2026 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION UNITED STATES

SANTA CLARA, CA, USA
MARCH 2 - 5, 2026

Closing the safety Verification Loop, FMEDA-Driven Fault Simulation and Advanced Debug for Efficient Fault Classification

Sagar Hema Vidya
Sr Manager
Silicon Design Engineering
AMD India

Vedant Garg
Sr Solutions Architect
Safety and Reliability
Synopsys Austin

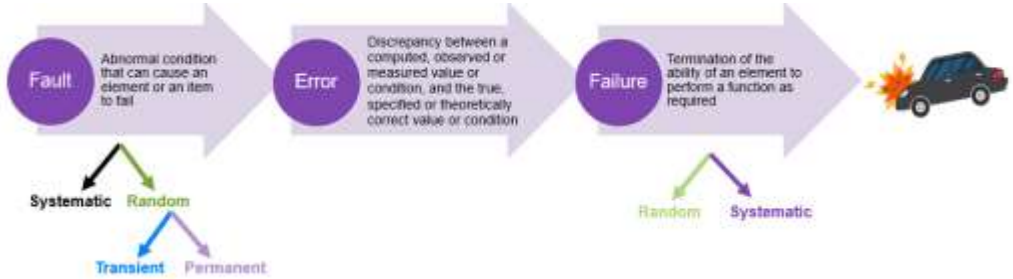
Agenda

- Introduction and Problem Statement
- Proposed Methodology
  - Elementary Subpart Extraction
  - FMEDA and Safety verification plan
- Experimented Methodology
  - Fault Sampling
  - Faults analysis
  - Fault Simulation Iterations
  - Residual Fault analysis
- Results
- Best practices – Meeting Safety Goals
- Conclusion

Introduction and Problem Statement

FMEDA identifies which elements require safety mechanisms to avoid failures.

Fault simulation provides experimental evidence by injecting faults and checking whether the safety mechanism responds correctly.



Non-targeted fault campaigns

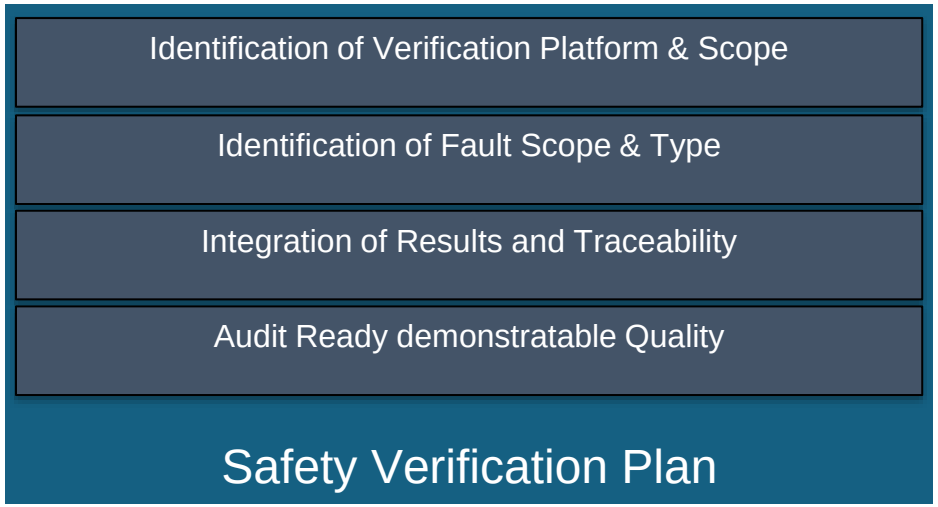
- Which Failure mode and Safety Goal does these Instances represent?
- How to generate In Scope or Safety Relevant Faults Space

Weak traceability

- Simulated fault IDs do not directly map to FMEDA entries, complicating coverage justifications and audits.
- Gaps in Verification of Safety relevant Area

