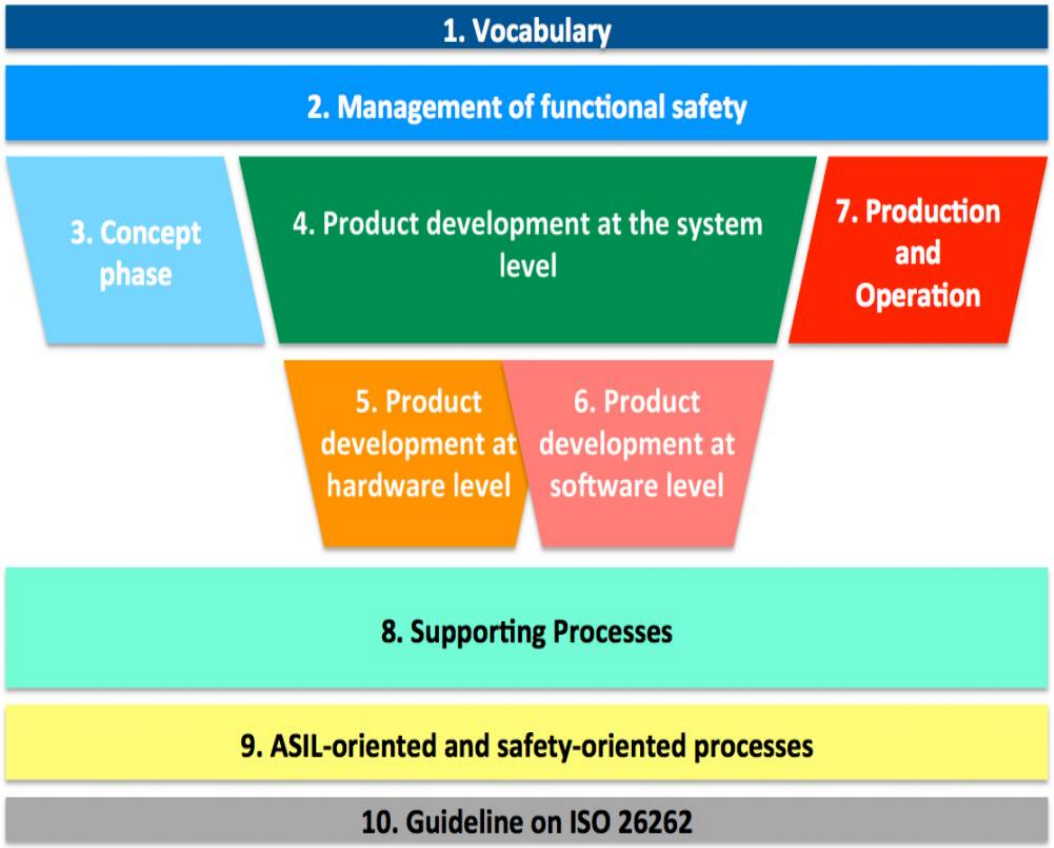




FMEDA-Driven Digital Safety Analysis and Verification

ISO 26262 Functional Safety

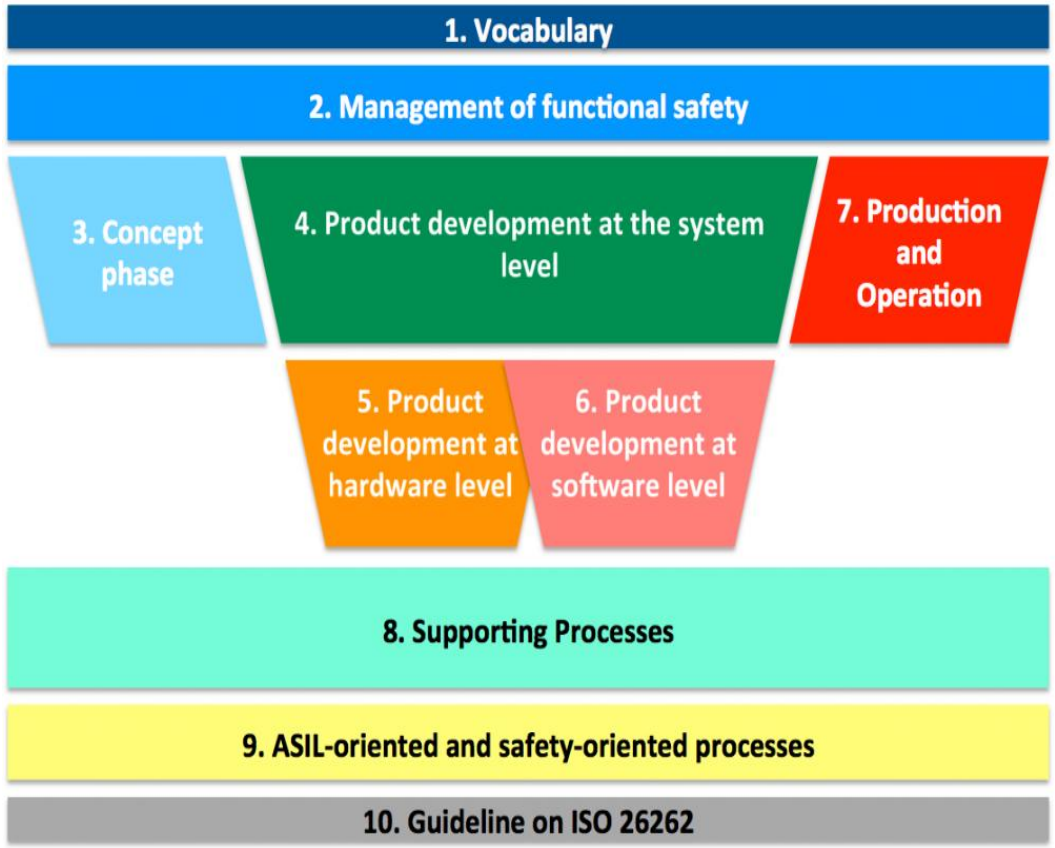




FMEDA-Driven Digital Safety Analysis and Verification

ISO 26262 Functional Safety

ISO 26262 Functional Safety



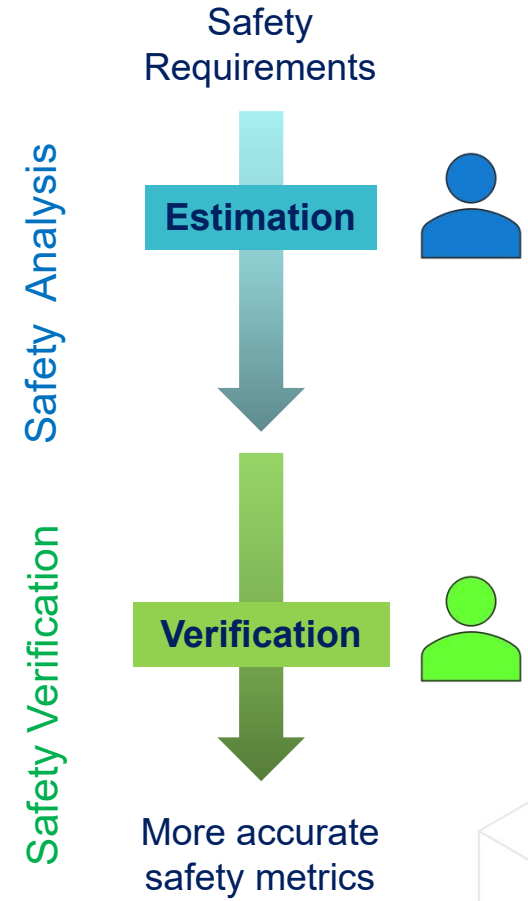
Failure Modes Effects and Diagnostic Analysis

- **Verify** that the **Safety Mechanisms** and their diagnostic coverage reach the required ASIL level by calculating the architectural safety metrics: **SPFM, LFM**
- FMEDA **validates** the **Safety Architecture** (collection of safety mechanisms) and the **safety performance** of the system (SPFM, LFM).

