TITLE OF PAPER	An Ideal FuSa Verification Solution!
AUTHOR 1	Name: Prashantkumar Ravindra Organization: Analog Devices Job Title: Staff Engineer, DV Email ID: Prashantkumar.ravindra@analog.com Mobile no:+91-8123868668

***Abstract*-Functional Safety is a challenging and an absolute requirement of the automotive and industrial SoCs and ASICs that need to show compliance to ISO26262 and IEC61508 respectively. It adds a new dimension to the world of pre-silicon design verification (DV) and hence requires purpose-built tools, flows and methods (TFM) to achieve the same. Conventional DV TFMs are nearly sufficient to show compliance with the systematic failure requirements, but the random hardware failure requirements demand newer EDA solutions. Through the learnings from real-life use cases of multiple ASIL-D / SIL3 SoCs and ASICs development, an ideal FuSa verification solution is proposed that leverages innovative FuSa aware debug and AI/ML technologies.**

I. Introduction

Functional Safety (FuSa) is defined as the absence of unreasonable risk due to hazards caused by malfunctioning of electrical/electronic systems. In other words, FuSa is about ensuring the safe operation of systems even when they go wrong. As shown in Figure 1 early detection of potential FuSa vulnerabilities is essential for the product success.

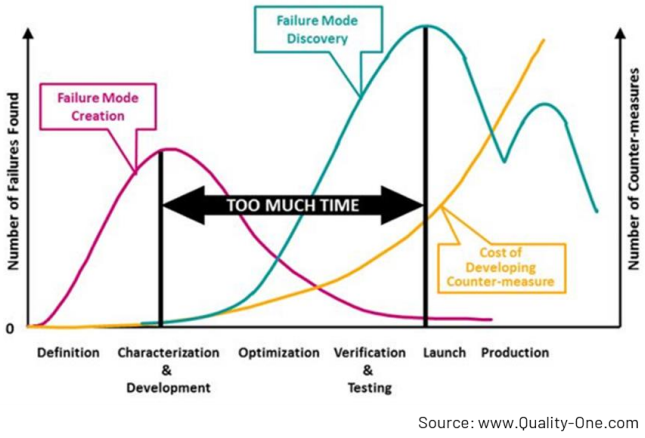

Figure 1. Approximation of time spent for every iteration of fault campaign.

Typically, there are two types of failures: Systematic and Random hardware failures. In ISO26262 systematic failure is defined as failure related in a deterministic way to a certain cause, that can only be eliminated by a change of the design or of the manufacturing process, operational procedures, documentation, or other relevant factors. Similarly random hardware failure is defined as failure that

can occur unpredictably during the lifetime of a hardware element and that follows a probability distribution.

Functional and Functional Safety Verification

FuSa Verification is a super-set of functional verification as it demands actions performed beyond the scope of functional verification. Figure 2 provides a more details of these requirements.

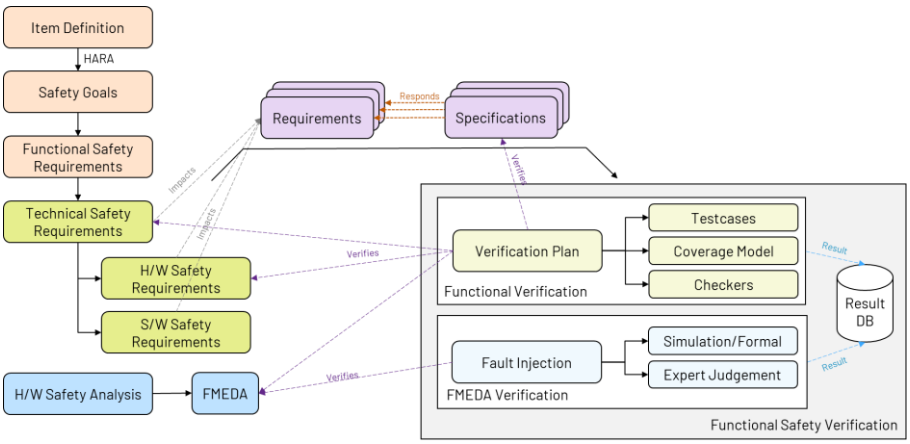

Figure 2. Approximation of time spent for every iteration of fault campaign.