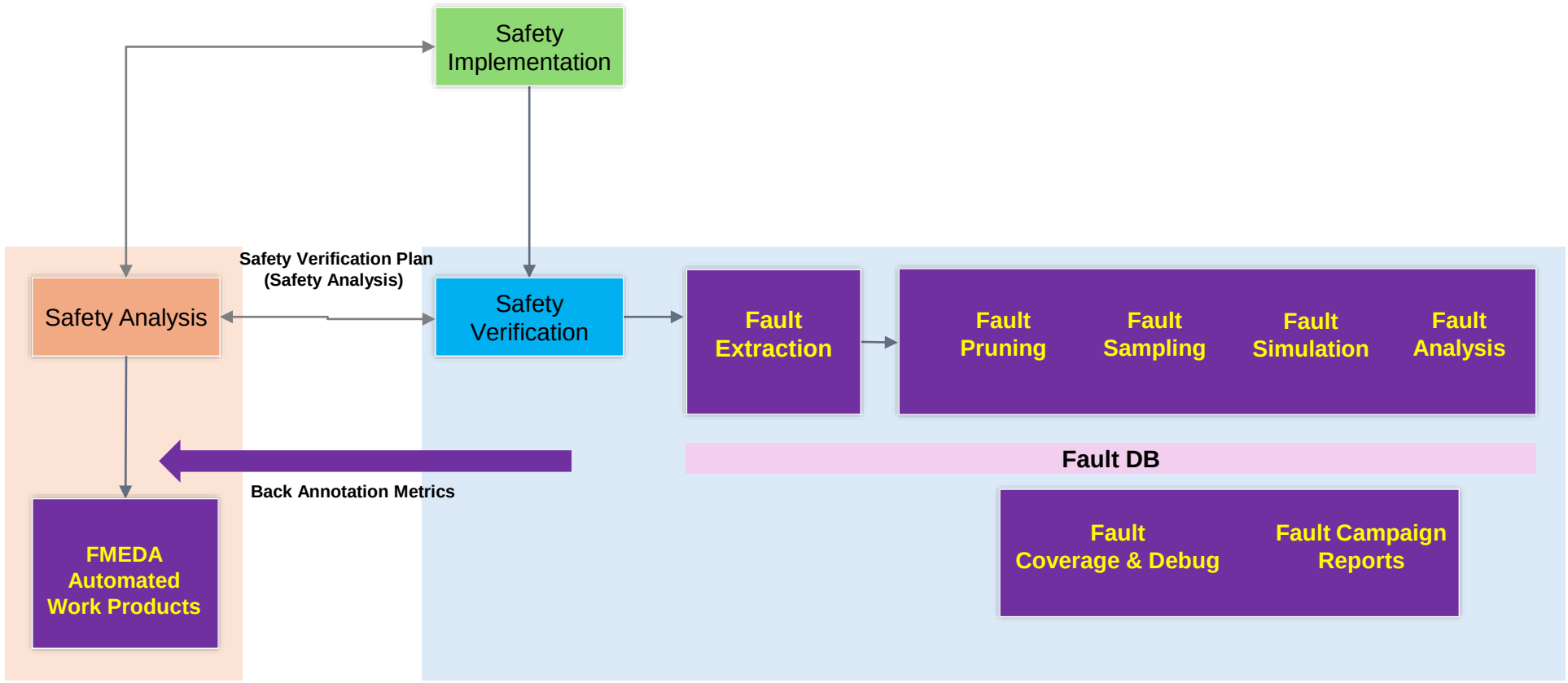
Manual classification effort

- Safety teams must manually accommodate FMEDA spreadsheets with simulation reports.
- Scope and understanding of the SEooC IP



Proposed Methodology

	VC FSM, Primetime
	VCS, VC Z01X



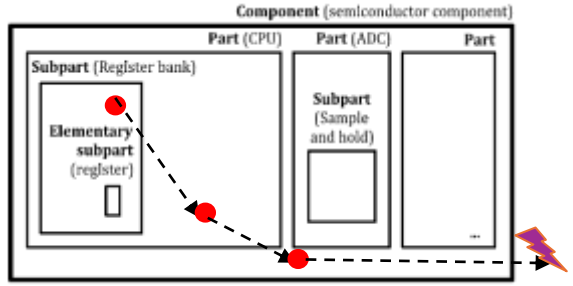
Elementary Subpart Extraction

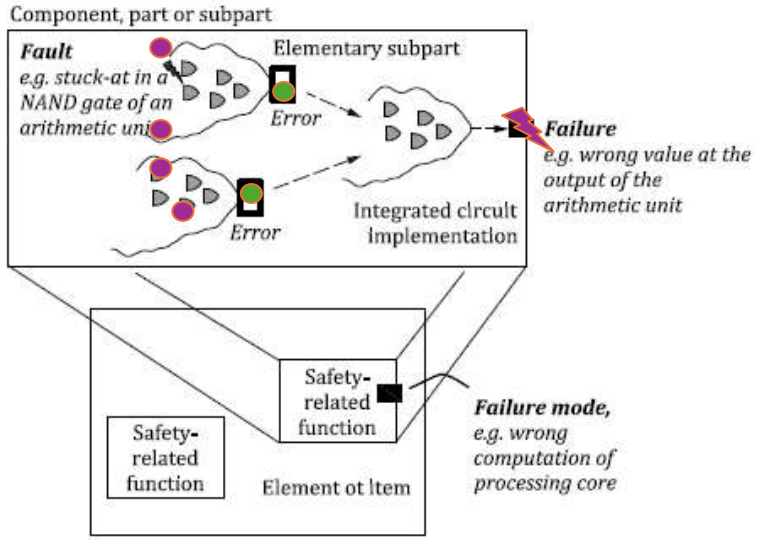
- Faults originate at the “Elementary Sub Part” level and may propagate further to result in system failures.
- Random HW faults can be of both Permanent or transient type and can occur at any time.
- Base Failure Rate is allocated based on the technology data for different HW logic types, such as digital, memory, analog etc.
- FIT (Failure In Time) is calculated by combining the Failure Mode, Elementary Sub Part, and Base Failure Rate.

$$\lambda\_ESP = \lambda\_seq + \lambda\_col$$

λ_seq represents the intrinsic failure rate of the sequential element. λ_col represents the cumulative failure contribution from combinational COL.