ASIL	ASIL A	ASIL B	ASIL C	ASIL D
SPFM	n.d	≥90%	≥97%	≥99%
LFM	n.d	≥60%	≥80%	≥90%
PMHF (FIT)	< 1000	< 100	< 100	< 10
1FIT = 1E-9				

Closing the Gap Between FMEDA and Safety Verification

	Abstraction	Safety Step	User
Functional Safety Concept	Functional	FMEA	Safety Architect (System level)
Technical Safety Concept SoC	Block Diagram	FMEDA (architectural)	Safety Architect (SoC level)
SoC Design	RTL/netlist	FMEDA (detailed)	Safety Engineer (RTL/gate level)
SoC Safety Verification	Netlist	Safety Verification (Formal/Fault Injection)	Safety Verification Engineer
Safety Metrics	Verification Result	FMEDA backannotation	Safety Verification Engineer



FMEDA Creation and Safety Analysis

Cadence Functional Safety Solution

Unified Safety Format

accellera SYSTEMS INITIATIVE™

Midas™ Safety Platform

Digital Design

- **Innovus™** Implementation
- **Genus™** Synthesis
- **Conformal®** Equivalence Checking

Digital Verification

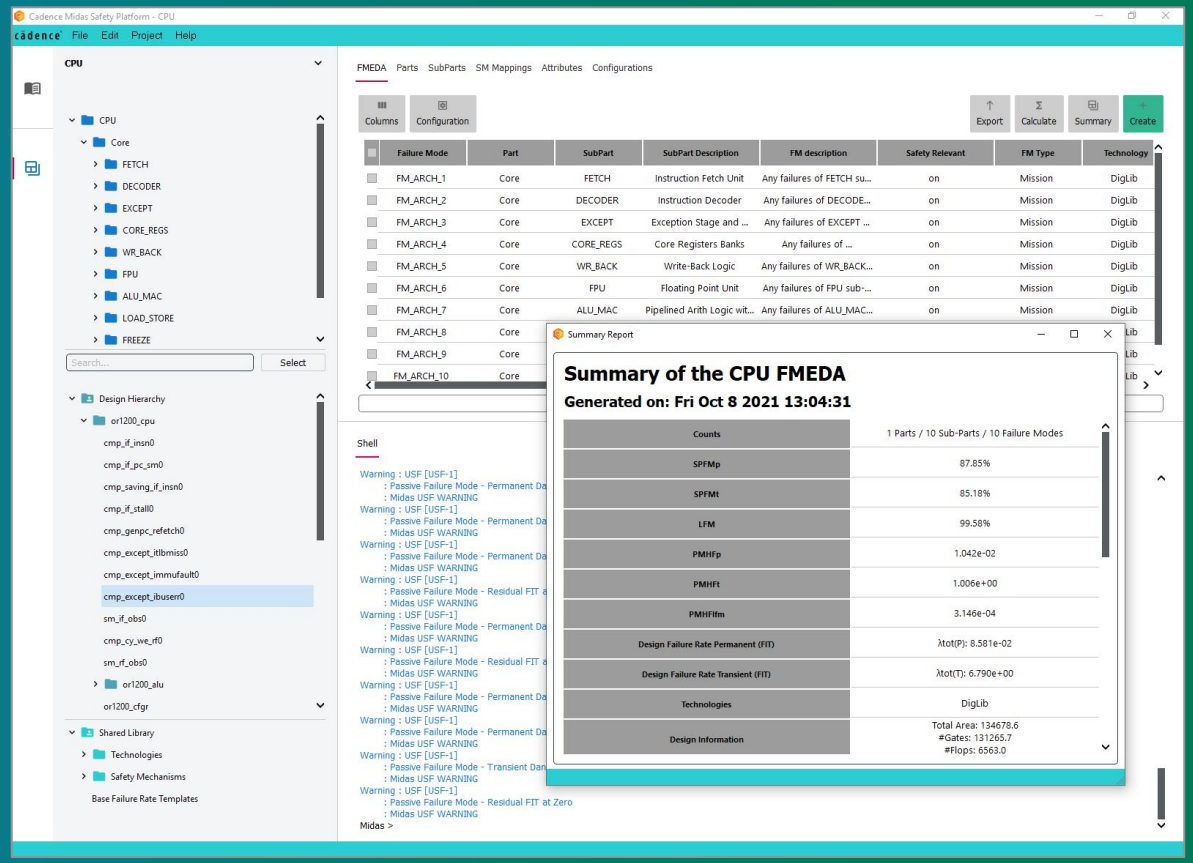
- **Verisium™ Manager** Verification Management
- **Xcelium™** Digital Simulation
- **Jasper™** Formal Verification

Analog/Mixed Signal

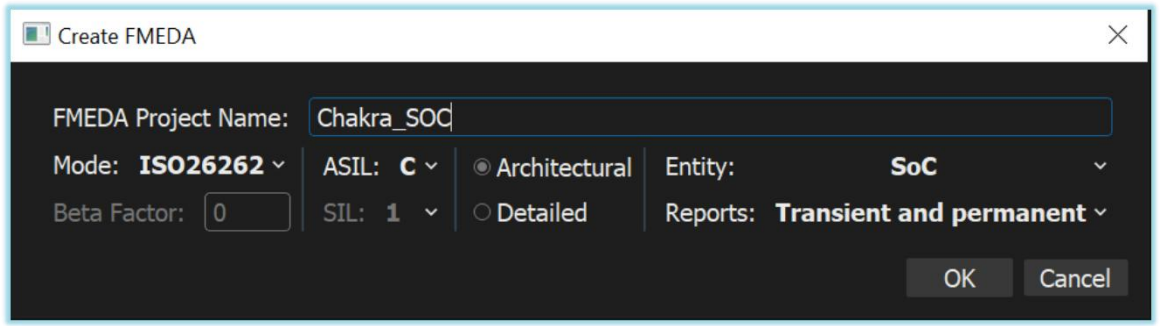
- **Virtuoso®** Design Environment
- **Legato™** Reliability
- **Spectre®** Analog Simulation

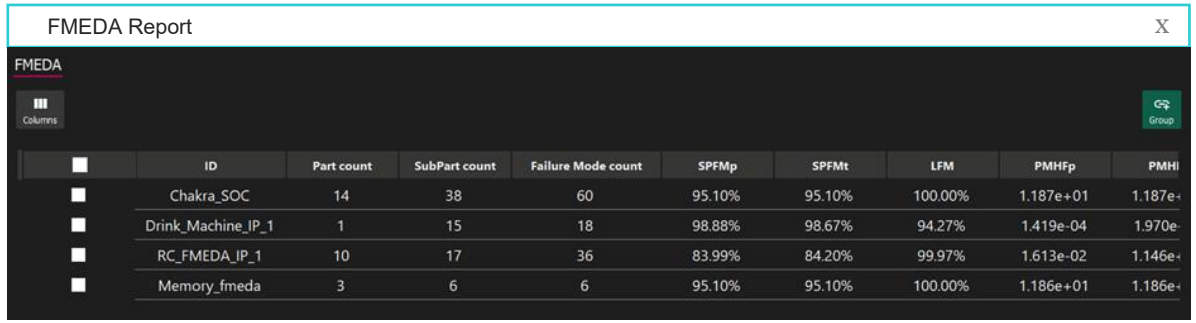
Unified Midas Safety Platform for FMEDA-Driven Functional Safety

- **Midas™ Safety Platform** driving analog and digital flows for FMEDA-based functional safety
- Early phase safety analysis and architecture exploration
- Automated safety mechanism insertion and verification
- Native chip design data for accuracy and detailed safety analysis
- Unified Safety Format (USF) support



Architectural FMEDA Setup





FMEDA Project (IP and SoC)

BFR calculation engine (IEC TR 62380)

Safety Hierarchy (Parts/Subparts)