In addition to the functional verification covering true and error scenarios, fault injection is introduced in the FuSa verification to validate the diagnostic numbers of the FMEDA. Conventional functional verification covers even covers the systematic failure verification and FI covers the random hardware failure verification.

Hence the conventional functional verification TFMs can be reused for FuSa verification with the additional tool confidence level analysis to ensure no systematic fault is introduced by the DV tools.

While the concept of FI has been there in the industry for a while, the scale and complexity are substantial for the FuSa SoC and ASICs. Hence purpose-built solutions are required.

II. Requirements

To ensure shorter Time-To-Revenue (TTR) and faster FuSa certification, there is a need to identify the best-in-class FuSa verification solution. In this section let us explore the various requirements to perform FuSa verification. Functional verification is subset of the FuSa verification and the TFM requirements are well understood by the DV community and hence will not be discussed here. Figure 3 lists various requirements and the expectations of the unified FuSa verification solution. These will be discussed in detail in the final paper.

The intention of the paper is not to promote one EDA vendor over the other but to rather acknowledge the best that already exists and suggest upgrades from the eyes of the SoC/ASIC creators.

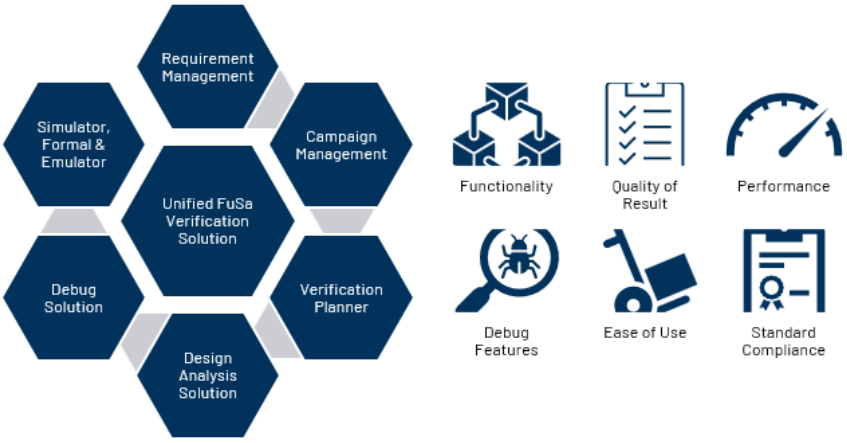

Figure 3. FuSa solution requirements and expectations.

Let us focus a bit further on a particular aspect of the FuSa verification which is an active area of EDA innovation: FMEDA verification with Fault Injection

FMEDA verification with Fault Injection

FMEDA is an analysis technique in the eyes of the Safety engineer, however from the DV engineer's perspective, in the document form, it's analogous to a verification plan. It defines the scope and the sign-off criteria.

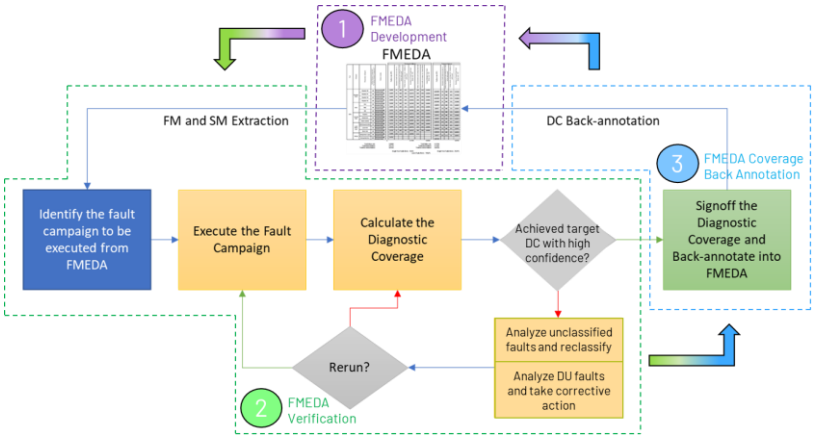

Figure 4. Approximation of time spent for every iteration of fault campaign.

