The second wave in automotive ISO 26262 analysis

By Jamil Mazzawi and David Kelf

It has become well known that the analysis required for the Automotive ISO 26262 Functional Safety Standard involves lengthy and laborious fault analysis, performed using outdated fault simulation designed for manufacturing test quality grading.

As with many high value markets, advancement comes in waves. When meeting a new challenge, the initial response is to piece together a methodology using existing technologies. As the size of the market becomes established, new players will be attracted who will innovate different approaches, creating a second wave of tools. We are witnessing this evolution in the automotive space today, as next-generation fault analysis, formal verification, test suite synthesis and other approaches become apparent

What is fascinating about this evolution is that this second wave will also enable opportunities that were either out of reach or unimaginable, having a dramatic impact on design quality and functionality.

This article will both look at the improvements-on-offer to the automotive verification core methodology, as well as discuss potential new opportunities.

Fault simulation glass ceiling

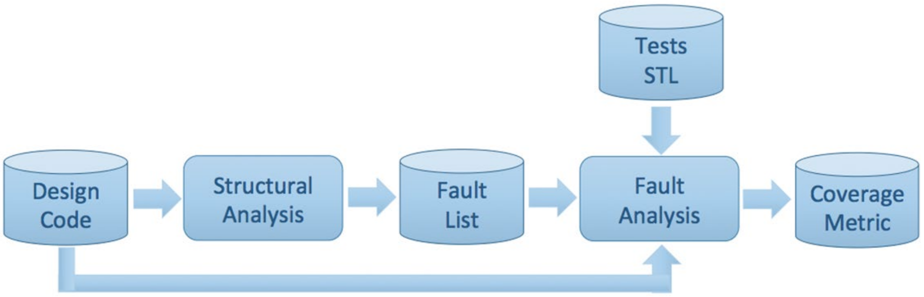
The ISO 26262 Automotive Functional Safety Standard defines specific risk tolerance levels required in electronic automotive devices. To achieve the maximum “ASIL-D” rating a very high degree of tolerance is required. This is specified in terms a general Failure-in-Time (FiT) metric of less than 10 failures in 1 billion hours of operation, as well as the “Single Point Fault Metric” greater than 99% and the “Latent Fault Metric” (LFM) to be greater than 90%.

To ensure that a device can meet these stringent goals, safety mechanisms are inserted that eliminate the vast majority of these random faults that occur naturally during device operation. The fault tolerance of the device must be tested prior to fabrication, to ensure these safety mechanisms are doing their job. In ISO 26262 nomenclature, this is known as the Failure Mode Effect and Diagnostic Analysis (FMEDA) process. Today, the only way to measure the required fault metrics is to use traditional Fault Simulation.

Fault simulation bottleneck

Fault simulation is a technique that was invented approximately three decades ago for the purpose of ensuring manufacturing test quality. The idea is simple. Firstly a simulation is run of a clean design using some test vectors derived specifically for this purpose, and the output recorded. A fault (either stuck-at-1 or stuck-at-0) would be inserted on a specific design node and the simulation run again. This would be repeated for every node in the design. If the output was unaffected by a fault, the tests may need improvement since the fault was not detected.

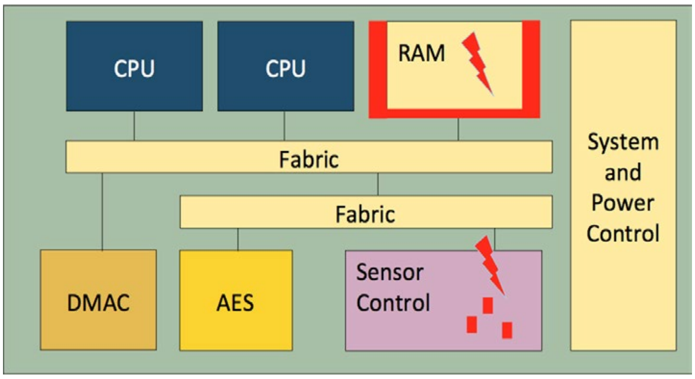
Of course the execution time of this process, which in its raw form would be equivalent to the number of faults * the size of the simulation, was enormous. Even after optimizations the simulation time would be measured in weeks or even months.