Failure Mode Creation

Safety Mechanisms Mapping

Safety Analysis

Metrics & Reports | Queries | Rule Checks

Project Setup

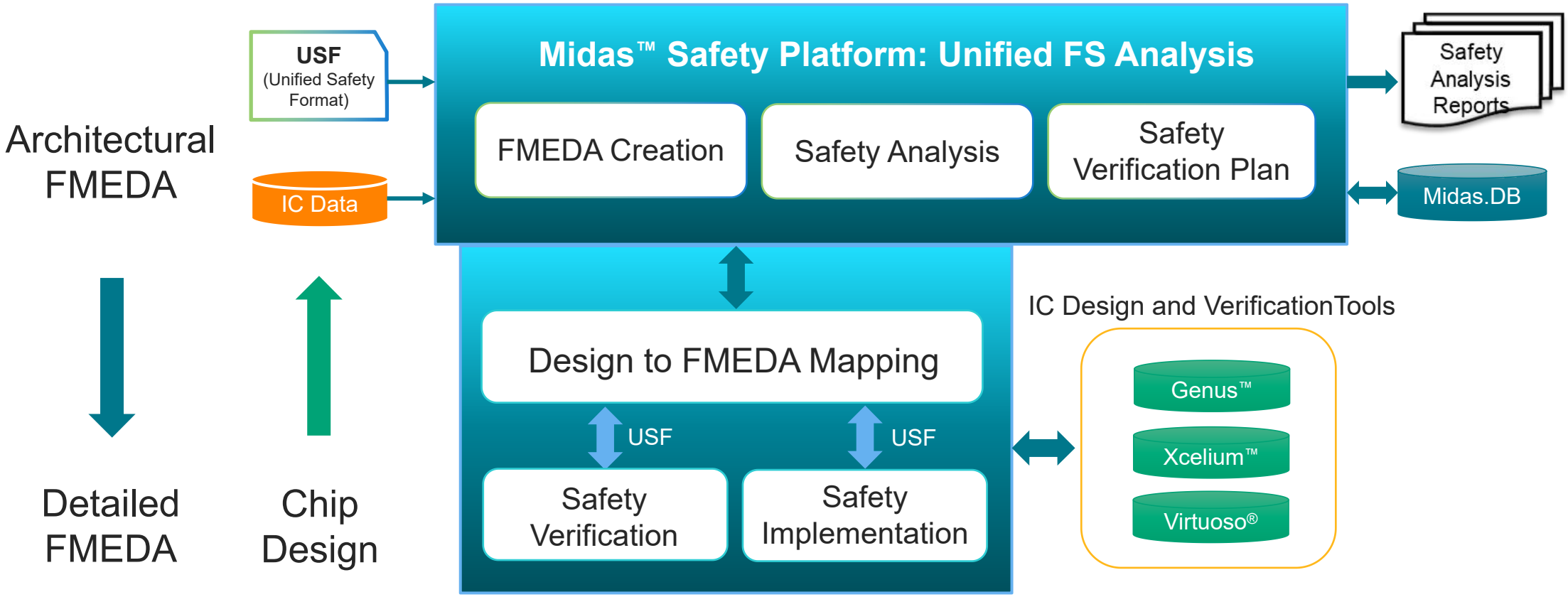
- Device Safety (IP / SoC)

FMEDA Creation

- FMEDA hierarchy only (no IC design)
- Failure Mode Distribution based on user estimation

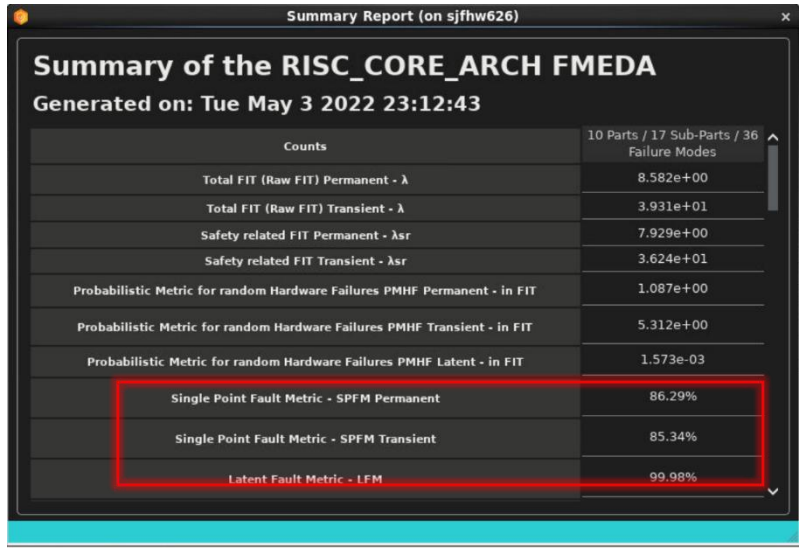
Analysis and Reporting

Safety Design and Analysis at System/SoC/IP Level



Refining FMEDA Leveraging Design and Simulation Data

Architectural FMEDA


Summary Report (on sjfhw626)

Summary of the RISC_CORE_ARCH FMEDA

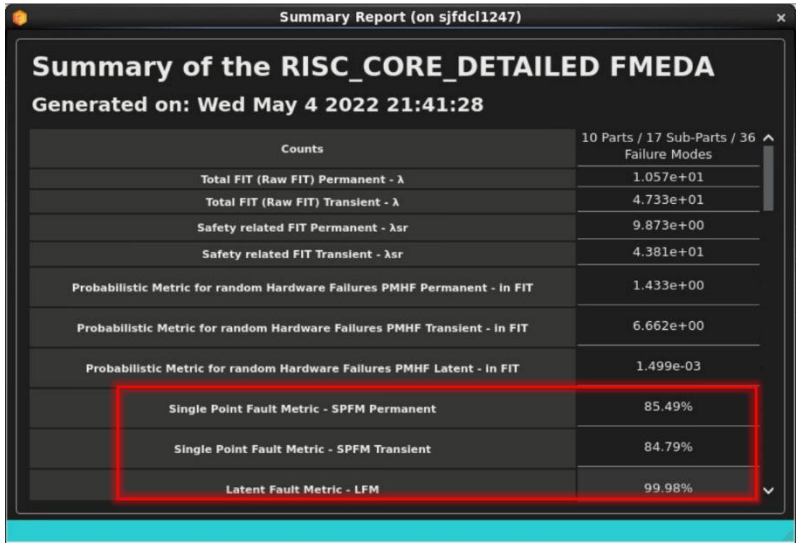
Generated on: Tue May 3 2022 23:12:43

Counts	10 Parts / 17 Sub-Parts / 36 Failure Modes
Total FIT (Raw FIT) Permanent - λ	8.582e+00
Total FIT (Raw FIT) Transient - λ	3.931e+01
Safety related FIT Permanent - λsr	7.929e+00
Safety related FIT Transient - λsr	3.624e+01
Probabilistic Metric for random Hardware Failures PMHF Permanent - in FIT	1.087e+00
Probabilistic Metric for random Hardware Failures PMHF Transient - in FIT	5.312e+00
Probabilistic Metric for random Hardware Failures PMHF Latent - in FIT	1.573e-03
Single Point Fault Metric - SPFM Permanent	86.29%
Single Point Fault Metric - SPFM Transient	85.34%
Latent Fault Metric - LFM	99.98%

- No design data available
- FMEDA hierarchy only
- Failure rates and distribution solely based on early estimations

SPFM = 86.29%

Detailed FMEDA


Summary Report (on sjfdcl1247)

Summary of the RISC_CORE_DETAILED FMEDA

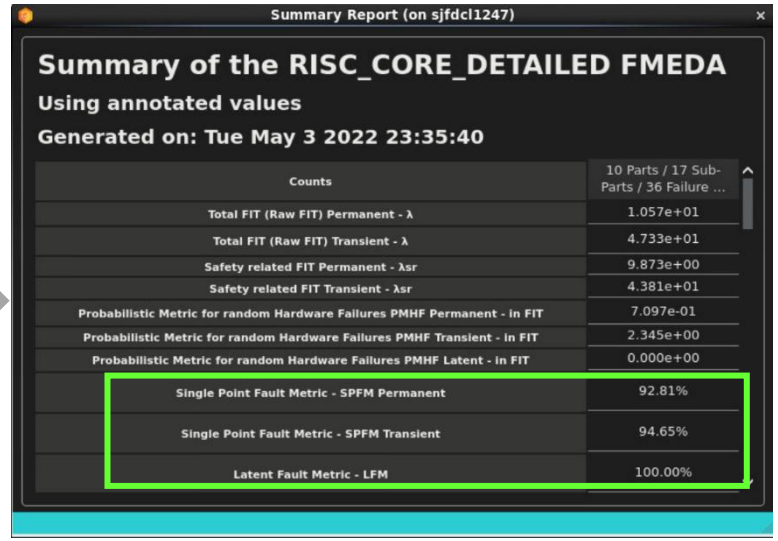
Generated on: Wed May 4 2022 21:41:28

Counts	10 Parts / 17 Sub-Parts / 36 Failure Modes
Total FIT (Raw FIT) Permanent - λ	1.057e+01
Total FIT (Raw FIT) Transient - λ	4.733e+01
Safety related FIT Permanent - λsr	9.873e+00
Safety related FIT Transient - λsr	4.381e+01
Probabilistic Metric for random Hardware Failures PMHF Permanent - in FIT	1.433e+00
Probabilistic Metric for random Hardware Failures PMHF Transient - in FIT	6.662e+00
Probabilistic Metric for random Hardware Failures PMHF Latent - in FIT	1.499e-03
Single Point Fault Metric - SPFM Permanent	85.49%
Single Point Fault Metric - SPFM Transient	84.79%
Latent Fault Metric - LFM	99.98%

