White Paper

The Transformational Acceleration of Automotive Safety Analysis

New Tools and Approaches for Achieving Comprehensive, Timely ISO 26262 Fault Analysis

Version: 191127
November 2019

Optima Confidential

Abstract
Current ISO 26262 fault analysis methodologies are hampered by outdated technology platforms, far too slow and onerous given today's tight project schedules. Three month plus certification processes have no place in modern automotive semiconductor projects under extreme time-to-market pressure. A next-generation suite of technologies and associated streamlined methodologies are becoming available and these promise transformational change to automotive electronic projects. These are arriving just in time given the electronic processing requirements for emerging driverless vehicles.

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement no. 850104

Optima Design Automation Inc.
www.optima-da.com

Copyright Optima Design Automation, Inc. ©2019 All Rights Reserved

Introduction

The ISO 26262 safety standard has defined risk tolerance measurement and management processes for automotive electronic systems and semiconductors. Following this standard has proven difficult and time consuming where existing tools and methodologies are leveraged, particularly given the extreme time-to-market constraints of this industry. Indeed, the length of time it takes to perform fault analysis has lead many companies to circumnavigate the process altogether, providing less reliable statistical measures of risk tolerance.

New approaches are needed, based on fundamental technology transformations to dramatically shrink analysis time while increasing capability. This paper describes one such transformation in fault simulation that enables new techniques for both Hard and Soft Error analysis with significant improvements.

ISO 26262 Safety Analysis Requirements Recap

In [1] we describe the ISO 26262 safety analysis requirements and processes. The requirements must consider both Systematic and Random Failures. Systematic failures result from errors introduced during development, manufacturing or another part of the production process, and are controlled by improving that process is a rigorous fashion to ensure no issues make it through into the final product. Random failures are errors that occur naturally while the device is operating, and these are controlled by understanding the impact of faults that can occur during operation, and controlling dangerous faults using Safety Mechanisms that correct errors on–the-fly.

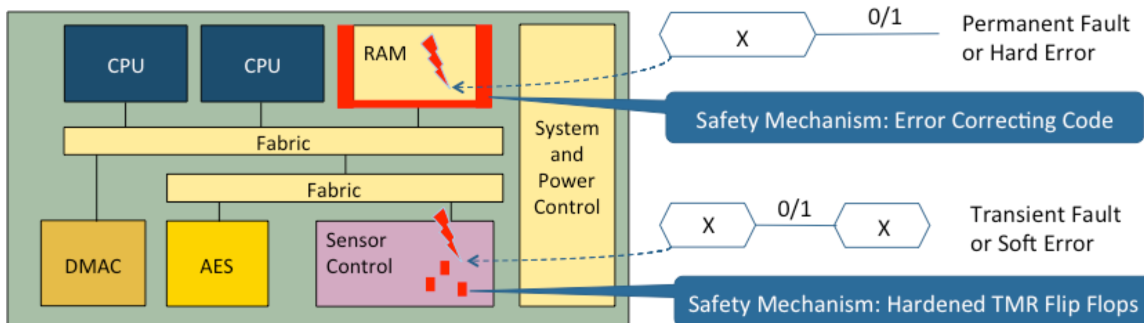

Figure 1: Permanent and Transient Faults in an Electronic Semiconductor

The Automotive Safety Integrity Level (ASIL), a risk reduction category required given the type of device, is calculated using analytical methods to inspect critical metrics. This applies to two fault types: Hard Errors or Permanent Faults, and Soft Errors or Transient Faults, see Figure 1. It uses a process called Failure Mode Effect and Diagnostic Analysis (FMEDA), and it is this subject on which the rest of this paper is focused.

Current Technical Approaches

Today the predominant method to perform quantitative FMEDA is fault simulation. Fault simulation is a technique invented for the qualification of manufacturing tests and has been used for more than thirty years for this purpose.

Manufacturing test fault simulation was applied primarily at the gate level and made assumptions that these tests would be provided mostly through a scan path, or Built-In-Self-Test (BIST). As such, the logic sections in the design could be broken up and the technique applied with some parallelism across the design. It was assumed that any type of fault could be represented as a stuck-at-1 or stuck-at-0 fault type, which produced a reasonable approximation for manufacturing yield purposes. Furthermore, various optimizations could be applied, such as specific fault collapsing and pruning, to reduce the fault list further. Even with all these shortcuts, fault simulation was a lengthy and painful process.