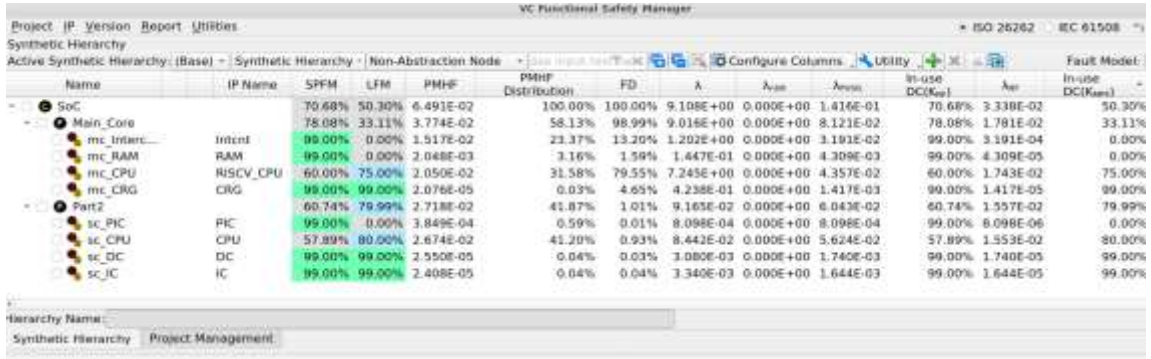
Guidance from ISO 26262 Part 11 show the use of Elementary Sub Parts to define Failure Modes.





FMEDA and Generation of Safety Verification Plan

- **Data exchange:** FMEDA driven fault campaigns and back-annotation of diagnostic coverage
- **Safety-focused filtering:** Faults that do not contribute to SPFM, LFM, or latent fault metrics are automatically excluded, significantly reducing simulation scope.
- **Prioritization based** on ASIL and coverage relevance: High-ASIL blocks or mechanisms with weak diagnostic coverage are simulated first.
- **Traceable mapping:** Every fault in the simulation plan is linked to its corresponding FMEDA entry, enabling automated reporting for audits or safety cases.
- Read by fault campaign compiler to create faults in fault database

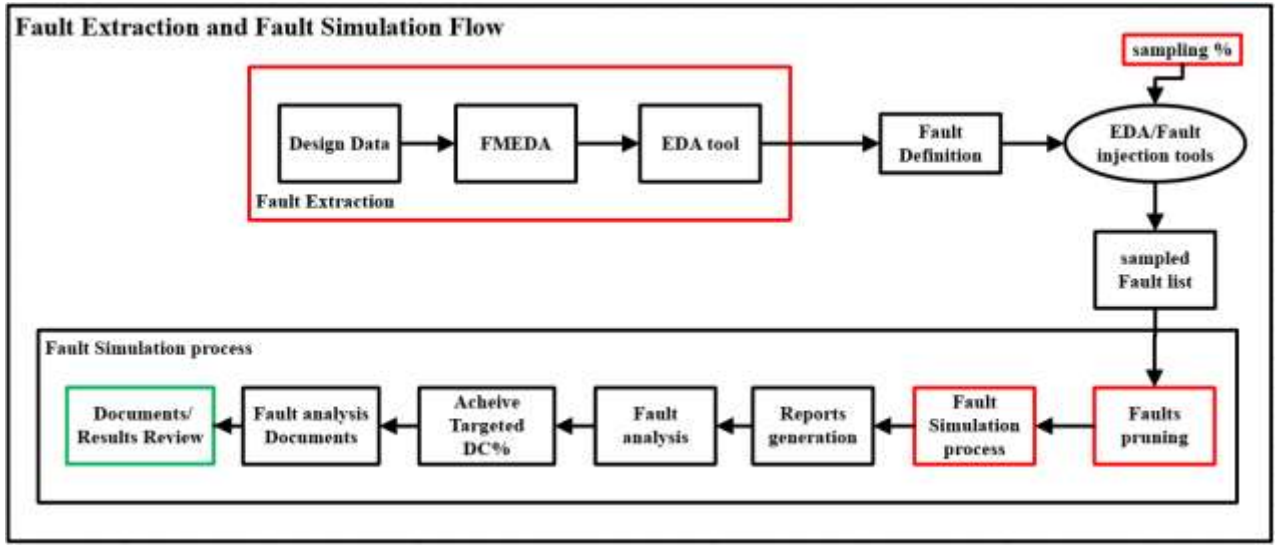



```
#### Safety Verification Plan ####

# Safety Mechanism Definition
SafetyMechanism PSM_001 {
  Detect {
    " top_testbench.dut_top_i.core_cpu.ipx_rf.safety_err_code"
  }
}
# Failure Mode Observability
FailureMode FM_001 {
  Observe {
    "top_testbench.dut_top_i.core_cpu.ipx_rf"
  }
  SafetyMechanisms (PSM_001)
}
# Safety Aware Fault Generation
FaultGenerate FM_019,FM_021 {
  NA [0, 1] { PORT "top_testbench.dut_top_i.core_cpu.ipx_rf.**" }
  NA [0, 1] { VARI "top_testbench.dut_top_i.core_cpu.ipx_rf.**" }
}
```

