2026
DESIGN AND VERIFICATION™
DVCON
CONFERENCE AND EXHIBITION
UNITED STATES
SANTA CLARA, CA, USA
MARCH 2 - 5, 2026

Early FMEDA at RTL for Functional Safety: Correlating RTL Metrics to GLS for Accurate Architectural Analysis

Vedant Garg
Sr Solutions Architect
Synopsys Austin

Myungkyoon Yim
Principal Researcher
Hyundai Korea

Agenda

- Motivation, Why this work matters?
- Traditional Methodology
- Proposed Methodology (RTL FMEDA)
- Case Study
  - Open Core RISC-V
  - Automotive SOC / IP
- Correlation Summary
- Overall Closed-loop Safety Workflow
- Conclusion

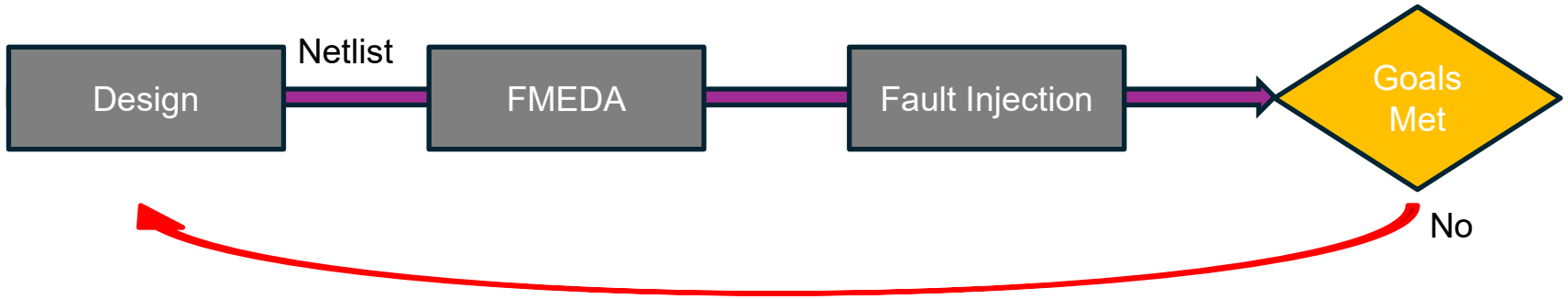
Motivation: Why This Work Matters

- ISO 26262 requires quantitative proof of random hardware fault coverage
- Traditional safety metric analysis is **performed late** in the design cycle using Gate-Level Simulation or post-layout analysis.
- Gate-level fault injection is:
  - **Computationally expensive**
  - **Slow to iterate**
  - **Poorly mapped back to RTL intent**
- This **reactive approach conflicts with ISO 26262's** goal of proactive, "safety by design."

Key Question?

Can we trust RTL-based safety metrics early and prove it?

Traditional Methodology



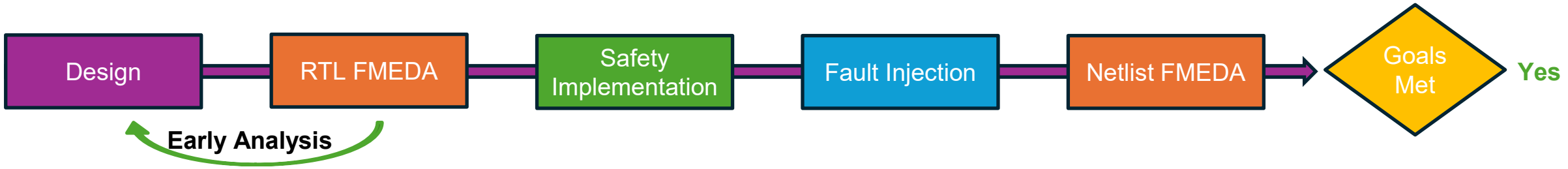
- Design hierarchy is flattened for timing and optimization
- **RTL hierarchy is lost**, No connection to architectural intent
- **Manual reconstruction** required:

  - Mapping gates -> RTL blocks

  - Mapping safety mechanisms -> logic cones
- **Missing hardware protection** leads to slower, software-based integrity checks.
- Underscores the need for early safety analysis, as enabled by **RTL-based FMEDA.**

Flattened Node (Netlist)	Digital_Area (μm^2)
U3254/AOI22_X1	4.8
U3255/INV_X2	1.5
U3256/NAND3_X1	3.6
U3257/BUF_X1	1.2
U3258/DFFR_X1	4.3
U3259/OR2_X1	2.4

Proposed Methodology Driven By RTL FMEDA



Lightweight Synthesis Abstraction:

- Fast structural extraction from RTL
- Bridges RTL intent with gate-level reality

Cell_Type	Digital_Area (µm²)	Transistor Count
DFF_X1	4.2	20
NAND2_X1	2.5	10
NOR3_X2	3.8	14
INV_X1	1.1	6
XOR2_X1	3.2	12
AOI21_X2	4.5	16

Building Hierarchical RTL FMEDA:

- RTL module extracted based on cell type, area, transistor count.
- Aggregate Structural data per block

Metric(M) = i∑n(Ni×Ai)

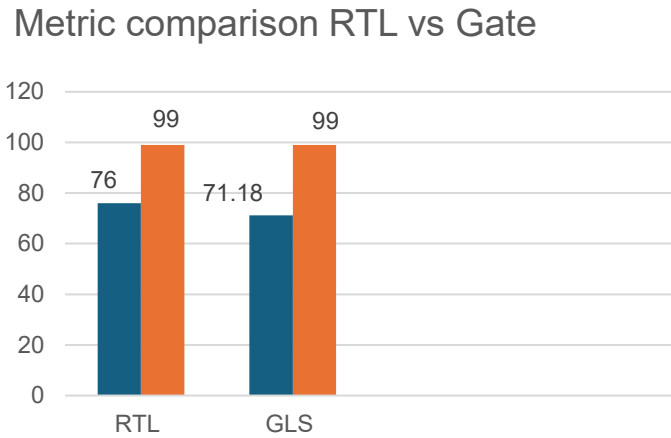
RTL_Hierarchy	Total_Cells	Aggregated_Area (µm²)	Total_Transistors
top.cpu.alu	22,450	65,800	290,000
top.cpu.decoder	11,320	34,200	155,000
top.memory.controller	14,970	42,750	195,000
top.io.interface	8,540	21,900	99,800

RTL Fault Injection and Validation:

- Automated Fault list
- Injected at RTL with structural intent
- Reduces risk of late-stage changes by enabling early validation

Correlation Results: RTL vs Gate-level

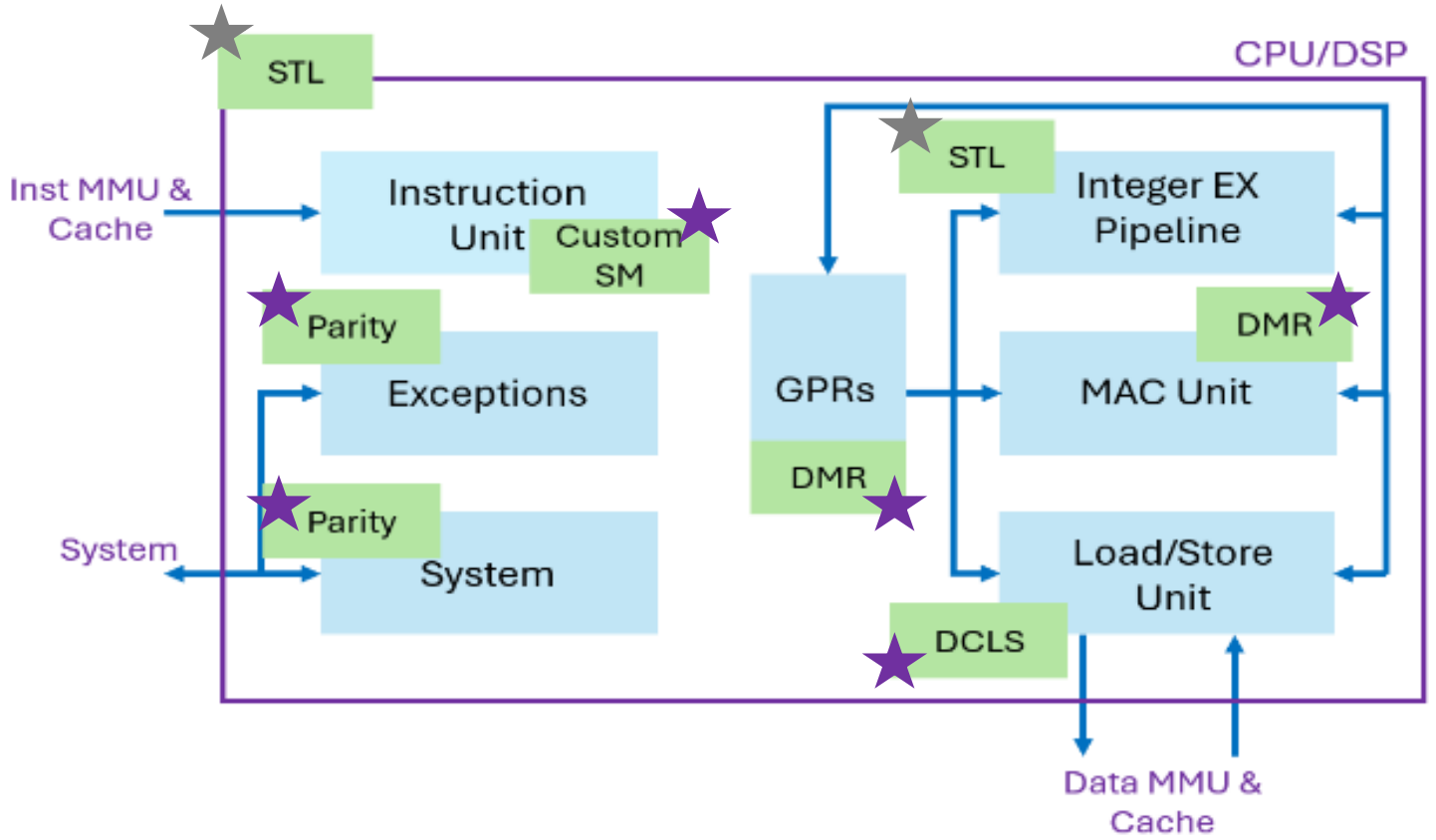
Metric	FIT (Failures in Time)	PMHF (FIT)	SPFM (%)	LFM (%)
RTL FMEDA	0.1805	0.07821	76.0	99.0
Gate-Level FMEDA	0.09933	0.06012	71.18	99.0
Delta	0.08117	0.01809	6.34%	0.0%



