Synergizing Functional Safety and Fault Simulation:

Towards Robust and Reliable Systems in Safety-Critical SoCs.

Santosh Mahale (smahale@marvell.com)

Shantanu Lele (slele@marvell.com)

Problem Statement/Introduction

Streamlining Fault Simulation Workflows for IP, Sub-System & SoC Verification with Marvell methodology flow.

- Safety-critical design requires all potential failures in the design to be evaluated and determines whether they can be detected.

Problem: The verification of large and complex SoCs requires efficient fault simulation workflows to optimize simulation time and the rapid identification and analysis of "Dangerous and Not Detected" faults during the verification process to improve safety mechanisms. Relying solely on functional verification can delay the processes in achieving required safety process matrix.

Objective: Optimize fault simulation workflows for Complex IPs, leveraging parallel processing, divide & concur approach, simulation acceleration, formal verification, and other techniques to reduce simulation times without compromising accuracy.

Fault Detection Criteria

ND: Not Detected
DD: Detected Dropped
PD: Potential Detected

Good Design	Faulty Design			
	0	1	Z	X
0	ND	DD	PD	PD
1	DD	ND	PD	PD
Z	ND	ND	ND	ND
X	ND	ND	ND	ND

Proposed Methodology/Advantages

What is Functional Safety (FuSa)…?

- To ensure that system operate safely and reliably when dealing with potential hazards or dangerous situations.
- Functional Safety is based on the idea of preparing for the risk as failure occurs.
- **What is Functional Safety Mechanism…?**
  - The ability of the safety mechanism to correct, react, or flag the violation of a safety goal.

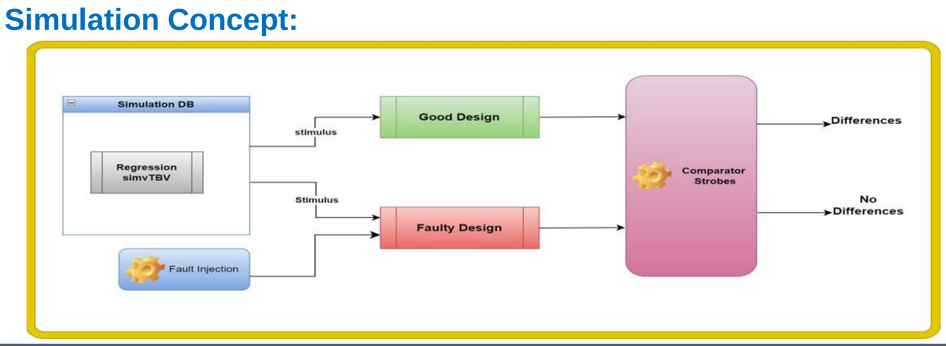
Types Of Functional Safety Mechanism:

1. Error Detection and Correction 2. Redundancy
3. Watchdog Timer 4. Parity Protection

Types Of Faults to be injected in the design:

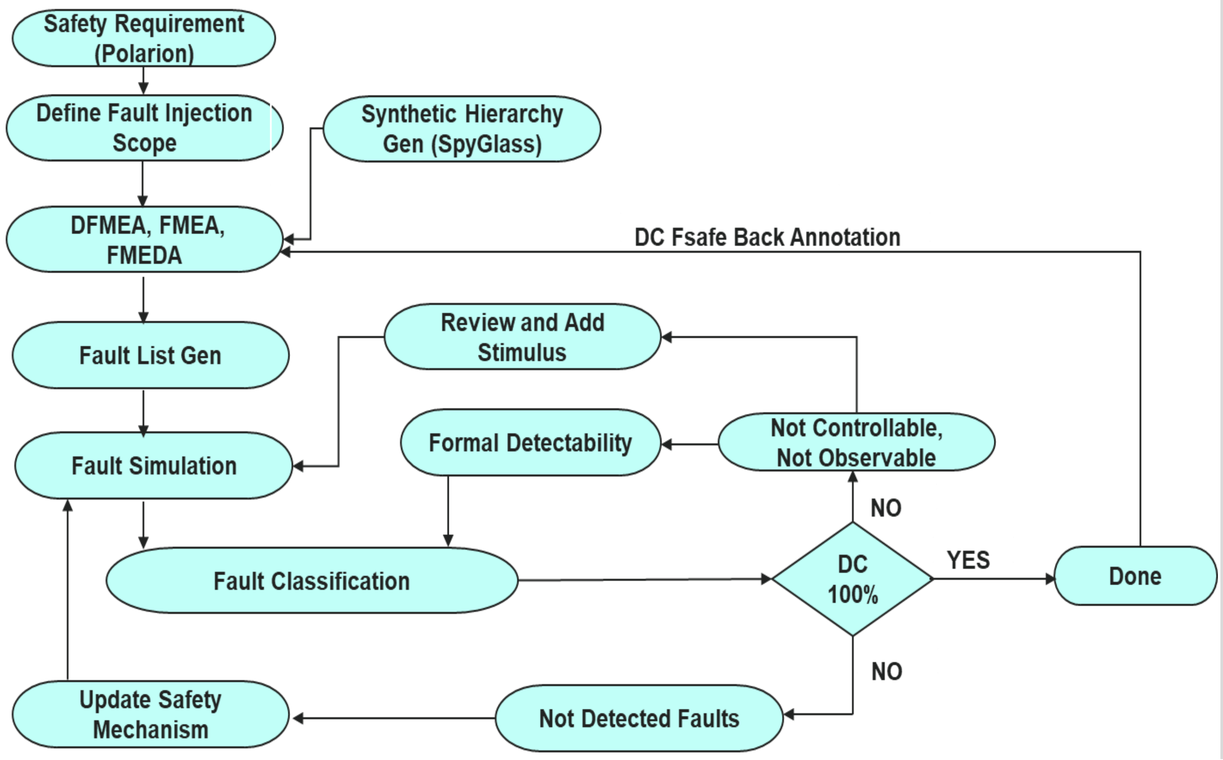
1. Stuck-At Faults 2. Transient Faults 3. Expression Faults