Fault simulation process.

Testing for automotive faults is not dissimilar to manufacturing test, in that faults must be injected and the device reaction to them measured. As such, it was inevitable that fault simulation would be the initial tool of choice for ISO 26262 characterization. However, there are important differences that made the older technology inappropriate.

For example manufacturing tests were scan-path based which meant that a test would only be required to execute from one flip-flop, through logic, to another flip-flop. On the other hand, safety tests have to trigger a fault and measure its impact through multiple clocked flip-flop stages before reaching a Safety Mechanism or an output, thereby making the testing process much longer and more temporal in nature. The type of faults to be measured cannot easily be approximated to a simple stuck at 1 or 0 as in the manufacturing world, which means the simulator has to work with new fault models, such as transient faults, bridging faults, etc.



Faults and safety mechanisms

Inevitably, automotive semiconductor companies will try to meet the ISO 26262 requirements with a minimum of fault simulation. Some companies will run simulations on small blocks and show how the measurements obtained could be translated up to the broader system level.

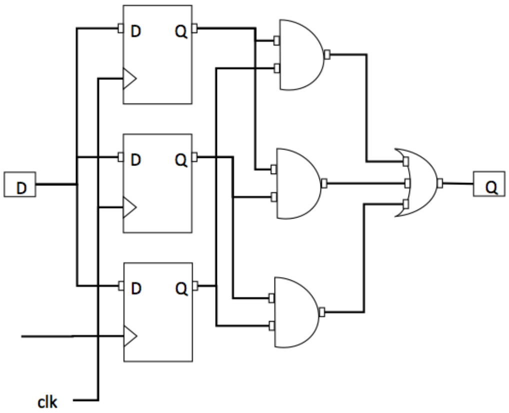
Others would perform statistical analysis on the results to show that the probability of a safe device is reasonable. Given the size and competitiveness of this market, it is inevitable that improved fault analysis methods would be introduced.

Jamil Mazzawi is CEO of Optima Design Automation - www.optima-da.com
David Kelf is Board Advisor, Marketing at Optima Design Automation.

Tool evolution

As automotive electronics have become more sophisticated and are used as a significant source of differentiation and value for the entire vehicle, the market for these devices has exploded. This has attracted specialized development efforts in the area of tooling that are needed to improve safety verification.

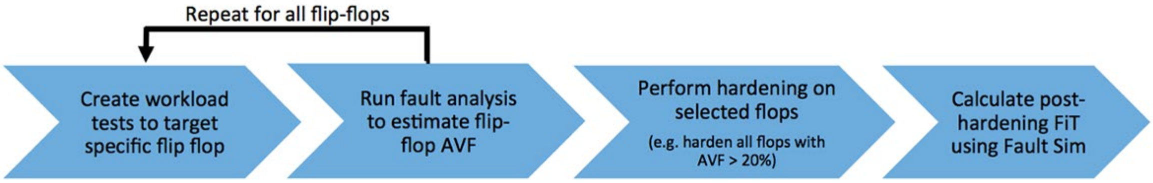
Examples of these new tools and methodologies include Test Suite Synthesis, Formal Verification and enhanced Fault Analysis. Test Suite Synthesis enables tests to be produced based on scenario specifications, increasing coverage dramatically. Formal Verification has been used to prune and optimize the fault lists that must be analyzed by the fault simulator to reduce the overall simulation burden. Both of these developments are very worthy and valuable.



Hardened flip-flop.