The primary reason for this was that fault simulators were often architected on top of regular gate level software simulators, and some of the classic gate optimizations used for regular logic simulation could not be applied, as they masked some part of the fault simulation process. Even with applied parallelism, fault list optimization, and other acceleration techniques, the fundamental equation of simulation performance depicted by the function f(#gates * #faults) was onerous. On the fastest of machines, fault analysis often required weeks of simulation and did not scale with increasing design size.

For ISO 26262 FMEDA even more restrictions exist that make the use of classic fault simulation even harder. A greater number of fault types have to be considered, and these cannot always be approximated to stuck-at-1/0 faults. The test stimulus that must be applied has to represent realistic operational scenarios and cannot simply be derived manufacturing tests passed through a scan path. For fault effect observation, it is not enough to check the scan path output to see if a fault was detected. In this case the actions of the Safety Mechanisms must be observed with the resulting fault elimination and alarm signals, where appropriate.

Fault simulation has been augmented with other techniques to improve this situation. Formal verification solutions have been employed to prune the fault list further and aid with the debug of more complex faults. Safety Mechanism synthesis techniques that include fault grading have also helped. However, all of these solutions still rely fundamentally on fault simulation and until this technology is improved, they will all suffer from the same issues.

New Fault Injection Engine Technology

Although other technologies have been employed in these design flows, fault simulation still remains the mainstay approach to all the automotive analysis

functions. However, the performance of traditional fault simulators makes exhaustive analysis prohibitive.

A new breed of fault simulation technology has been developed that is specially designed for automotive analysis. By eliminating the overhead often contained in these simulators for the purpose of generic simulation, as well as manufacturing test simulation, it has been possible to derive an entirely new algorithm that makes use of formal and similar techniques to produce a fault simulation style execution engine without unnecessary overhead.

Number of flip-flops examined in design	Well known simulator results		Optima FIE results		Acceleration Factor
	Single Fault Injection Simulation	Total "Safety" Campaign Extrapolation	Single Fault Injection Simulation	Total "Safety" Campaign Extrapolation	
24,000	56 sec	7.95 years	0.019 sec	1.02 days	**2,000 X**
48,000	478 sec	136 years	0.020 sec	2.15 days	**23,000 X**
96,000	25 min	851 years	0.027 sec	5.60 days	**55,000 X**

Figure 2: Actual Benchmark Results for FIE on a Commercial Automotive Design

Optima-DA has pioneered this new style Fault Injection Engine (FIE™) technology, which has already exhibited significant performance improvements, typically greater than 1000X, over previous methods, see Figure 2. Although the actual algorithm is proprietary, the results speak for themselves. The company has used this to create a series of solutions, or Apps, for common FMEDA analysis functions.

Structural Analysis Methods

Before performing fault analysis on a design it is important that the design is inspected and the various fault types that require analysis identified. This phase can be performed manually but is dramatically improved using automated techniques. In [1] various fault types were identified as follows:

- Safe Faults: Are located in part of the logic not relevant for the safety of the device, or they do not impact the safety of the device.
- Single Point Faults: These faults impact the safety of the device and are not handled by a safety mechanism. As such, these are dangerous faults.

- Residual Faults: Occurs in an area buffered from a safety mechanism, but cannot be handled by the safety mechanism. These lie outside the risk calculation.
- Multipoint Faults: These faults are handled by the safety mechanism.

Multipoint Faults are sub-classified into:
- Detected: Detected and corrected by the safety mechanism
- Latent: Corrected by the safety mechanism, but with no indication they existed
- Perceived: Not detected and have some affect on the driving experience (Note: this last category rarely applies to digital ICs)

These fault types require identification, and this may be performed by analyzing the Cone of Influence (COI) that emanates from the input to a Safety Mechanism (SM) or other key point in the design. The COI is the logic that drives the SM.

Note the design section example shown in Figure 3. This shows a typical Safety Mechanism in use, a Lock Step capability where the Master logic is mirrored using an identical Shadow logic block, and the outputs compared. The unit outputs represent the regular output of the design block, and the detection output represents signals that will be activated if a mismatch is detected between the blocks.