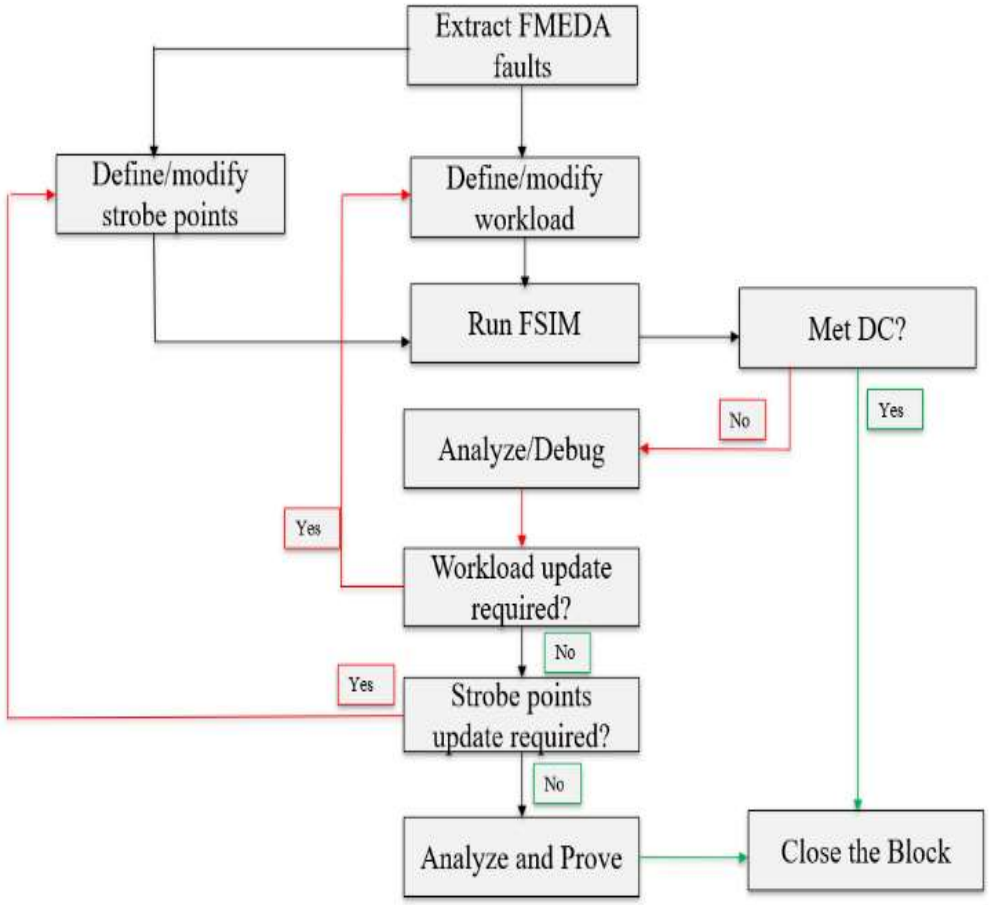
Experimented Methodology

- Accurate mapping of safety-relevant faults is key to efficient fault simulation.
- Targeted fault simulation plans, based on FMEDA data, optimize resource use and ensure ISO 26262 coverage.
- Fault injection and diagnostics are automated and prioritized by safety relevance.
- **Fault pruning:** Removes irrelevant or redundant scenarios.
- **Fault sampling:** Simulates a representative subset, reducing analysis time by up to 10×.
- **Automation:** Streamlines classification and reporting of diagnostic responses.



Fault Injection Iterations

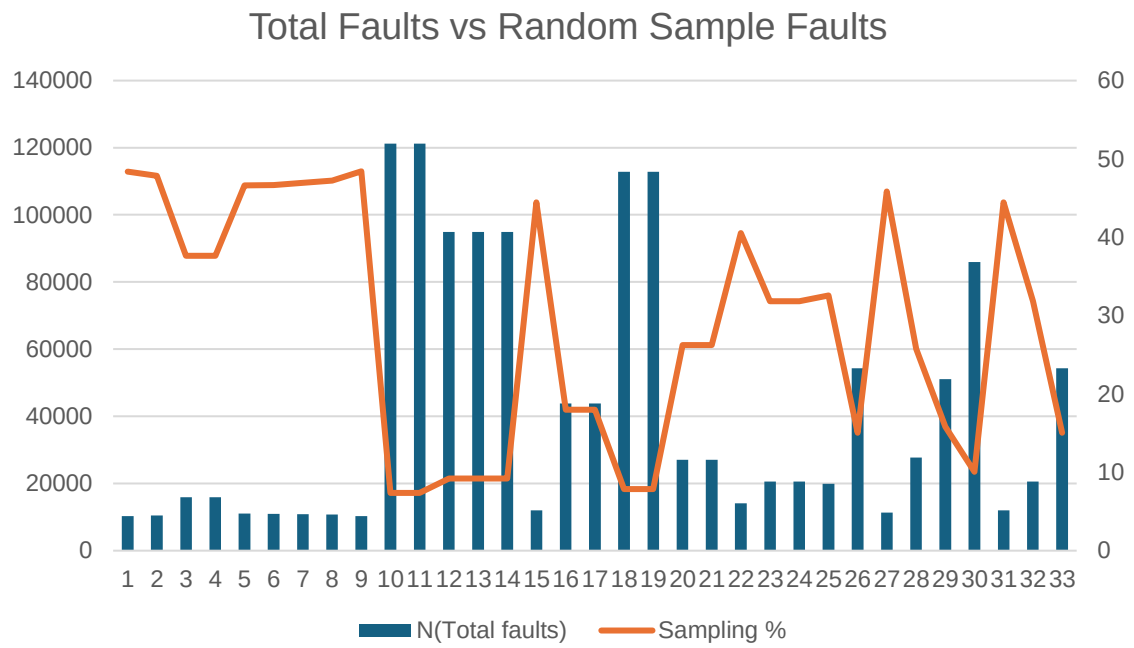
- Process starts with fault extraction, integrating FMEDA data into the fault simulation flow
- **Workload Definition:** Test stimuli and Software Test Libraries (STLs) activate safety mechanisms for each FMEDA partition.
- **Strobe Point Selection:** Critical observation points are added to capture fault effects and diagnostic responses.
- **Fault Simulation & Analysis:** Simulations validate diagnostic coverage; undetected faults are analyzed and workloads refined iteratively.
- **Advanced Fault Debug:** AI and machine learning classify ambiguous faults and suggest targeted injections (phase ongoing).
- **Final Validation:** Once diagnostic coverage targets are met, results are formally proven and the block is closed.