While it may appear that a significant DV time is spent on fault campaigns, it's a thing of the past! As it stands today, owing to the fabulous work by the EDA engineers, concurrent fault simulator has addressed the run-time limitation and is being discussed further in the results section. Debugging the campaign for cause of unexpected fault classification, identifying tests that boost fault coverage, etc. take 80% of the time compared to 20% in fault simulations as shown in Figure 5.

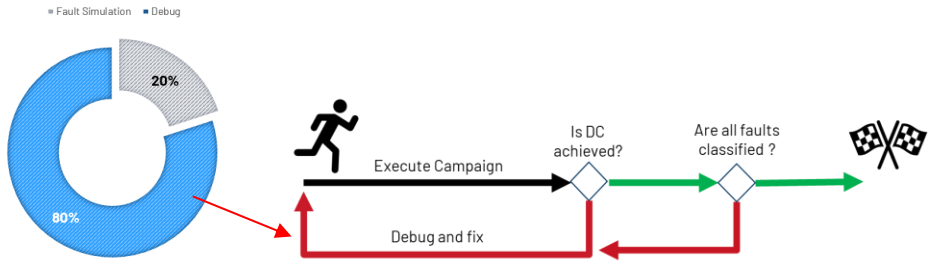

Figure 5. Approximation of time spent for every iteration of fault campaign.

III. Proposed (Ideal) Solutions

Looking beyond the raw-throughput of the fault simulator, there is an immediate need to have a feature rich true-unified FuSa verification solution. With learnings from working on multiple FuSa SoC/ASIC designs, Figure 6 is a depiction of the 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. More on each element in this figure and its interaction with each other will be discussed in the final paper.

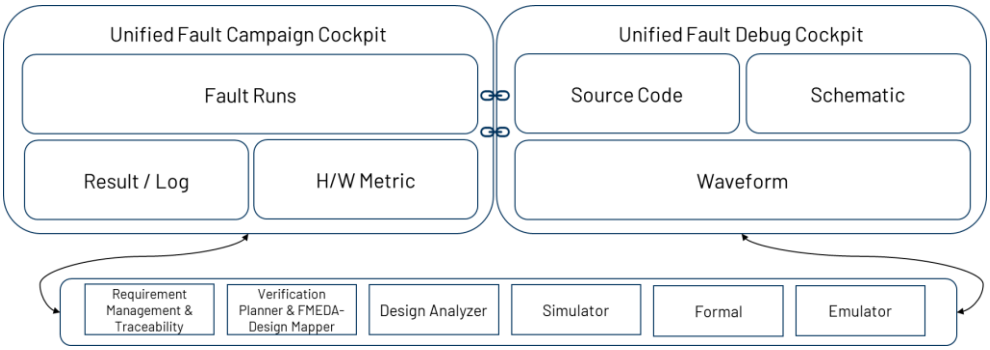

Figure 6. Feature rich unified FuSa verification solution.

Further to address the unsolved problem of unclassified faults, there is a need to look beyond the available solutions such as formal assisted propagation analysis and simulator assisted fault blocker analysis solution as both these involve manual work costing both time and resources.

