An Ideal FuSa Verification Solution!

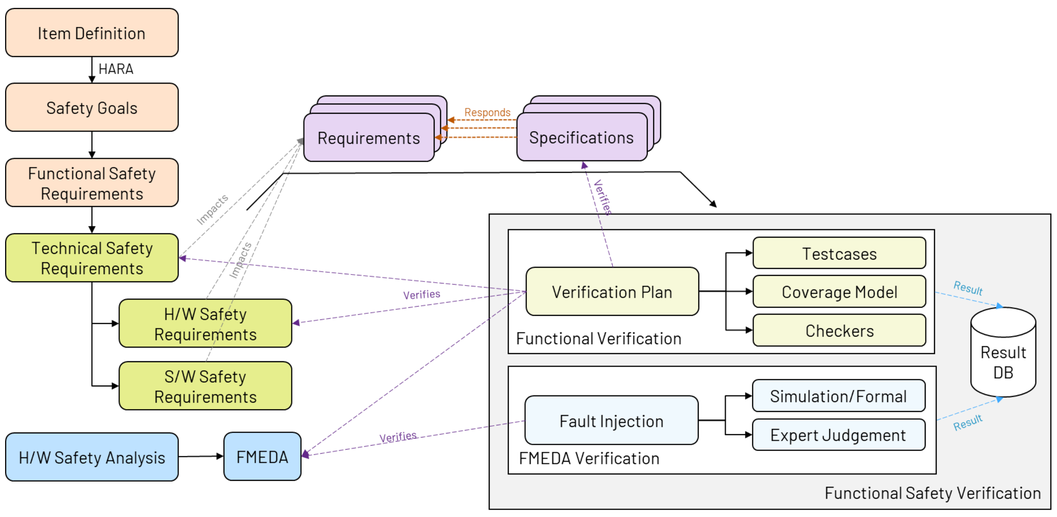
Prashant Ravindra

Analog Devices

Introduction

Functional Safety (FuSa) – Ensuring of absence of unreasonable risk due to hazards caused by malfunctioning of electrical/electronic systems.

FuSa Verification is a super-set of functional verification as it demands actions performed beyond the scope of functional verification.



Requirements and Expectations

Fault debugging | Comprehensive fault classifier | Campaign and result analyzer

Single source of truth | Spec-Design-Verif correlation | Safety design development

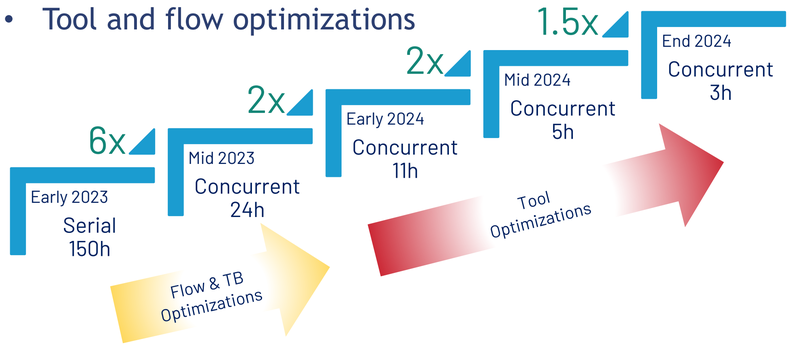
Evolution

While it may appear that a significant DV time is spent on fault campaigns, it's a thing of the past!

Close collaboration with EDA partners resulted in massive reduction of the fault-campaign runtimes from 1-week to 3h for an SoC developed for ASIL-D applications.

It involved two stages:

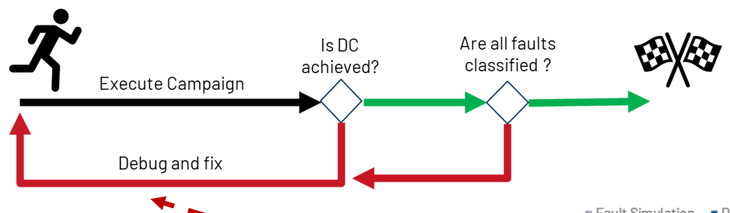
- Serial to Concurrent migration
- Tool and flow optimizations