- With design data
- Design/FMEDA hierarchy mapping
- Failure rates based on area, gates, and flops
- Safety metrics based on estimated DC, S numbers

SPFM = 85.49%

Detailed FMEDA (annotated)


Summary Report (on sjfdcl1247)

Summary of the RISC_CORE_DETAILED FMEDA

Using annotated values

Generated on: Tue May 3 2022 23:35:40

Counts	10 Parts / 17 Sub-Parts / 36 Failure ...
Total FIT (Raw FIT) Permanent - λ	1.057e+01
Total FIT (Raw FIT) Transient - λ	4.733e+01
Safety related FIT Permanent - λsr	9.873e+00
Safety related FIT Transient - λsr	4.381e+01
Probabilistic Metric for random Hardware Failures PMHF Permanent - in FIT	7.097e-01
Probabilistic Metric for random Hardware Failures PMHF Transient - in FIT	2.345e+00
Probabilistic Metric for random Hardware Failures PMHF Latent - in FIT	0.000e+00
Single Point Fault Metric - SPFM Permanent	92.81%
Single Point Fault Metric - SPFM Transient	94.65%
Latent Fault Metric - LFM	100.00%

- With design data
- Design/FMEDA hierarchy mapping
- Failure rates based on area, gates, and flops
- Safety metrics based on simulation-based DC, S numbers

SPFM = 92.81%

Detailed FMEDA Using USF

FMEDA Project (IP and SoC)

BFR calculation engine (IEC TR 62380)

Technologies (Digital, Analog)

Safety Hierarchy (Parts/Subparts)

Failure Mode Creation

Mapping Safety Mechanisms

Mapping Design Hierarchy to FMEDA Hierarchy

Queries

Metrics and Reports

```
set_fmeda myFMEDA -ASIL B -t -p -detailed
```

```
create_technology DigLib -type Digital -fitperm 1.07e-6 -fittrans_gate
1.64e-6 -fitbit 1.64e-6 -refarea 1.026
```

```
create_part    "OpenRISC Core" -fmeda myFMEDA -instances
{hinst:or1200_cpu/or1200_if hinst:or1200_cpu/or1200_genpc}
create_subpart FETCH -desc "Instruction Fetch Unit" -part "OpenRISC Core" -
fmeda myFMEDA -instances {hinst:or1200_cpu/or1200_if}
```

```
create_failure_mode FM_ARCH_1 -desc "Any failures of FETCH sub-block‟ -type
Mission -technology DigLib -subpart FETCH -safe_perm 1 -safe_trans 0 -fmeda
myFMEDA -instances {hinst:or1200_cpu/or1200_if}
```

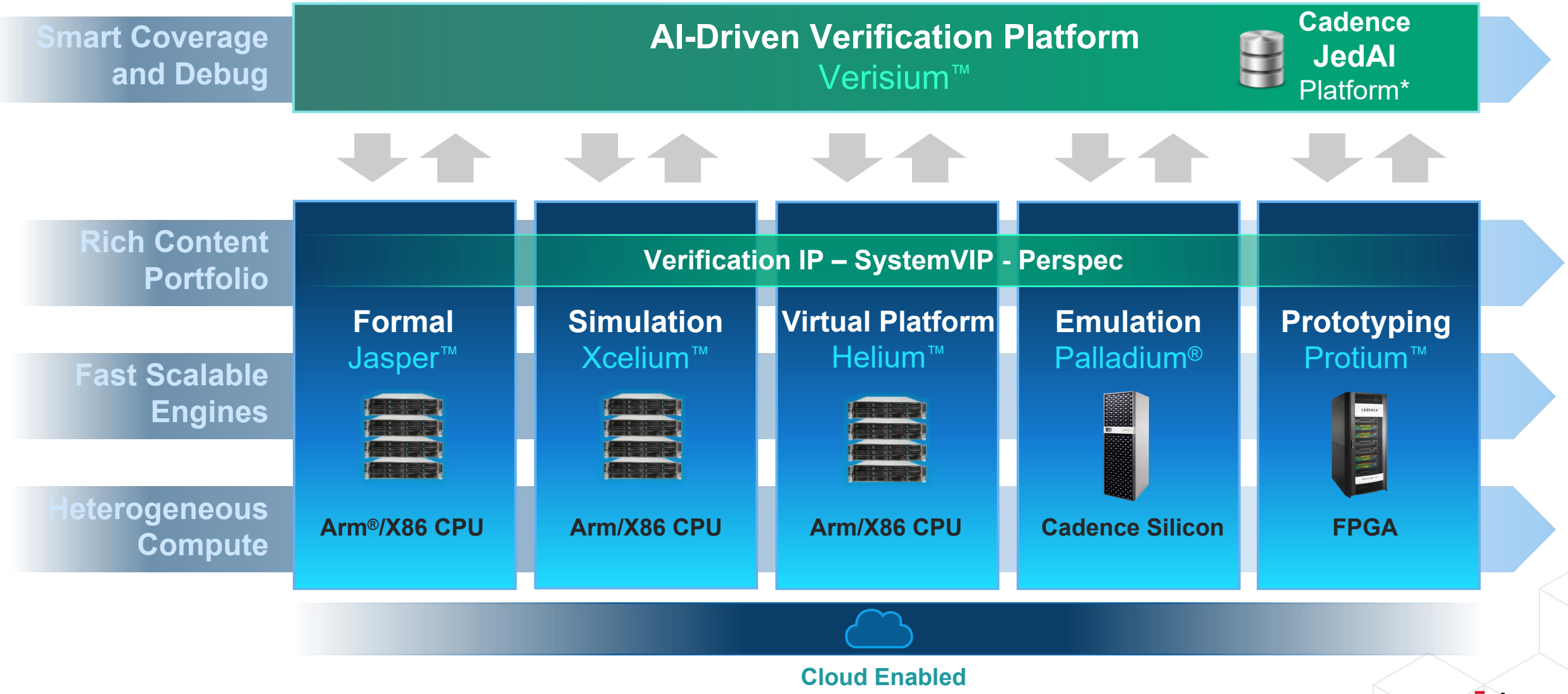
```
create_safety_mechanism SM-IF -desc "Instruction Fetch redundancy" -type
Custom -class HW
apply_safety_mechanism  SM-IF -to FM_ARCH_1 -fmeda myFMEDA -dcperm 95 -
dctrans 0 -dclat 100
```

```
report_safety -fmeda myFMEDA permanent csv   OpenRISC_Permanent.csv
report_safety -fmeda myFMEDA transient csv   OpenRISC_Transient.csv
report_safety -fmeda myFMEDA report    html  OpenRISC_Report.html
```