- SPFM Delta exists, some logic optimization, are reduction etc
- Does not invalidate architectural safety intent
- RTL still correctly identifies where protection is needed

Case Study 1: RISC-V Open Core Architecture

	SW Test
	Fusion Compiler FuSa



Case Study 1: FMEDA Data (RTL vs Gate)

	VC FSM
	Spyglass FA, DC

Simple Hierarchy Name	Digital_Area
or1200_alu	8580.00
or1200_rf/rf_a	7413.00
or1200_mult_mac/or1200_gmultp2_...	3971.00
or1200_sprs	2875.00
or1200_except	2765.00
or1200_mult_mac	2677.00
or1200_genpc	1850.00
or1200_ctrl	1153.00
or1200_operandmuxes	768.00
or1200_wbmux	761.00
or1200_if	590.00
top	499.00

Name	SPFM	LFM	PMHF	PMHF Distribution	FD	λ	λ_{nSR}	λ_{nS}	λ_{PVSG}	In-use DC(K_{RF})	λ_{RF}
SoC	77.23%	-	8.167E-02	100.00%	100.00%	1.923E-01	0.000E+00	1.385E-01	1.385E-01	77.23%	1.809E-02
or1200	77.23%	-	8.167E-02	100.00%	100.00%	1.923E-01	0.000E+00	1.385E-01	1.385E-01	77.23%	1.809E-02
or_CPU	76.00%	-	7.821E-02	95.76%	93.87%	1.805E-01	0.000E+00	1.311E-01	1.311E-01	76.00%	1.802E-02
or_DC	99.00%	-	1.606E-03	1.97%	2.62%	5.043E-03	0.000E+00	3.413E-03	3.413E-03	99.00%	3.413E-05
or_IC	99.00%	-	1.192E-03	1.46%	2.77%	5.332E-03	0.000E+00	2.539E-03	2.539E-03	99.00%	2.539E-05
or_PIC	99.00%	-	6.624E-04	0.81%	0.74%	1.424E-03	0.000E+00	1.424E-03	1.424E-03	99.00%	1.424E-05

Simple Hierarchy Name	Digital_Area
or1200_rf/rf_a	4439.00
or1200_alu	3173.00
or1200_mult_mac/or1200_gmultp2_...	2370.00
or1200_except	1675.00
or1200_sprs	1632.00
or1200_mult_mac	1599.00
or1200_genpc	1050.00
or1200_ctrl	776.00
or1200_wbmux	456.00
or1200_operandmuxes	423.00
or1200_lsu_shadow	334.00
or1200_lsu	334.00
or1200_if	324.00