Fault Sampling

FMEDA ENTRY	N(Total faults)	n(Sample faults)	Sampling %
D007_LPD-	10254	4959.43073	48.3658156
D007_LPD-	10480	5011.697456	47.8215406
D007_LPD-	15908	5988.806084	37.6465054
D007_LPD-	15908	5988.806084	37.6465054
D007_LPD-	10996	5126.733531	46.6236225
D007_LPD-	10976	5122.382234	46.6689344
D007_LPD-	10848	5094.332404	46.9610288
D007_LPD-	10740	5070.390798	47.2103426
D007_LPD-	10228	4953.341334	48.429227
D007_LPD-	121222	8899.033732	7.34110453
D007_LPD-	121222	8899.033732	7.34110453
D007_LPD-	94930	8721.721562	9.1875293
D007_LPD-	94930	8721.721562	9.1875293
D007_LPD-	94930	8721.721562	9.1875293
D007_LPD-	12008	5336.394984	44.4403313
D007_LPD-	43796	7876.866308	17.9853555
D007_LPD-	43796	7876.866308	17.9853555
D007_LPD-	112814	8850.614343	7.8453156
D007_LPD-	112814	8850.614343	7.8453156
D007_LPD-	26998	7084.199667	26.2397202
D007_LPD-	26998	7084.199667	26.2397202
D007_LPD-	14090	5711.406745	40.5351792
D007_LPD-	20590	6549.410791	31.8086974
D007_LPD-	20590	6549.410791	31.8086974
D007_LPD-	19898	6477.759805	32.5548286
D007_LPD-	54258	8159.813219	15.0389126
D007_LPD-	11354	5203.216873	45.8271699
D007_LPD-	27718	7132.811875	25.7335012
D007_LPD-	51048	8083.378543	15.8348585
D007_LPD-	85908	8638.381255	10.0553863
D007_LPD-	12008	5336.394984	44.4403313
D007_LPD-	20590	6549.410791	31.8086974
D007_LPD-	54258	8159.813219	15.0389126

- **Fault pruning** eliminates irrelevant, redundant, or low-impact faults, focusing analysis on scenarios that affect system safety and functionality.
- **Fault sampling** selects a statistically representative subset of faults for simulation, significantly reducing the number of cases to analyze.
- These techniques together improve efficiency, cutting simulation time by up to 10× while maintaining accurate safety coverage.
- Running **1 million faults takes huge FSIM time**, analysis time-typically weeks.