save_usf → **load_usf**

Safety Verification

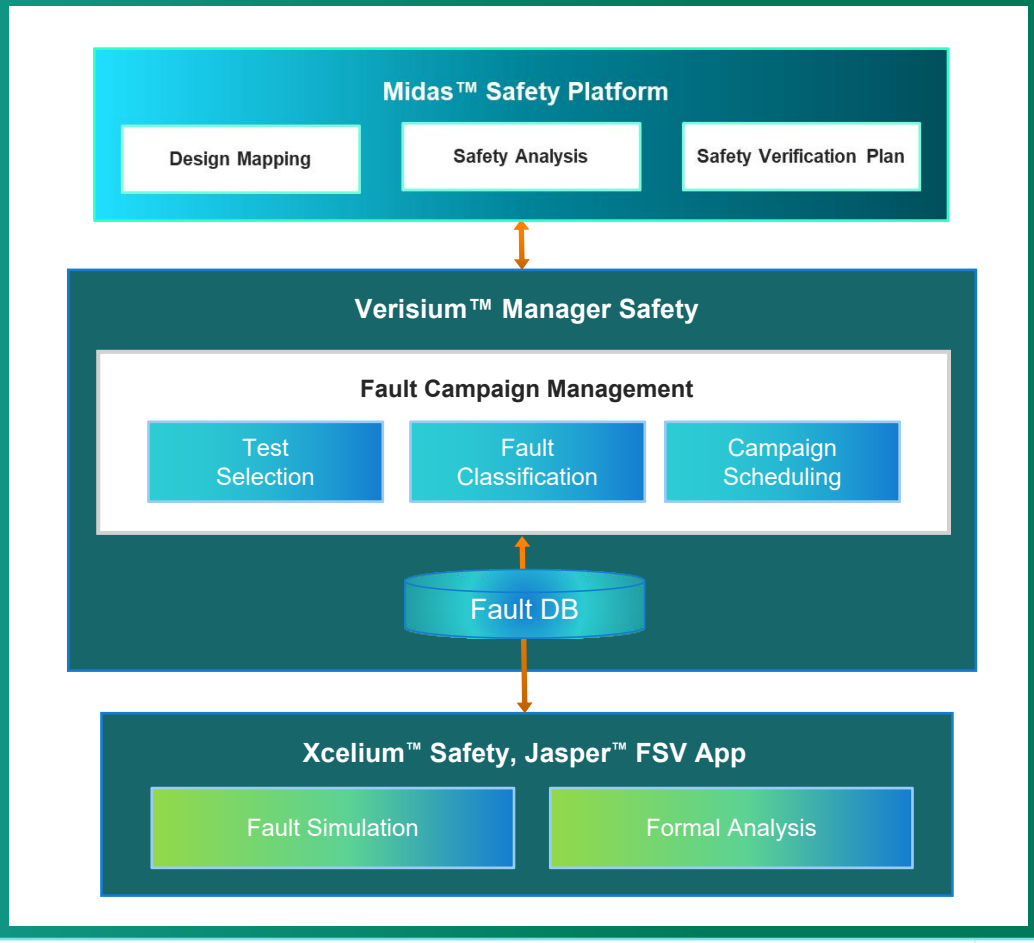
Optimizing Throughput Across the Full Verification Flow



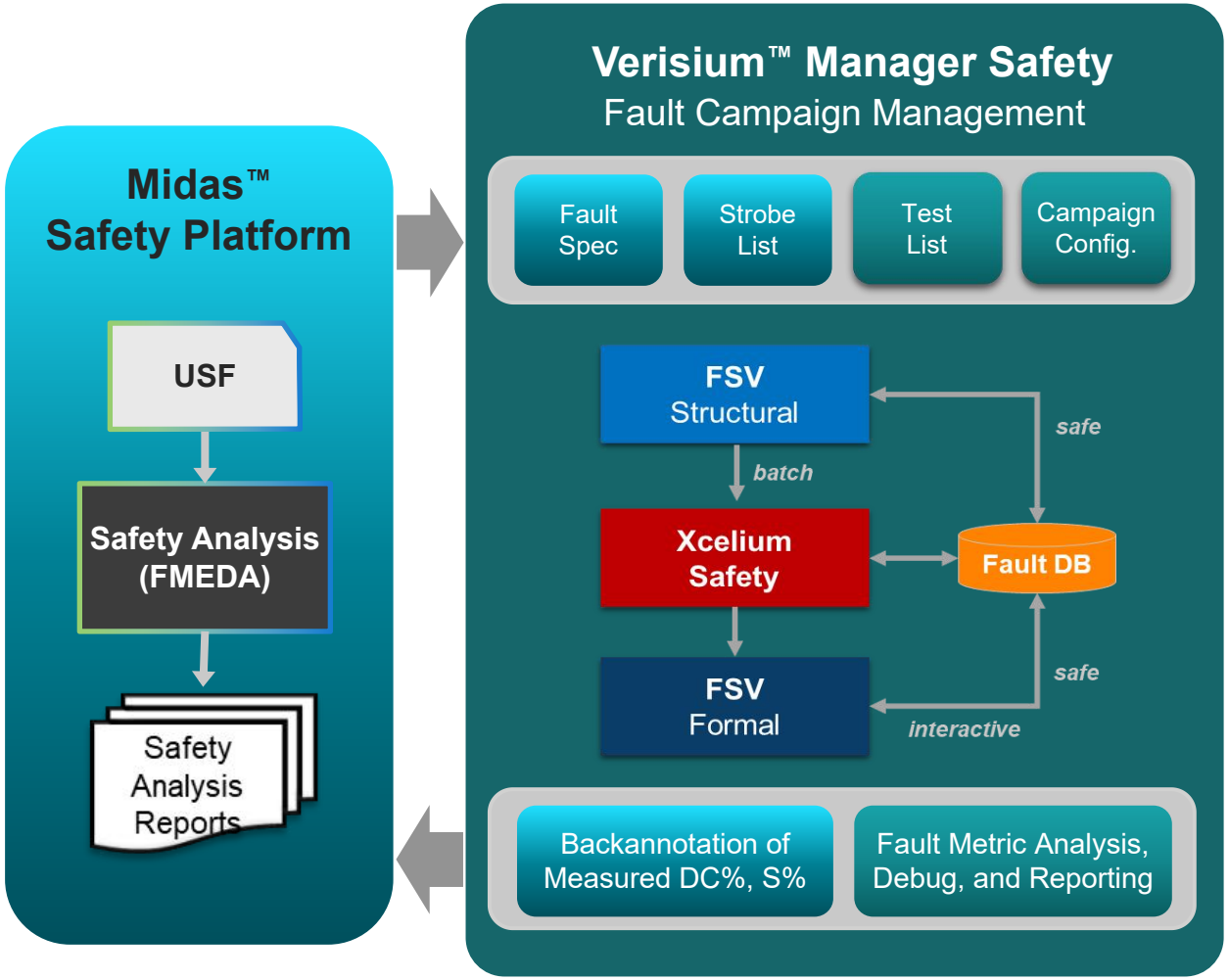
* Cadence® Joint Enterprise Data and AI (JedAI) Platform

Digital Safety Verification
Fault analysis and simulation

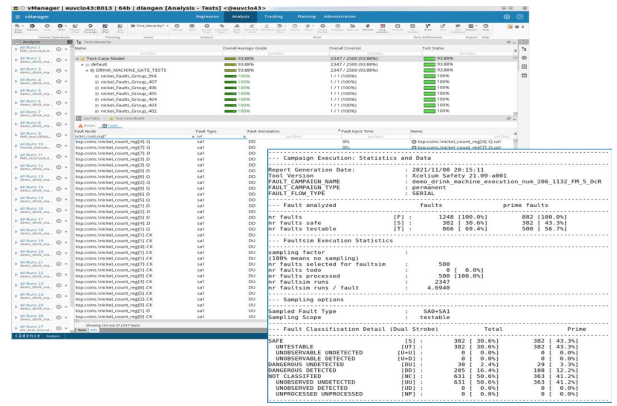
- ✓ Fault Campaign Management – Verisium™ Manager Safety
  - Unified campaign management across all engines
  - Backannotation of DC results into Midas
  - Requirements traceability
  - Reporting for safety documentation
- ✓ Fault Analysis – Jasper™ FSV App
  - Applies formal techniques to fault analysis
  - Significantly reduces the simulation fault list
  - Increases safety verification performance
- ✓ Fault Simulation – Xcelium™ Safety
  - Native serial and concurrent fault verification
  - Same simulator for functional verification (GOOD machine) and fault simulation (BAD machine)