Fault Simulation Concept:



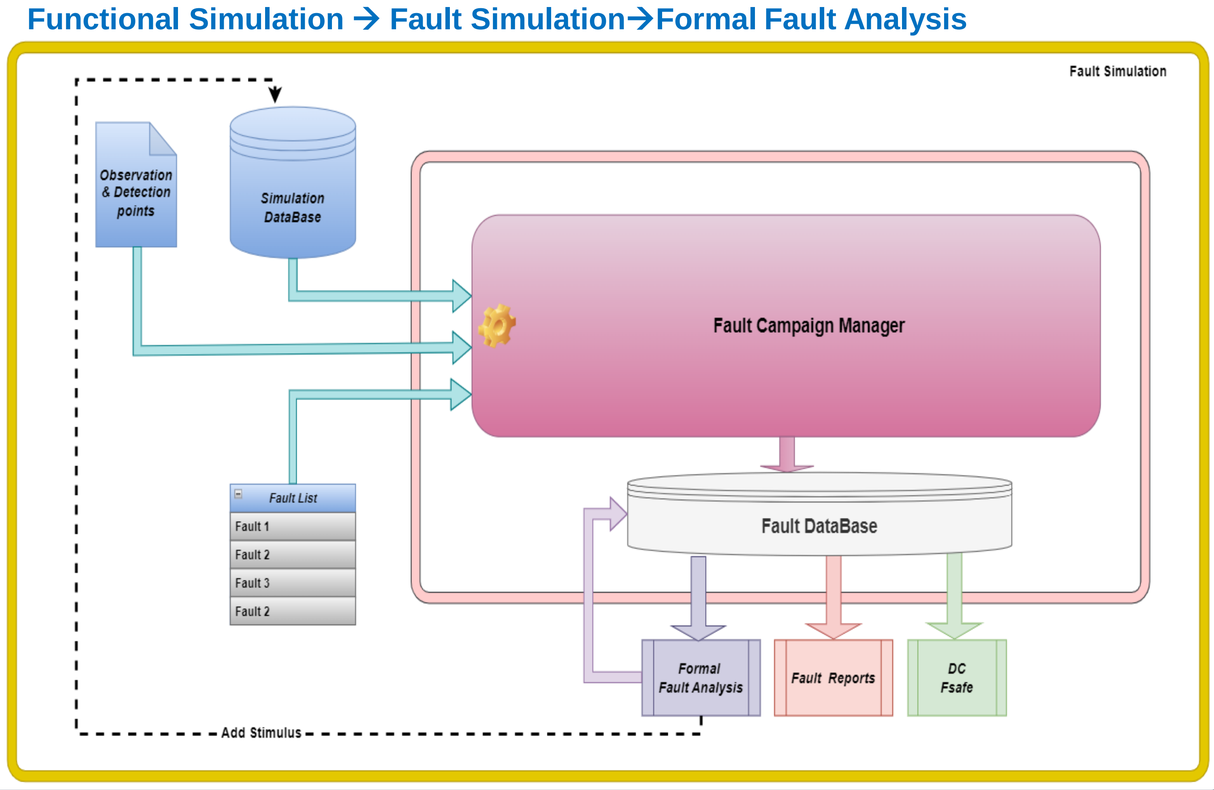
Implementation Details/Diagram

Fault Simulation Methodology Flow: (Functional Sim→Fault Sim→Formal Analysis)