However, real advancement can only come from changing the fundamental tool in the overall flow, the fault simulator. New fault analysis techniques, such as the one from Optima Design Automation, are designed to replace the fault simulator with an engine optimized directly for automotive fault analysis that can offer order of magnitude acceleration over previous techniques.

New fault analysis solutions target the ISO 26262 automotive requirements, eliminating unnecessary processing legacies left over from manufacturing fault simulation. It has applied separate optimizations that make use of fault pruning and collapsing techniques as well as parallel processing opportunities. Finally it has leveraged formal verification and performance-simulation algorithms to produce an entirely new engine that can offer great performance improvement.


Repeat for all flip-flops
Create workload tests to target specific flip flop
Run fault analysis to estimate flip-flop AVF
Perform hardening on selected flops
(e.g. harden all flops with AVF > 20%)
Calculate post-hardening FiT using Fault Sim

Transient fault analysis process.

By accelerating the fault simulation process, the FMEDA metrics based on stuck-at-1/0 hard errors, may be calculated more quickly. In the case of Optima, this is an acceleration of an order of magnitude or more. In addition, the “fault list” (the faults that must be examined) may be optimized using a range of algorithms. Formal techniques allow this list to be pruned based on the impact of the fault condition, as well as more standard techniques such as fault collapsing, further accelerating execution.

This allows fault simulation for the existing FMEDA process to be accomplished in hours rather than weeks. Given this, it is possible to eliminate statistical approximations to system level fault tolerance, and instead perform exact measurements. It is also possible to try various options with different safety mechanisms and experiment to optimize the design itself for power consumption and performance, while still maintaining ASIL-D tolerance.

A major issue with the FMEDA process is tracking down and improving coverage issues. Closing fault coverage can be a laborious and time-consuming activity, which involves adjusting either the test vectors or the design itself. Improved fault analysis allows various coverage inspection techniques to be applied efficiently, driving for the automated improvement of coverage closure.

Safety analysis gets an upgrade

With traditional fault simulation only the most basic of fault conditions (stuck-at-1/0) may be analyzed. However, more complex faults can also cause disruption, and these should also be handled appropriately.

Transient faults, if occurring at the wrong time on the wrong signal, can be as catastrophic as a permanent fault. The ideal safety mechanism to trap such faults is hardened flips-flops, using an approach known as Triple Modular Redundancy (TMR). A single flip-flop is replaced by three flip-flops. The flip-flop outputs are compared and if one is different it is assumed faulty and the other two are used to provide the correct signal.

The problem with flip-flop hardening is that the size and power consumption of the flip-flops is dramatically increased. If it is not possible to accurately assess which flip-flops to harden, using selective hardening, a large number of them will be changed, significantly degrading the performance and power consumption of the entire device. In most designs some flip-flops will only be updated on a small percentage of clock cycles (e.g. control registers) or will not perform critical functions, whereas others perform key functions or are updated on every clock cycle (e.g. datapath registers).

To calculate the potential FiT rate of a design that might experience transient faults during operation, a workload set of tests must be designed that target a specific flip flop with a broad range of transient fault types.

This allows the Architectural Vulnerability Factor (AVF) of the flip flop to be very accurately estimated. Combining the AVFs of all the flips flops may be used to provide an assessment of the FiT rate. These algorithms require fault simulation to be run for every flip-flop with different workloads, and as such it has not been possible to perform this “selective hardening” process until now.

High-performance fault analysis, coupled with other techniques, allow enough iterations to be performed to complete this analysis, generating appropriate metrics and the ideal hardened flip-flop configuration. By enhancing the core verification methodology, many new safety checks can be performed, as well as other critical issues. Security analysis is also possible using some of these same techniques.

Summary

As we are witnessing a new generation of AI devices for automated driverless vehicles, and these powerful, complex semiconductors require a new design methodology. This is not just about maximizing safety, but is necessary to revolutionize the entire integrity of these designs. High performance fault analysis is at the heart of this new approach and will become the center of next-generation automotive design methodologies.