Fault Campaign Management – Automation and Optimization

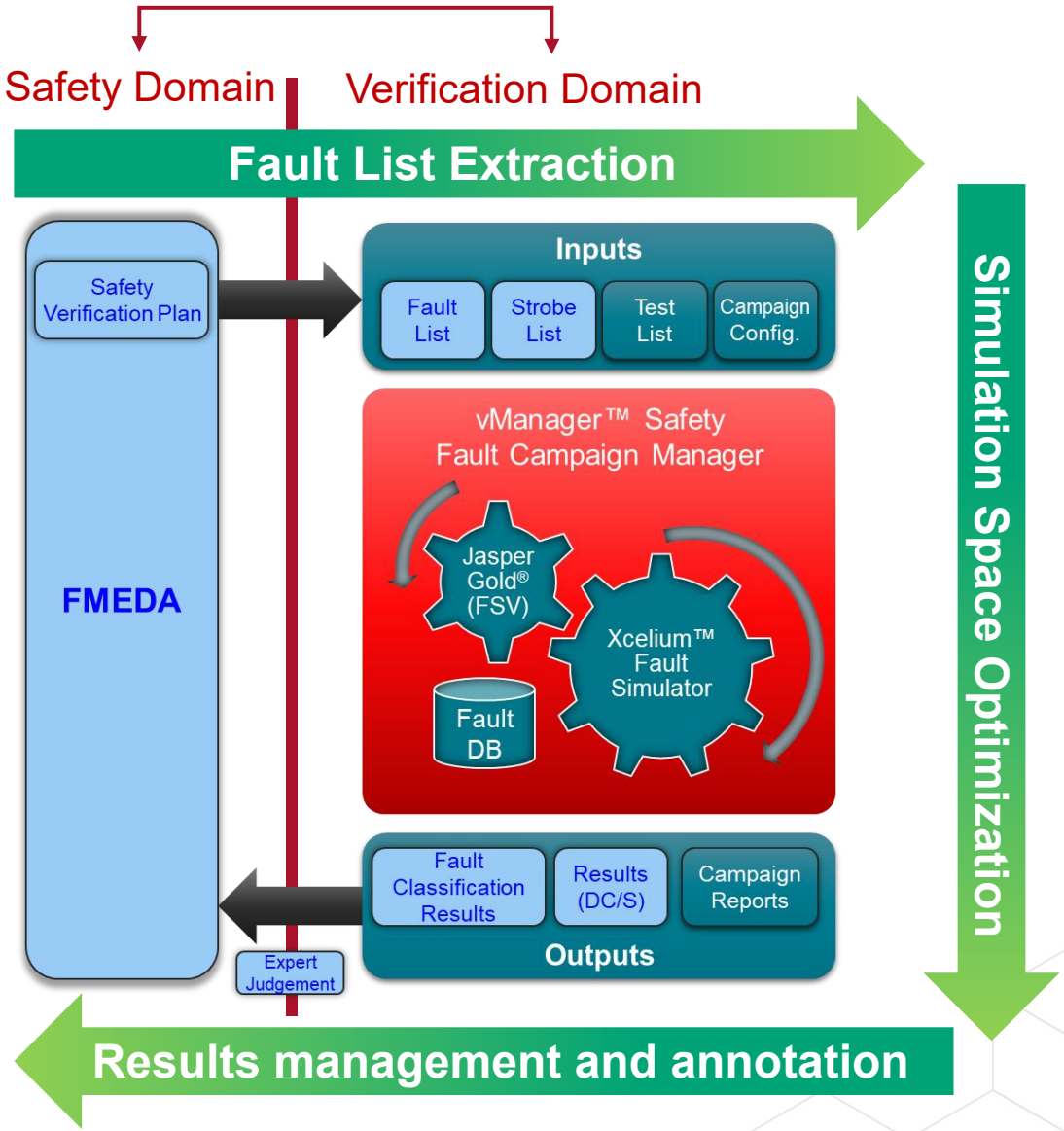


- Test selection and ranking
  - Coverage-based test selection
  - Customizable ranking criteria
  - Test Dropping
- Fault list reduction
  - Fault collapsing
  - Testability analysis
  - Fault sampling
- Fault campaigns execution
  - Measured Diagnostic Coverage and Safeness
  - Back-annotation of results to FMEDA
  - Generate reports and analyze fault metric
  - FMEDA, fault classification, campaign summary

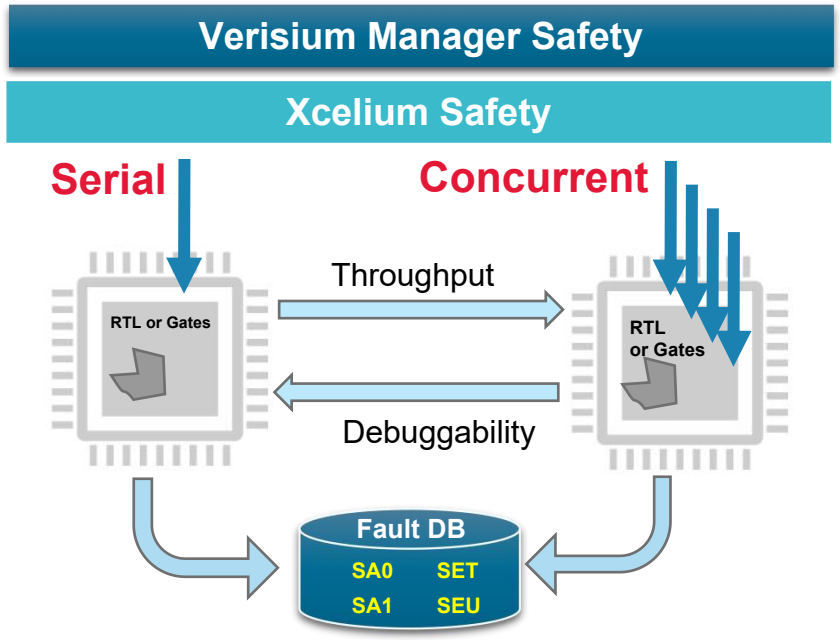


Xcelium Safety App

- Integrated Xcelium™ Safety flow with Midas™, Verisium™ Manager, and Jasper™ FSV
- Native fault simulation
  - Integration of functional and safety engines
  - Xcelium: a single simulator for functional and fault simulation
  - Superior traceability and debug visibility
- Covers all digital safety verification use cases and provides comparable quality results
- Supports reactive TBs and various abstractions

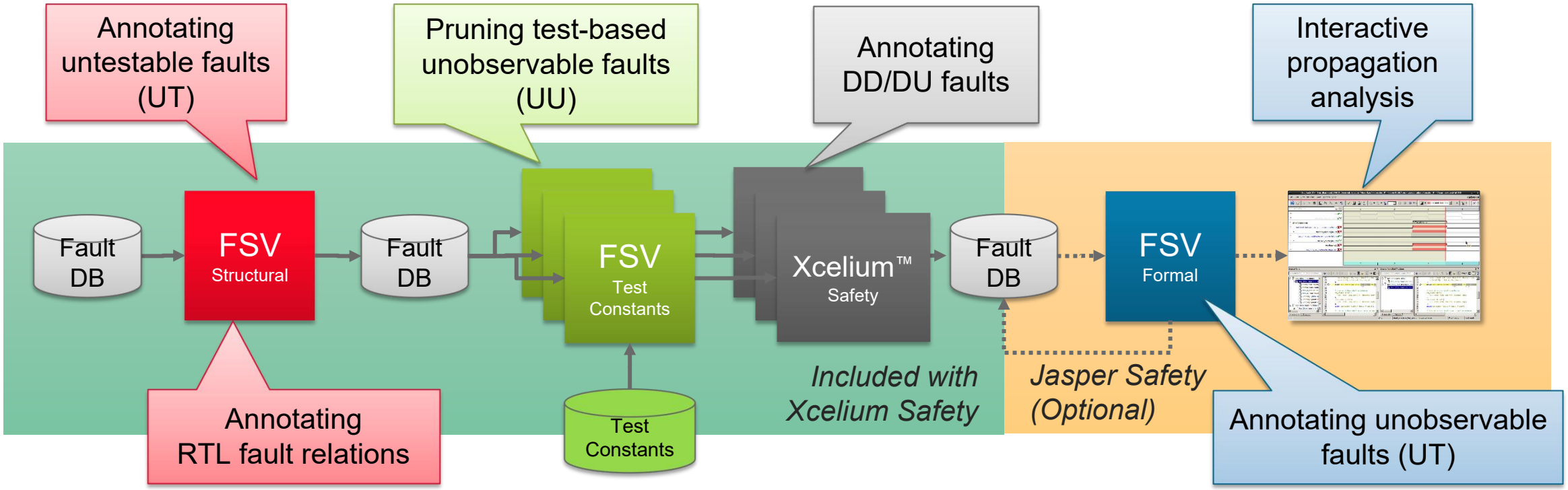


Xcelium Safety – Fault Simulation



- Native fault simulation
  - Integration of functional and safety verification engines
- Support reactive TBs, various abstractions
  - Integrated serial and concurrent engines
  - Serial support for VHDL and Verilog, RTL, and gate-level
  - Concurrent support for untimed gate-level and RTL
- Congruency flow between two modes
  - Serial mode: Strength in debuggability, generally used in flow setup and faults debug
  - Concurrent mode: Strength in performance throughput, generally used for whole fault campaign mass runs
  - Two modes use identical flow and can easily switch back and forth