Name	SPFM	LFM	PMHF	PMHF Distribution	FD	λ	λ_{nSR}	λ_{nS}	λ_{PVSG}	In-use DC(K_{RF})	λ_{RF}
SoC	73.16%	-	6.356E-02	100.00%	100.00%	1.067E-01	0.000E+00	1.041E-01	1.041E-01	73.16%	1.794E-02
or1200_cpu	71.18%	-	6.012E-02	94.59%	93.08%	9.933E-02	0.000E+00	9.667E-02	9.667E-02	71.18%	1.787E-02
or1200_dc_top	99.00%	-	1.465E-03	2.30%	2.94%	3.140E-03	0.000E+00	3.140E-03	3.140E-03	99.00%	3.140E-05
or1200_ic_top	99.00%	-	1.588E-03	2.50%	3.19%	3.399E-03	0.000E+00	3.399E-03	3.399E-03	99.00%	3.399E-05
or1200_pic	99.00%	-	3.852E-04	0.61%	0.79%	8.408E-04	0.000E+00	8.408E-04	8.408E-04	99.00%	8.408E-06

Case Study 1: Fault Injection Validation (Gate-Level)

- 12500 Randomly sampled stuck-at faults
- Key Metrics, Fsafe (safe faults) and Fault Coverage (DC)

		Total
Number of Faults:		12500
Untestable Faults:		59
Untestable Unused	UU	46
Untestable Tied	UT	13
Testable Faults:		12441
Status Groups		
Assumed Dangerous Unobserved	AU	197
Dangerous Detected	DD	8813
Dangerous Not Detected	DN	1126
Unselected	NG	2305
Untestable	UG	59
Coverage		
Fsafe		0.98%
DC		70.50%
Errors		0

Correlation Analysis

Metric	RTL Abstraction (Proposed)	GLS w/o verification (Traditional Est)	GLS w Verification (Traditional Actual)	Correlation Est (Traditional Est vs Traditional Actual)	Correlation Actual (Traditional Actual vs Proposed)	Overall Prediction Accuracy
SPFM	76%	71.18%	70.78% (With Fsafe)	70.78 / 71.18 = 0.995 (99.5%)	70.78 / 76 = 0.932 (93.2%)	(99.5+93.2) /2 = 96.35%
LFM	99%	99%	-	-	-	100%

- Comparison of FMEDA-derived metrics and fault injection results established quantitative correlation between gate-level and early RTL metrics.
- Demonstrates the value of early safety assessment and continuous validation throughout the design flow.

Case Study 2: Automotive SoC

	VC FSM
	Spyglass FA

- Case study focused on a **production Automotive SoC IP block**
- **RTL FMEDA** built from lightweight synthesis
- Early metrics, SPFM at RTL:96.49%
- **High diagnostic coverage**

Simple Hierarchy Name	Digital_Area
iomux_aud_top/iomux_aud_sfr	3202.00
iomux_aud_top/iomux_aud	1173.00
iomux_aud_top/iomon_aud_gpio0	477.00
iomux_aud_top/iomon_aud_gpio10	477.00
iomux_aud_top/iomon_aud_gpio11	477.00
iomux_aud_top/iomon_aud_gpio12	477.00
iomux_aud_top/iomon_aud_gpio13	477.00
iomux_aud_top/iomon_aud_gpio14	477.00
iomux_aud_top/iomon_aud_gpio15	477.00
iomux_aud_top/iomon_aud_gpio1	477.00
iomux_aud_top/iomon_aud_gpio2	477.00
iomux_aud_top/iomon_aud_gpio3	477.00

