Breaking Down Failures: Elementary Subpart Granularity Being Foundation of Safety Analysis & Verification

Luc Baudoin, Sr Safety Engineer, AMD Austin

Vedant Garg, Solution Architect, Synopsys Austin

accellera SYSTEMS INITIATIVE

2026 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION UNITED STATES

SANTA CLARA, CA, USA

MARCH 2 - 5, 2026

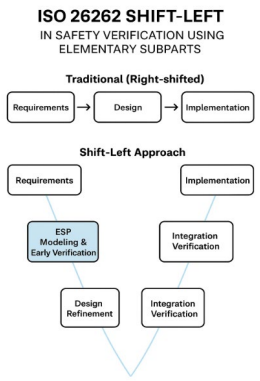
Introduction and Objective

Problem with Traditional approach

1. Late availability of data:
Traditionally fault injections and quantitative FMEDA are performed on netlists. Any architectural change is extremely hard to incorporate and making the step just a final checkpoint.

2. Simulation and compute overhead:
Multiple iterations are spent removing most injected faults which are functionally or structurally redundant thereby adding to computing overhead.

3. Limited architectural insight:
Traditional FMEDA is reactive, focusing on what fails rather than why it is vulnerable.



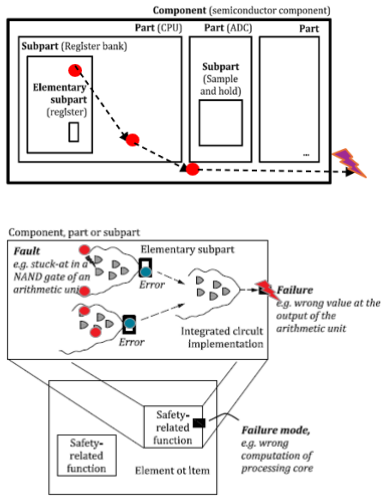
We propose **elementary subpart extraction (ESE)** an automated safety analysis methodology that decomposes the design's sequential logic into safety-relevant units using **fan-in COL analysis and timing-based overlap correction**. The ESE framework establishes an analytical mapping between the RTL and FMEDA level failure contributions, such enabling quantitative evaluation well before fault simulation.

Elementary Subpart extraction

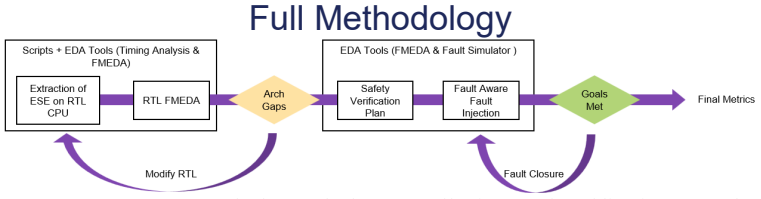
- Faults originate at the "Elementary Sub Part" level and may propagate further to result in system failures.
- Random HW faults can be of both Permanent or transient type and can occur at any time.
- Base Failure Rate is allocated based on the technology data for different HW logic types, such as digital, 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.



Full Methodology

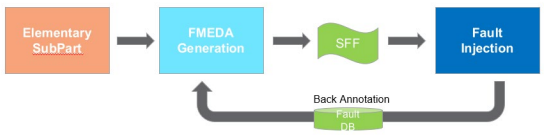


Extraction of ESE on RTL: Calculate each element's effective area by adding its own and upstream COL gate areas, then use timing analysis to proportionally adjust overlaps, resulting in weighted ESE's that reflect each element true failure exposure.

RTL FMEDA: Structurally similar ESEs are grouped into FMEDA entries, combining effective area and failure rate, enabling early What-If analysis and safety metric previews, EDA tools automate, check for errors, and track changes throughout the FMEDA process.

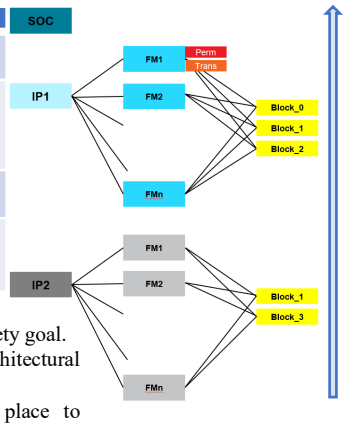
Safety Verification Plan: Automated FMEDA extraction creates a traceable Safety Verification Plan.