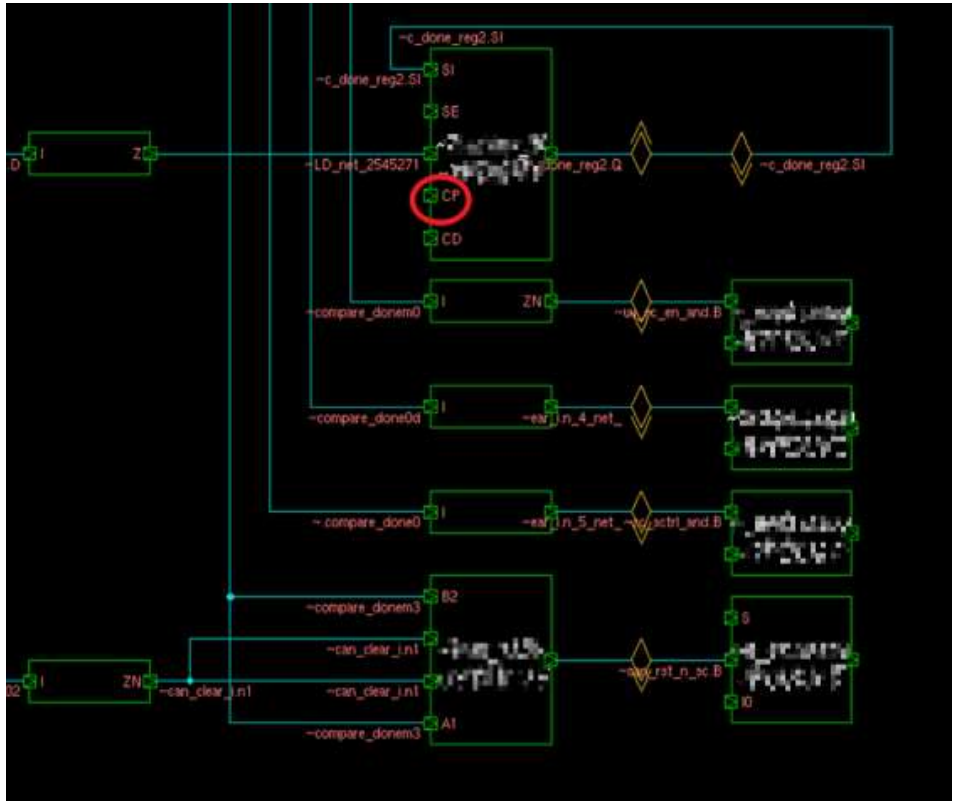


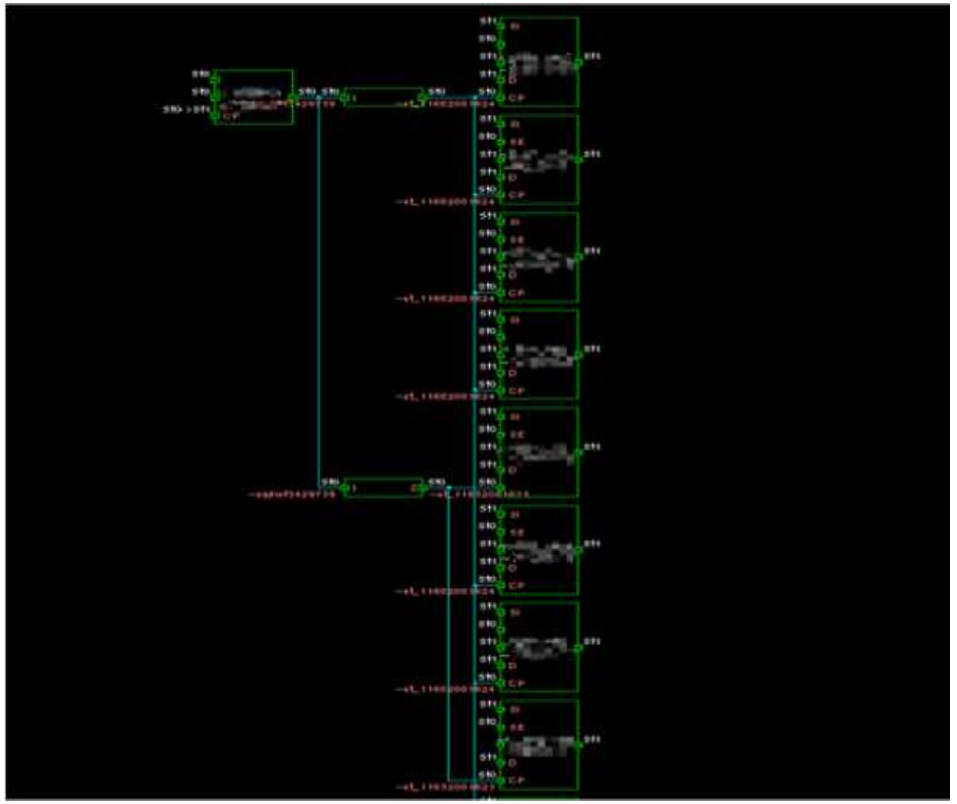
Fault Injection Results (First Iteration)

- Not Observed and Not Controlled faults make around ~26%
- Dangerous Not Detected needs to be reviewed on Residual status
- Assumed Dangerous Unobserved needs to be rerun with different workloads

```
#------------------------------------------------------------------------
# Fault Coverage Summary
#
#                                          Prime              Total
#------------------------------------------------------------------------
# Total Faults:                             7782               7809
#
# Not Observed                    NO         914   11.75%       915  11.72%
# Not Controlled                  NC        1192   15.32%      1193  15.28%
# Not Obs & Not Det               NN         518    6.66%       524   6.71%
#     Obs & Not Det               ON         584    7.50%       596   7.63%
#     Obs &     Det               OD        4574   58.78%      4581  58.66%
#
# Assumed Dangerous Unobserved    AU         518    6.66%       524   6.71%
# Dangerous Detected              DD        4574   58.78%      4581  58.66%
# Dangerous Not Detected          DN         584    7.50%       596   7.63%
# Unselected                      NG        2106   27.06%      2108  26.99%
#
# Fsafe                                              0.00%              0.00%
# DC1                                               58.78%             58.66%
# DC2                                               80.58%             80.35%
# DC3                                               88.68%             88.49%
# DC(Krf)                                           58.78%             58.66%
# DC(Kmpf)                                          58.78%             58.66%
# Max(DC)                                             ---                ---
# SM Faults                                             0                  0
# Errors                                                0                  0
#------------------------------------------------------------------------
# 7809 faults sampled from 11604 possible faults (67.30%)
```

Fault Analysis: Safe Faults





Safe: Scan FF (fault on CP / D / Q, SE=0)

- Safety Reason: Fault cannot reach functional logic
- Diagnostic Logic: Scan disabled, path masked

Safe: Clock Gate (EN S@0)

- Safety Reason: No impact on functional data/control
- Diagnostic Logic: Clock toggles but logic unaffected

Fault Analysis: Expert Judgement (By Debug)

Faults on memory data islands hierarchies are Detected on ecc_ce, ecc_ue signals. As only few memories are exercised in the testcase, faults on those memory Island locations are detected. If workload is enhanced to exercise other RAM memory island's locations faults will be detected. So, the other faults are considered as Detected by Analysis.