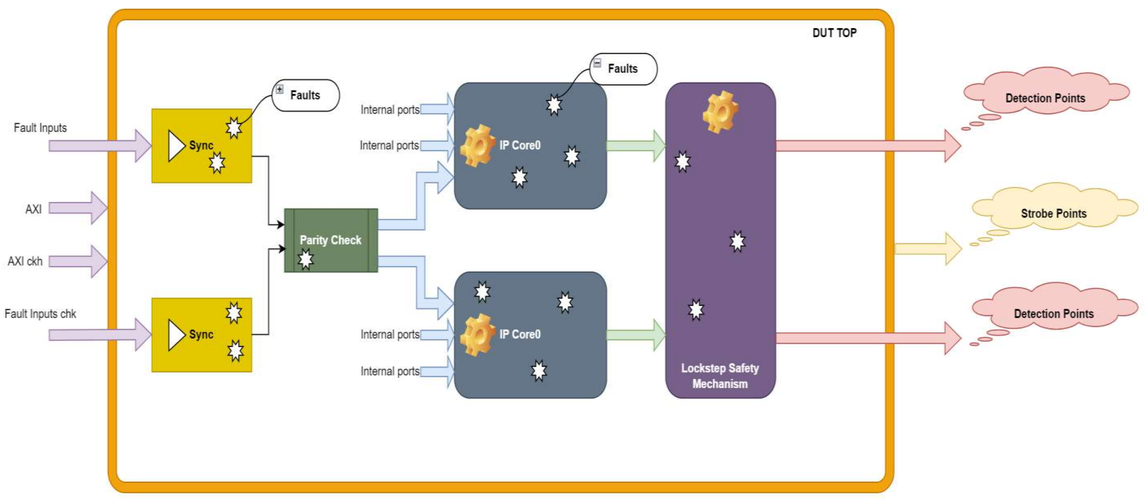


Implementation Details/Flow Chart

Functional Simulation → Fault Simulation→Formal Fault Analysis



Case Study:



Conclusion

- Developed the standard and uniform methodology flow for fault simulation to achieve an ASIL-D compliance for complex critical safety designs.
- Reduction in time to achieve 100% Diagnostic Coverage with the methodology flow (Functional Sim→Fault Sim→Formal Fault Analysis).
- "Not Observed and Not Detected" dangerous faults can expose potential holes in functional verification as well.

Results :

Fault Simulation with Formal Fault Analysis Final Report:

In below report the OD (Observed & Diagnosed) status faults in fault simulation is 93.97%.

After performing the formal Fault Analysis on same database, the OD status faults are increased up to 97.92% in DC , providing more confidence in design.

Fault Simulation				
Category	**Subcategory**	**Count**	**Percentage**	**Cumulative %**
Total Number of Faults		14342	100.00%	
Untestable Faults		100	0.70%	100.00%
	Untestable Blocked (UB)	58	0.40%	58.00%
	Untestable Tied (UT)	42	0.29%	42.00%
Testable Faults		14242	99.30%	100.00%
	Not Tested (NT)	136	0.95%	0.95%
	Not Observed (NO)	22	0.15%	0.15%
	Not Controlled (NC)	123	0.86%	0.86%
	Not Observed Not Diagnosed (NN)	484	3.37%	3.40%
	Observed Diagnosed (OD)	13477	93.97%	94.63%
Status Groups				
	Dangerous Diagnosed (DD)	**13477**	**93.97%**	**93.97%**
	Safe (SA)	100	0.70%	
	Safe Unobserved (SU)	765	5.33%	
Coverage	Diagnostic Coverage			100.00%

FuSa Formal (Cumulative With Simulation Results)				
Category	**Subcategory**	**Count**	**Percentage**	**Cumulative %**
Total Number of Faults		14342	100.00%	
Untestable Faults		245	1.71%	100.00%
	Untestable Unused (UU)	89	0.62%	36.33%
	Untestable Blocked (UB)	58	0.40%	23.67%
	Untestable Tied (UT)	98	0.68%	40.00%
Testable Faults		14097	98.29%	100.00%
	Not Observed & Not Detected (NN)	54	0.38%	0.38%
	Observed & Detected (OD)	14043	97.92%	99.62%
Status Groups				
	Assumed Dangerous Unobserved (AU)	54	0.38%	
	Dangerous Detected (DD)	**14043**	**97.92%**	
	Untestable (UG)	245	1.71%	
Coverage				
	Fsafe			1.71%
	DC(Krf)			99.62%

REFERENCES

- ISO 26262 Safety guide.