Fault Aware Fault Injection: Fault-aware injections improve test relevance, accelerate creation, and link results to failure modes, reducing manual effort, minimizing errors, and supporting compliance and collaboration



FMEDA

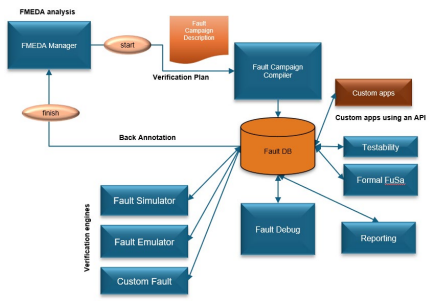
Level	Safety Activities	Verification Focus
Component	Full Semiconductor device under analysis	SoC safety plan, FMEDA summary
Part	Safety architecture design, ASIL decomposition, top-level SPFM/LFM computation	Architectural verification, safety goal tracing
Subpart	FMEDA preparation, local safety mechanism definition	Block-level simulation and fault injection
Elementary Subpart	Fault modeling, diagnostic coverage analysis	RTL/Gate Fault injection, formal proofs



1. Identify faults that can propagate to and violate the safety goal.
2. Determine the effects of each fault within the architectural context.
3. Ensure the appropriate diagnostic coverage is in place to mitigate the faults.
4. Demonstrate that residual risk after applying diagnostics is acceptable for the assigned ASIL.

A hierarchical decomposition model enables scalable, traceable safety analysis of complex SoCs by refining details at multiple levels and aggregating lower-level results into system-level safety metrics.

Integrated Fault DB and Fault Simulation Results



- Support reading the verification plan and extraction of Faults per FM
- Connection with Simulation, Emulation, Formal and Custom fault.
- Connection with Verdi Fault debug app
- Support loading the verification results back to FMEDA tool
- Preserve the traceability

Metric	Traditional Flow	ESE Fault Aware	Improvement
IP 1			
SPFM	62.3%	91.5%	46.8%
Faults Simulated	11,604	7,809	33%
Unresolved Faults	1,200	600	50%
IP 2			
SPFM	77.8%	90.7%	16.5%
Faults Simulated	72,867	43,632	40%
Unresolved Faults	5,100	870	83%

- **Higher accuracy**: Achieved 30–40% better correlation between injected faults and safety goals
- **Reduced redundancy**: Cut redundant fault simulations by over 60% through more targeted injections.
- **Enhanced traceability**: Improved audit confidence by mapping each test to a specific logical unit (ESE) rather than arbitrary gates

Conclusions

Proactive Safety Analysis: ESE systematically decomposes RTL into fine-grained subparts, shifting safety analysis from reactive verification to proactive architectural design.

Improved Metrics: Applying ESE leads to significant improvements in SPFM and LFM convergence, enhancing the reliability of semiconductor safety assessments.

Enhanced Accuracy: Area-weighted subpart modeling delivers more precise fault rate attribution and diagnostic balancing, resulting in more accurate safety analysis.

Topics	Elementary Subpart Methodology Contribution/Gains
Shift-Left Enablement (FMEDA)	Enables FMEDA computation at RTL without waiting for final gate-level data.
Architectural Visibility	ESE-based modeling allows detection of hidden architectural vulnerabilities.
Iterative Efficiency	Allows rapid re-evaluation of safety metrics when RTL or safety mechanism bindings change.
Overlap Correction	Eliminates double counting of shared logic via timing and dependency analysis, yielding realistic λ allocation.
Hierarchical Integration	Supports compositional safety analysis from IP to SoC level, enabling reuse of ESP data as verified work products.
Scalability	This enhanced FMEDA approach leverages early RTL data to quantify failure propagation paths thus improving scalability for both FMEDA and Fault injection flow.

Contact Information

Luc.Baudoin@amd.com

AMD together we advance_

Vedantg@synopsys.com

SYNOPSYS®