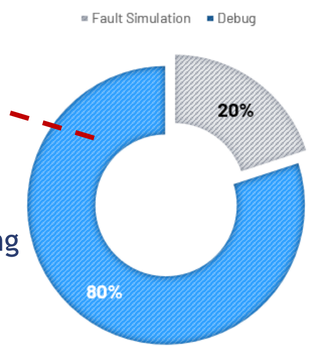


Production Design - GLS DFI Campaign

- 50K Nodes
- ~42K Detections (DD+DU) + ~7K Safe

Concern





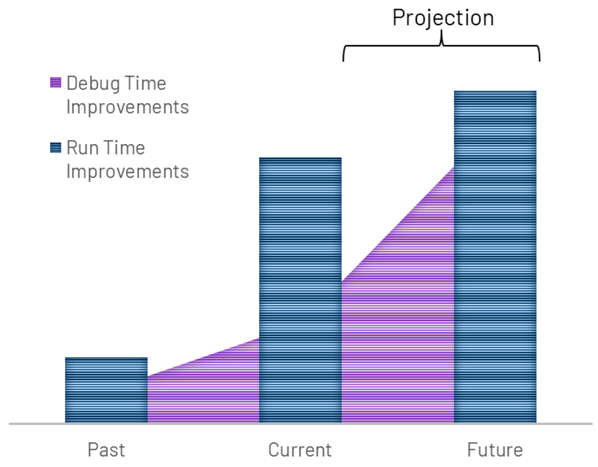
During each iteration of a fault campaign,

- 80% of the total time is spent in debugging the results and adjusting the setup to enhance the DC.
- Only 20% of the time is spent on actual fault simulation

Halving the debug time would result in substantial savings in time, energy, and resources for all FuSa teams, and expedite TTR and certification

Projection

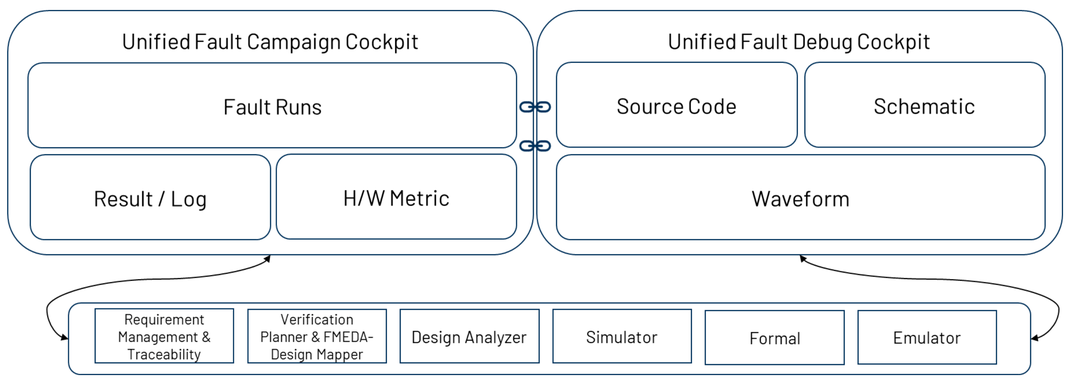
Comprehensive and FuSa aware debug solution is need of the hour and can significantly speed-up the fault-classification signoff



Mapping evolution of run-time improvements over that of debug-time

An Ideal Solution

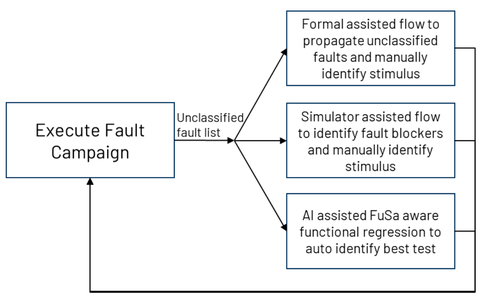
Authors vision of true unified FuSa verification, that focuses on the fault campaign execution and fault debug to improve the DV engineer's productivity and to achieve faster FMEDA verification closure.



Key goals:

1. Enhanced fault campaign execution
2. Integrated fault debug environment
3. Seamless traceability and planning
4. Platform-agnostic verification flow
5. Productivity and sign-off acceleration

Role of AI



Regression Mining

- Run full regression suite with barrier data and determine if any stimulus enables fault propagation
- If no existing test activates the barrier, fault can be marked as functionally safe

Fault Path Exploration

- Algorithms can identify active vicinity and predict easier route for fault propagation , even if the path spans multiple cycles or logic layers.

Conclusion

Leverage conventional TFMs to address systematic failures, while apply purpose-built solutions for random hardware failure analysis.

Fault debug and unclassified fault analysis challenges (major time consumers) could be addressed by common solution as described in this paper.

AI is here but hasn't penetrated this space and this paper proposes the use of AI to address a few of the problems in FuSa verification.

Acknowledgement

- Author would like to thank the members of Analog Devices Automotive BU and Engineering Enablement for their support and collaborative work.
- Author would also like to thank the Cadence and Synopsys FuSa team for their collaboration.

Contact:
Prashant Ravindra (Prashantkumar.Ravindra@analog.com)