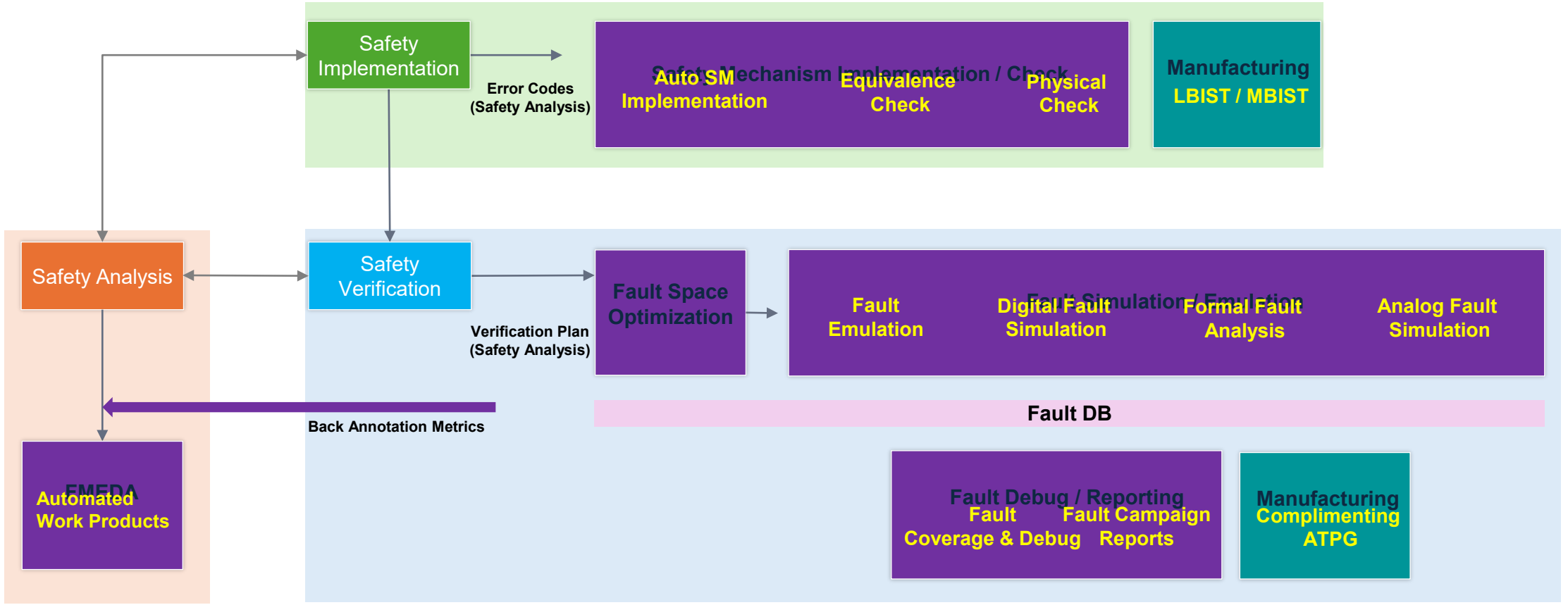
Name	SPFM	LFM	PMHF	PMHF Distribution	FD	λ	λ_{nSR}	λ_{nS}	λ_{PVSG}	In-use	λ_{RF}
IPDEV	96.49%	-	9.587E-03	100.00%	100.00%	4.008E-01	2.382E-02	9.252E-02	1.371E-02	72.37%	3.787E-03
DMA_Wrapper	100.00%	-	8.858E-05	0.92%	13.90%	5.572E-02	4.589E-03	1.885E-02	0.000E+00	NaN%	0.000E+00
GPIO_Controller	94.33%	-	6.284E-03	65.55%	21.80%	8.737E-02	1.923E-02	6.683E-02	1.371E-02	72.37%	3.787E-03
OTP_Wrapper	NaN%	-	0.000E+00	0.00%	0.00%	0.000E+00	0.000E+00	0.000E+00	0.000E+00	NaN%	0.000E+00
PWM	NaN%	-	0.000E+00	0.00%	62.45%	2.503E-01	0.000E+00	0.000E+00	0.000E+00	NaN%	0.000E+00
Top_FCCU	100.00%	-	3.214E-03	33.53%	1.85%	7.405E-03	0.000E+00	6.839E-03	0.000E+00	NaN%	0.000E+00

Correlation Summary

Comparison Stage	SPFM Ratio (ρ)	Delta (%)	Interpretation
Correlation Est (Traditional Est vs Traditional Actual)	0.995	0.4%	Excellent Consistency
Correlation Actual (Traditional Actual vs Proposed)	0.93	7%	Minor decrease, synthesis impact

- SPFM consistency across design stages is measured by the ratio of post-verification to pre-verification SPFM (~0.995), indicating excellent diagnostic coverage alignment, with minimal delta (0.4%).
- Gate-level vs. RTL SPFM yields strong correlation ($\rho \approx 0.93$), showing only slight reduction after synthesis.
- **Validates RTL FMEDA as a reliable predictor** of final safety performance,
- **Provide early confidence** and minimizing uncertainty before implementation

Overall Closed-Loop Safety Flow



Conclusion

- Demonstrates a robust, experimentally validated **RTL-based FMEDA methodology** for early functional safety assessment
- Lightweight synthesis abstraction enables accurate extraction of digital area and transistor data for early FMEDA analysis.
- Automated data aggregation and targeted fault injection support reliable calculation of SPFM and LFM, guiding architectural decisions.
- Integrates fault injection, classification, and safety metric derivation at the RTL stage for predictive safety risk and diagnostic coverage analysis.
- Correlation framework aligns RTL-based FMEDA results with gate-level outcomes; case studies **show high correlation (ρ = 0.93)** and minimal differences within engineering tolerances.
- Predictive Reliability, Architectural Traceability, and Early Safety Closure enabling efficient ISO 26262 compliance and "**Shift Left**" safety evaluation.

Thank You