Detected mem*data*island fault hierarchies:

DD 1 {PORT " mem_data_island0_reg_275_272_.Q3"}

Detected on the strobe points:
" .ram_isr_ecc_ue"
" .ram_isr_ecc_ce"

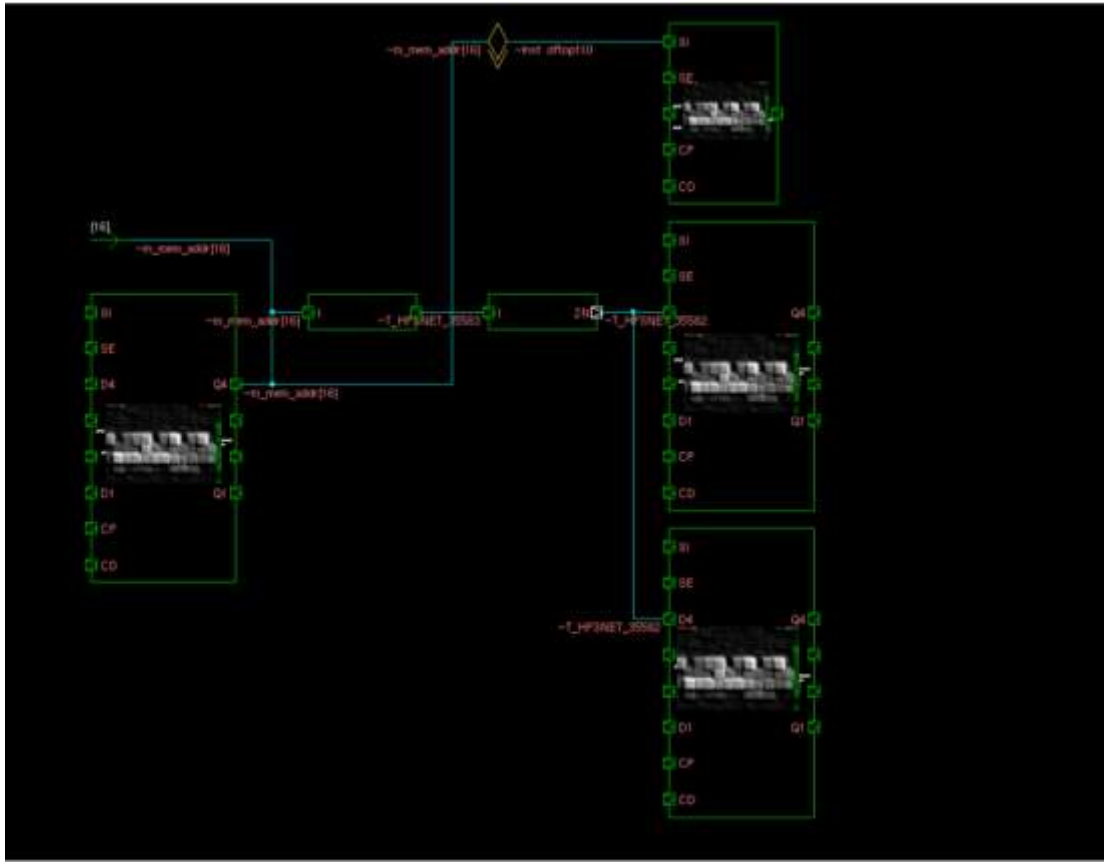
Undetected fault hierarchies:

NO 0 {PORT " _mem_data_island3_reg_251_248_.D4"}

NC 1 {PORT " _mem_data_island0_reg_163_160_.Q1"}

NC 0 {PORT " _mem_data_island0_reg_167_164_.D1"}

NO 0 {PORT " _mem_data_island3_reg_23_20_.CP"}



Detect by Analysis: RAM ECC (other banks)

- Safety Reason: Behavior consistent across all banks
- Diagnostic Logic: ECC guarantees detection and correction