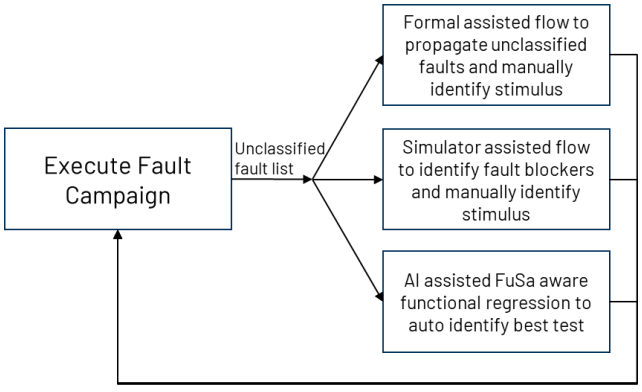

Figure 7.Solutions for unclassified fault analysis.

AI assisted FuSa aware functional regression potentially could be a practical answer to address unclassified faults. The final paper will include more lower-level details on the implementation of this solution but won't have the working prototype ready.

III. Results

Close collaboration with our EDA partners resulted in significantly reduction the fault-campaign runtimes from 1-week to 5h for an SoC developed for ASIL-D applications. As shown in Figure 8, in the first leg of this exercise, we migrated from serial fault simulator to concurrent fault simulator and did necessary modifications to the testbench (mostly on stimulus management) to get run-time down to 24h. In the second leg of this excise, the optimizations were done on the fault simulator by the EDA partner, based on the learnings from this exercise and others. We are currently at a state where we can finish this reference fault campaign of a failure mode with over 50k faults in GL netlist in 5h.

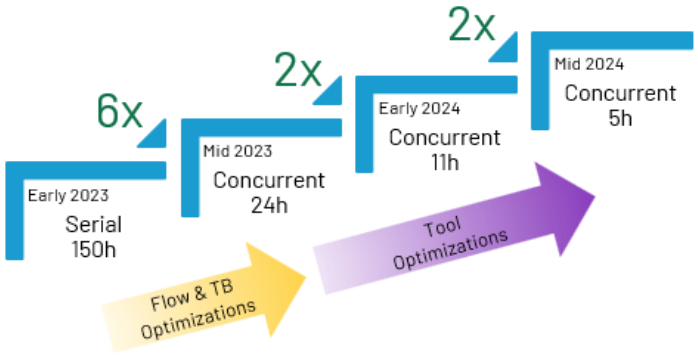

Figure 8. Evolution of fault simulator performance for a reference automotive SoC fault campaign

To minimize the significant time spent on fault-debug, there is a need to improve the debug solutions significantly. With proposed improvements (covered in previous section) in EDA solutions, major ramp is projected in debug-time improvement as shown in purple in Figure 9.

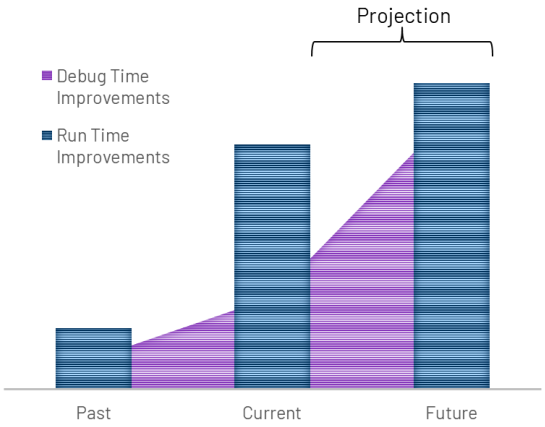

Figure 9. Mapping evolution of run-time improvements over that of debug-time

IV. Summary

Through the learnings from real-life use cases of multiple ASIL-D / SIL3 SoCs and ASICs development, an ideal FuSa verification solution is proposed in this paper. This paper advocates the reuse of conventional TFMs to address systematic failures, while stressing the need for 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 one of the many problems in FuSa verification. The aim is to cut-short the debug-time by over 50% to keep up with the growing complexity and scale of FuSa verification to enable rapid-development of products to-keep world safer than ever before.