Solving the safety analysis problem

Accelerated automotive fault analysis can improve more than just time-to-market, as **Jamil Mazzawi** and **David Kelf** explain

In addition to the standard integrated circuit development process, automotive semiconductors must undergo the additional burden of proving that they operate safely. However, showing that these devices operate within an acceptable level of risk, as depicted by the ISO 26262 automotive functional safety standard, can add months onto their development schedules, a significant factor given today's highly competitive automotive market.

The reason for this lengthy process is each device must undergo an analysis to demonstrate that a fault inserted into a location that could cause a critical malfunction will, in fact, not alter the execution of the device. The problem is that to date the only solution able to perform this analysis revolves around the use of a traditional fault simulator.

This 30-year-old technology designed for evaluating manufacturing tests, a totally different application, is laboriously slow. Consequently, producing the necessary metrics to satisfy the ISO 26262 measurements requires months of tool execution, delaying device delivery. Worse still is the fact that the measurement produced is the bare minimum necessary to demonstrate safety.

The automotive semiconductor market is expected to grow to $50billion by 2022, according to market research from MarketsandMarkets and, as such, represents a huge opportunity for Electronic Design Automation companies looking to solve the safety analysis problem. This has attracted considerable investment in tools and methodologies, leasing to a new wave of development tooling. New fault analysis technology looks set to dramatically accelerate ISO 26262 analysis, shaving off those potential months of painful delivery delay.

The advent of new verification techniques, such as formal verification tools, accelerated parallel simulation algorithms, and fault optimisation technologies has been combined to create a new method to perform fault analysis. This new approach can accomplish the same analysis as traditional fault simulation orders-of-magnitude faster. Indeed, in recent benchmarks it has been shown that these tools can process a complex design more than 100X more quickly, all but eliminating the month(s) long fault analysis process.



Author details:
Jamil Mazzawi is CEO, Optima Design Automation

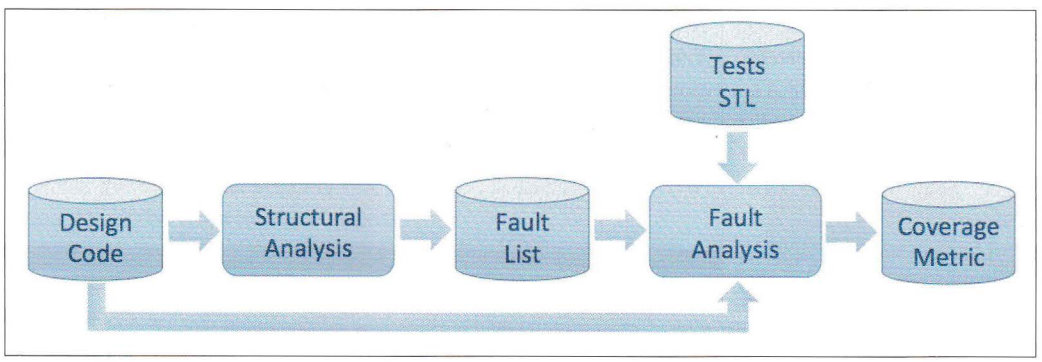


Figure 1: Traditional Fault Simulation Process

What is interesting is that the use of this new fault analysis technology has introduced new opportunities, which ensures a far greater degree of safety while also simplifying the entire development effort.

For example, traditional fault simulation relies on the fact that most fault types can be approximated, for the sake of the analysis, to a simple fault model where a signal is permanently either stuck-at-0 or stuck-at-1. This is fine for manufacturing tests, but does not describe the full story for automotive faults. For this we need to consider where these faults come from.

Environmental effects

In any semiconductor there is the possibility that environmental effects will change a bit value in a digital circuit. Electromagnetic radiation from the sun or heat from an engine has the potential to cause this problem. In most semiconductors this might require a device reboot at worst and as it happens so rarely this is not an issue. Of course automotive is different as a device failure could result in injury or worse.