Results: Traditional vs Proposed Methodology

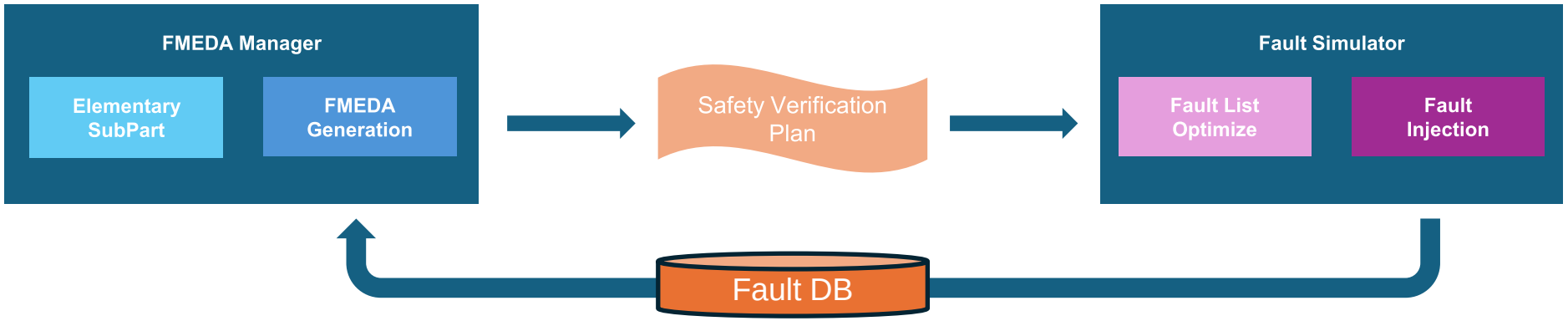
Metric	Traditional Flow	Proposed-Flow	Improvement
Faults Simulated	11,604	7,809	↓ 33%
Traceable Faults	65%	92%	↑ 42%
Unresolved Faults	~4000	~600	↓ 85%
Manual Debug Time	6 weeks	2 weeks	↓ 66%
Audit readiness	Partial	Full	✓

```
#-------------------------------------------------------------------------------
# Fault Coverage Summary
#
#                                                  Prime             Total
#-------------------------------------------------------------------------------
# Total Faults:                                    7782              7809
#
#     Obs &     Det                          OD    4574  58.78%      4581  58.66%
# Detected by Analysis - Expert Judgement    DA    584   7.50%       596   7.63%
# Safe by Analysis - Expert Judgement        SA    2624  33.72%      2632  33.70%
#
# Dangerous Detected                         DD    4574  58.78%      4581  58.66%
#
# Fsafe                                                  33.72%            33.70%
# DC(Krf)                                               100.00%           100.00%
# DC(Kmpf)                                              100.00%           100.00%
# SM Faults                                                  0                 0
# Errors                                                     0                 0
#-------------------------------------------------------------------------------
```

Reduces redundant fault campaigns and improves key safety metrics (SPFM/LFM).

Delivers measurable efficiency gains: 33% fewer faults, 66% less manual debug, 3–5× lower compute resource usage.

Back Annotation



- **Directly load measured/verified** values from Fault campaigns into FMEDA per failure mode to identify potential gaps
- **Maintain traceability** of verified failure modes for audit purposes
- Support **continuous improvement** by updating FMEDA with latest measured data
- **Enhance transparency** with a documented history of changes and updates
- **Ensure compliance** with industry standards through evidence of verification
- Improve collaboration by centralizing fault data and traceability

Best Practices: Meeting Safety Goals

FMEDA driven and Fault aware injection

- Target fault nodes (Safety relevant)
- Injection granularity

Clear and scalable safety verification plan

- Fault pruning, Random Sampling, closure goals (Target DC)

Strong debug and observability on the fault injection platform

- Automated Root close analysis and manual debug hooks
- Usage of AI models in assisted fault debug

Automation and data-driven closure

- Fault lists, and measured DC back to FMEDA
- Traceability

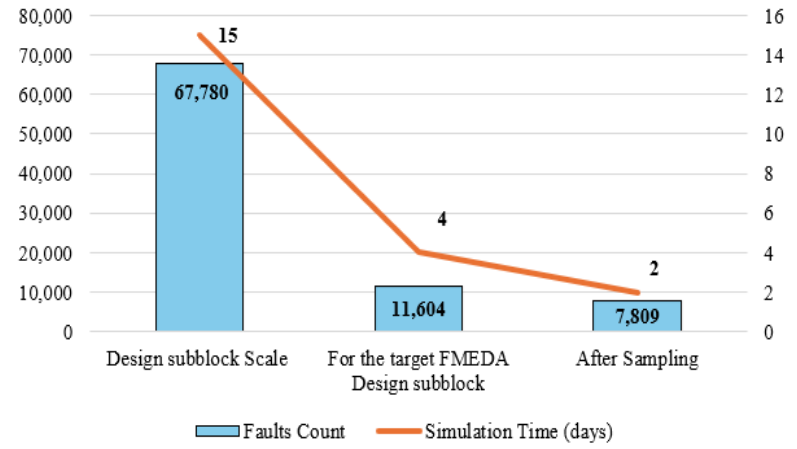
Partnership with EDA Solutions Providers

- Alignment and best strategy to success

Conclusion

- FMEDA-driven fault simulation provides a structured, ISO 26262-compliant safety verification process for automotive SoCs.
- Each simulated fault is mapped to its FMEDA entry, ensuring traceability, accuracy, and audit readiness.
- Automated progress tracking highlights coverage gaps and areas for improvement.
- Validated on production SoC blocks, demonstrating scalability for next-generation designs.
- Achieves equal or better diagnostic coverage than traditional methods with enhanced scalability and audit readiness.
- Transforms fault simulation into a repeatable, standards-compliant methodology, closing the safety verification loop.

Stage	Flop count	Faults Count	Simulation Time (days)
Design subblock Scale	26939	67,780	15
For the target FMEDA Design subblock	3562	11,604	4
After Sampling	3562	7,809	2



THANK YOU