Jasper FSV Integration with Xcelium Safety Simulator



- FSV Structural annotates untestable faults in database → safe faults will be ignored
- FSV annotates fault relations → equivalent faults will be skipped
- FSV TC annotates faults as unobservable by a particular test → pruned faults will be dropped
- Xcelium Safety simulates and annotates all remaining DD/DU faults in the database
- FSV Formal provides interactive propagation analysis for unobservable faults by test

Simulation Verification IP (VIP) for Automotive

VIP for Ethernet TSN (MAC)

- Mature, highly capable compliance verification solution
- TSN protocol stack incl. bus functional model (BFM), integrated protocol checkers, and coverage
- Easy integration in test benches at IP and system levels

VIP for Ethernet Base-T1 (PHY)

- Supports all Base-T1 speeds: 10Mbps, 100Mbps, 1Gps

VIP for MIPI A-PHY

- MIPI A-PHY support for sensor applications (CSI2, I2C)
- Compliance to MIPI A-PHY v1.0 and v1.1 specifications

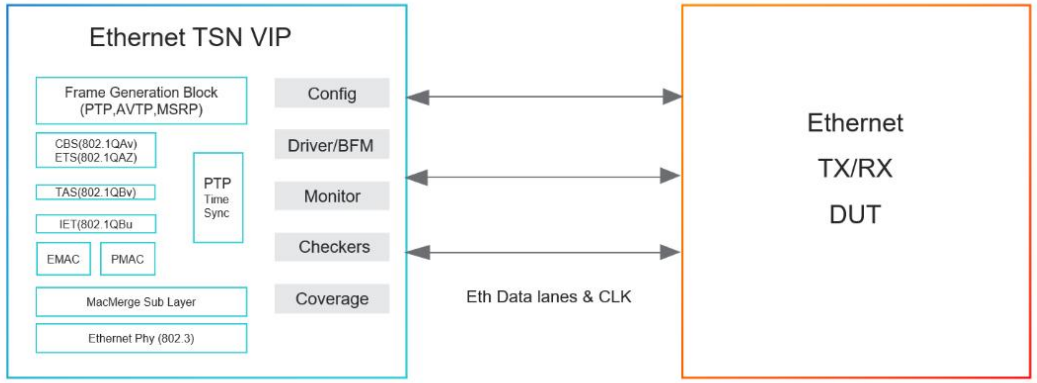
VIP for PCIe 3.0 / 4.0 / 5.0

- Best-in-class PCI Express® Verification IP for IP, SoC

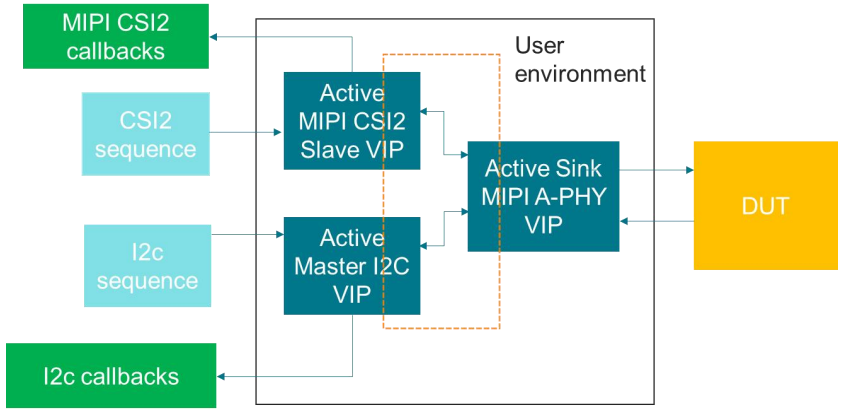
VIP for all CAN standards

- Supports CAN, CAN-FD, and CAN-XL specifications

Automotive Ethernet



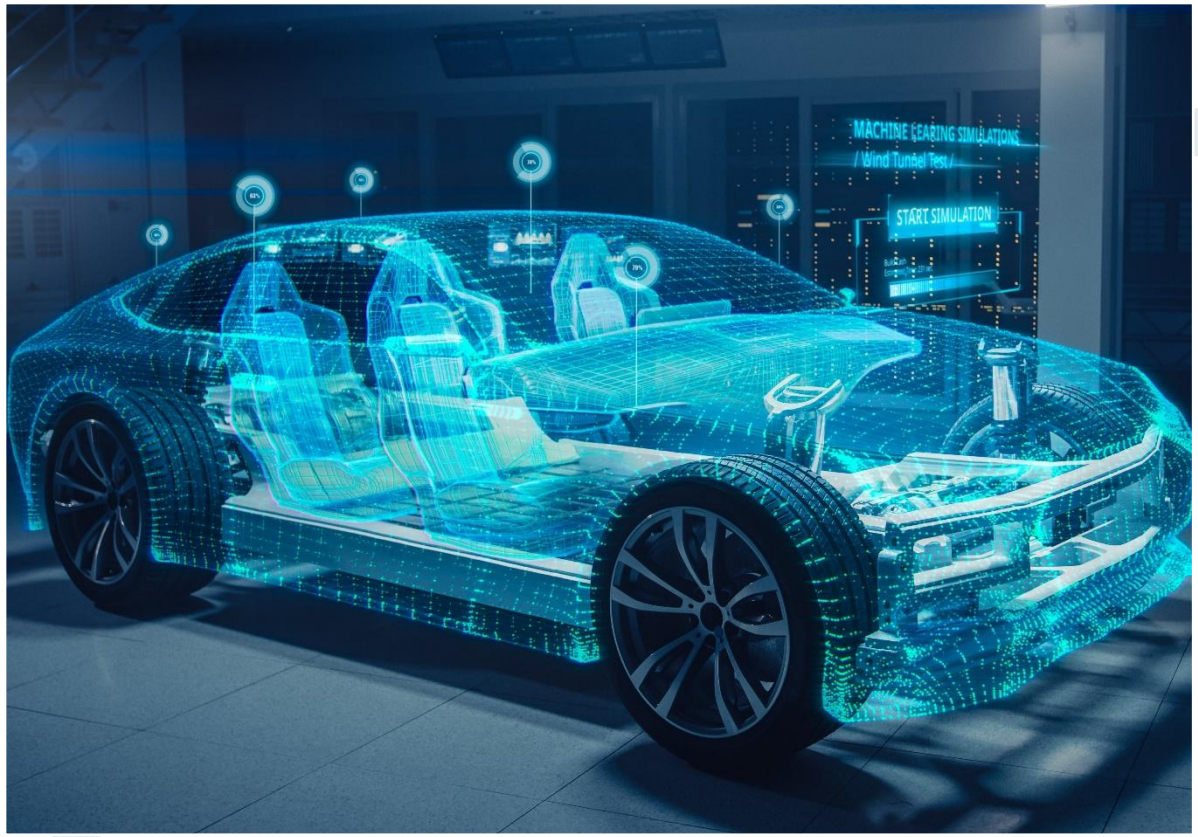
MIPI A-PHY



Sensor Simulation Verification: A-PHY with CSI2 and I2C VIPs

Helium Virtual Platforms

Virtual digital electronics designed to test full software binaries



Controllability, Observability, Repeatability

Digital Twin elements provided by the methodology:

Instruction Accurate

- Target software runs without changes

Full programmers view

- Memory, registers, and interrupts

Loosely Timed

- Fast enough for OS Boot

Available Early

- 6-12 months before silicon

All in Software

- Run on standard x86 workstations

Hybrid Platforms: Helium with Palladium or Protium

Combining pre-silicon verification with v-model verification and validation

Digital Twin elements provided by the methodology:

Mixed Accuracy

- Circuits for design under test
- Abstract for context

Full Programmers' View

- Memory, registers, interrupts, and pins

Mixed Abstraction

- Fast enough for OS Boot
- Detailed enough verification

Available Early

- As soon as the design is ready

Integrated with Hardware

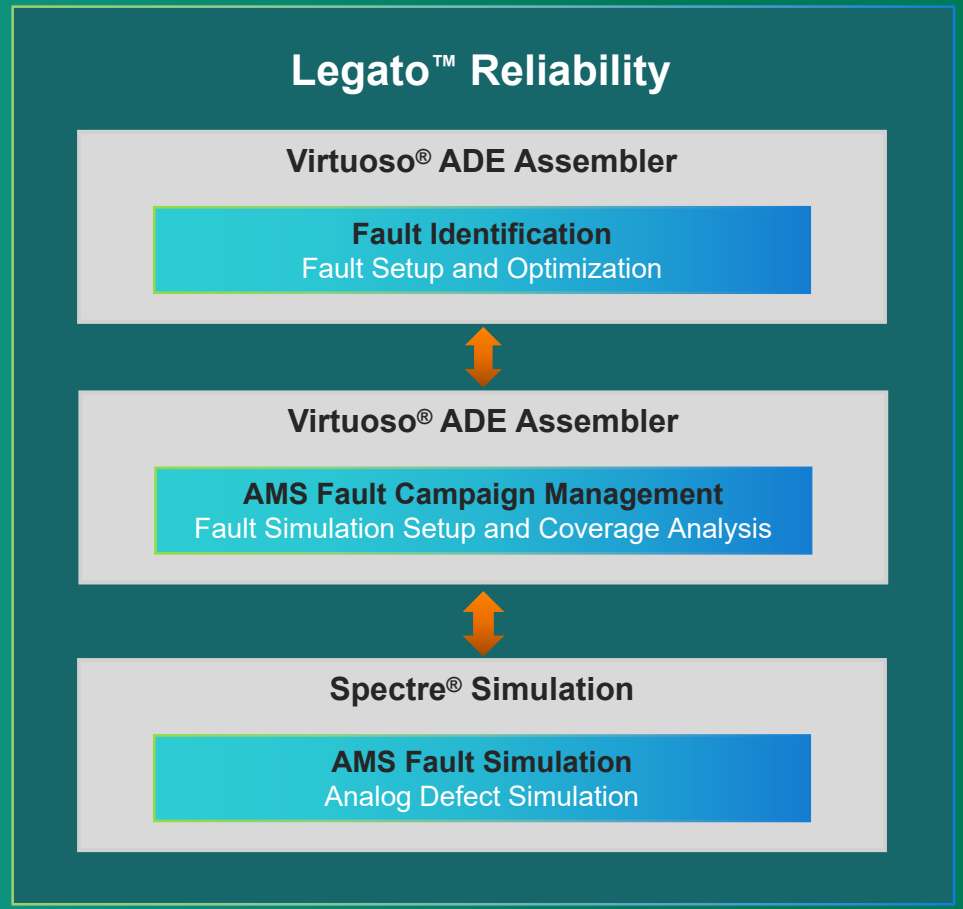
- Palladium® and Protium™ platforms for capability and performance

Balance of Speed and Accuracy

Analog / Mixed-Signal Safety Verification

Automated fault identification and simulation

- Developed in alignment with **IEEE P2427**
  - Standard for Analog Defect Modeling and Coverage
- Fault assistant for rule-based fault identification
  - Fault models: DC short/open, resistive bridge, AC coupling
- Integrates Spectre Simulation Platform and Legato Reliability Solution
  - New Spectre fault analysis simulation modes
- Automates launching of fault simulations for different failure modes
- Back-annotation of safety coverage into the Midas™ Safety Platform



Summary

ISO 26262 Tool Qualification

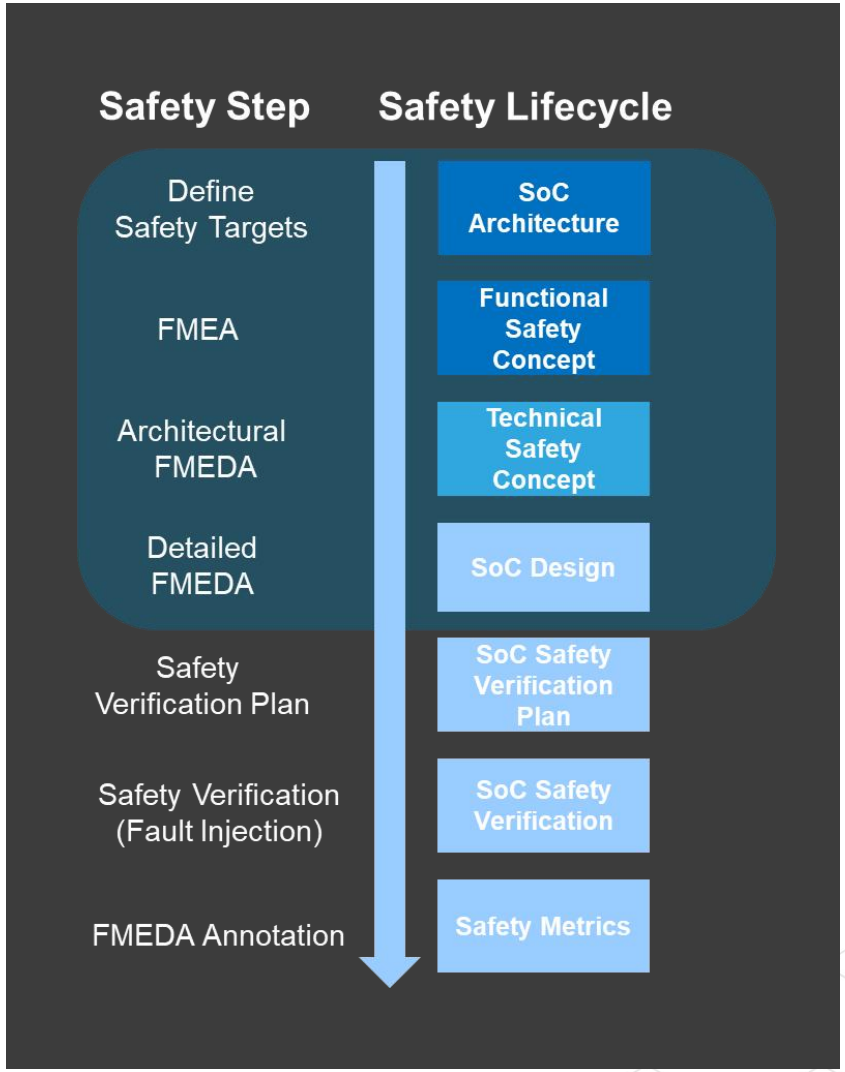
- First EDA supplier to achieve “Fit for Purpose - Tool Confidence Level 1 (TCL1)” for the full solution
- Status for medium/high-level confidence (TCL2/3):

Product	Release	Date
Midas	22.03	Available
vManager Safety	20.09, 21.03, 21.09, 22.03	Available
Xcelium Safety	22.03	Available
Jasper Safety	22.03	Applied for

Functional Safety Services

Achieve ISO26262 compliance

- Support in Safety Architecture definition
  - Architectural/Detailed FMEDA using Midas™ Safety Platform
  - Creation of a Technical Safety Concept
  - Safety Analysis and reporting
- Functional Safety Verification
  - Safety Verification flow definition
  - Generation of fault injection campaigns and execution using
    - Midas Safety Platform
    - Verisium™ Manager Safety
    - Jasper™ FSV
    - Xcelium™ Safety Simulator
  - Test bench re-use and qualification
- Support in Safety Manual creation (ISO 26262) based on Cadence® safety manuals



Advantages of the Cadence Functional Safety Solution

- Comprehensive architectural FMEDA
- Links to best-in-class digital, analog, and library tools for detailed FMEDA
- Accellera USF standard support for interoperability

- Links to digital synthesis and implementation tools with USF support
- Best-in-class RTL/gate/netlist equivalence checking

Digital Design	Digital Verification	Analog/Mixed Signal
Innovus™ Implementation	Verisium™ Manager Verification Management	Virtuoso® Design Environment
Genus™ Synthesis	Xcelium™ Digital Simulation	Legato™ Reliability
Conformal® Equivalence Checking	Jasper™ Formal Verification	Spectre® Analog Simulation

- Links to analog/mixed signal design tools with USF support
- Mixed signal fault simulation in same environment as functional verification

- Best-in-class verification management, coverage and traceability solution
- Same simulator for functional verification and fault simulation gives superior debug experience
- Best-in-class formal verification for fault list reduction and formally-proven fault classification

Functional Safety Verification customers:

Texas Instruments, Infineon, Renesas, Analog Devices, ST