A typical metric used to describe fault regularity is the Failure-in-Time, or FiT, rate, which is defined as one fault in one billion hours of operation. The highest risk tolerance level, known as ASIL-D, requires a FiT rate smaller than 10, or one fault in 100 million hours. This seems like a high number but when one considers the number of cars on the road that might use a specific device, the number does not seem so large. Radiation from the sun can produce a significantly larger number of faults than suggested by this metric.

The other issue is that a bit flip caused by radiation is often transient in nature, in that the fault appears briefly but the bit is then over-written through normal operation, eliminating the fault. These transient faults are not effectively modelled by the

standard stuck at 1/0 model, and as such may cause behaviour that would not be detected by traditional fault simulation. Even with a FiT rate of 10 or less, these faults have the capacity to send a car off a road.

A standard method to effectively eliminate transient faults requires replacing the flip-flops in a design with a more complex flip-flop component that more-than-triples its silicon area and power consumption, a process known as "flip-flop hardening." In devices where transient faults are an issue, design teams often take a "sledgehammer to crack a nut" approach and simply harden all the flip-flops in the design, dramatically increasing the power consumption in devices where power usage is a significant factor.

The analysis of transient faults across a system may be accomplished using an iterative fault analysis approach. This involves running the analysis many times. With traditional fault simulation techniques the cost of these runs is prohibitive. However, with the dramatic reduction in fault analysis time afforded by new tools, it is now possible to perform an analysis, which can lead to the replacement of just the flip-flops necessary to render the device safe.

Architectural vulnerability factor

To understand this approach, another metric, the Architectural Vulnerability Factor (or AVF) must be used. The AVF for a specific flip-flop is defined as the probability that a one cycle bit flip on that flip-flop will reach the output, and it is dependent on such factors as the probability of the bit having an unsafe influence, logical masking of the bit as it propagates through the system, etc. The overall FiT rate of the entire system may be approximated using the sum of the AVFs of the hardened flips-flops plus the AVFs of the regular flip-flops, calculated using fault analysis. By iteratively changing which flips flops are hardened, the optimum solution may be reached. Typically this will have a power consumption far less than the version where all flip-flops are hardened.

This is an example of the kind of analysis that may now be performed with this next-generation fault analysis. High-performance fault analysis may also be useful for related verification topics. For example, assessing coverage issues in a device can be very time consuming and problematic. Iterative fault analysis can be used to automatically track areas of the device for which test coverage is low, indicating a need to apply specific tests for this area or increase testing in general.

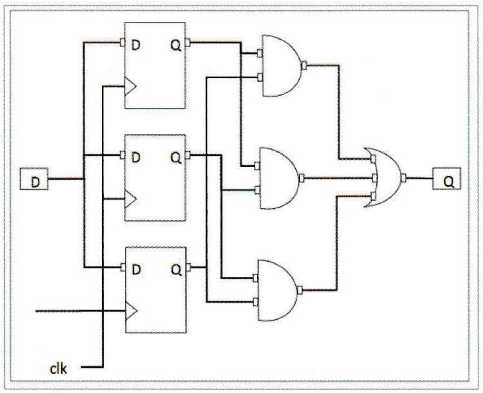


Figure 2: Hardened Flip-Flop

Using fault analysis, it is possible to insert faults and see if a testbench will pick up the change, thereby indicating if the area where the fault is inserted is effectively covered. Tradit5ional fault simulation is too flow, in general for this, but high-performance fault simulation can uncover untested items very quickly, leading to a more thorough verification process.

Fault analysis is at the root of most automotive safety verification processes, and the use of traditional fault simulation design for manufacturing test has led to overly slow safety metric evaluations. By improving fault analysis it is clear that this phase of automotive IC development becomes a lot faster, shaving months of device time-to-market. However, what is less clear is the additional functionality it provides, for example the ability to test for more complex fault models and perform automated coverage inspections. The use of high-performance fault analysis not only increases competitive time-to-market but also increases design quality and safety.



Author details:
David Kelf,
Board Advisor,
Marketing,
Optima Design
Automation