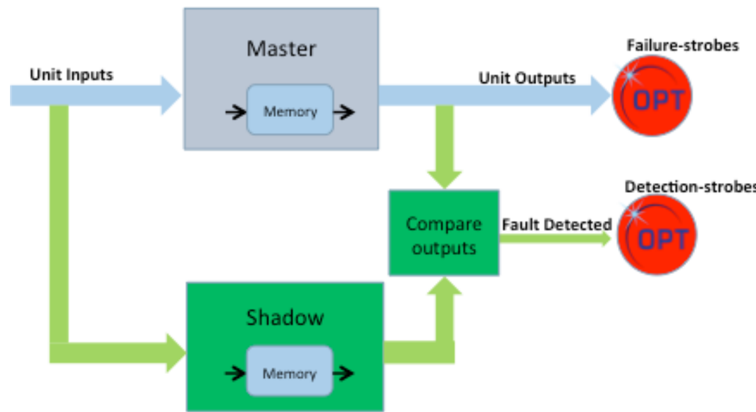

Figure 3: Lock Step Safety Mechanism Example

The outputs from this design block are both driven by separate, but overlapping, Cones of Influence logic. Figure 4 shows a diagrammatic representation of those COIs. The first COI represents the input to the Unit (or Critical) Output and the second to the Detection Output. Both of these outputs are strobed on every clock cycle to determine an output mismatch.

Any fault in the Detection COI only may be considered safe, as it has no influence on the output unless it is also contained in the Critical Output COI. Any fault that is in the Unit Output COI and is not in the Overlapping Detection COI are clearly unsafe and invisible to the Safety Mechanism.

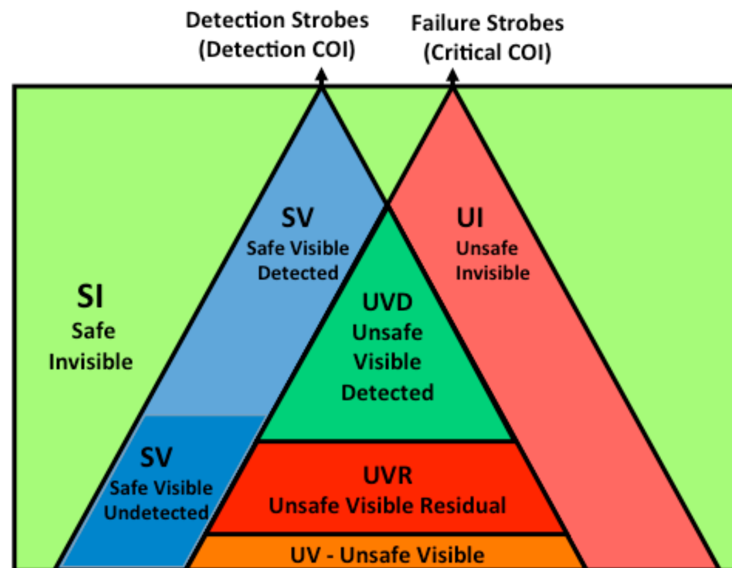

Figure 4: Fault Types Contained in COI Logic

Now, where the COIs overlap, it is clear that a fault will be visible to the Safety Mechanism, and some of these may be safe faults (will not cause an issue) whereas others will be unsafe. Some of these will also be residual or latent, where they are not directly unsafe, but influence another fault to make that fault unsafe. Ideally the COIs would exactly overlap, but typically there is always some logic that is not contained in the overlapping COI.

The FMEDA process, be it manual or automated, must first perform this fault categorization. Automating this process allows for a fault list to be reliably and quickly produced, and the fault list loaded into a management mechanism whereby the analysis results across many COIs and design sections may be compared and categorized together.

At this point in the process, some faults may be optimized away. Fault Collapsing is a well-known technique where a specific fault may also drive a related fault. For example, take a faulty invertor. If the input of the invertor exhibits a stuck-at-0 fault, this will appear as a stuck-at-1 fault on the output. As such, both faults may be represented by the fault condition on the output of the invertor, and only the output needs to be analyzed. The input signal stuck-at-0 and stuck-at-1 may be "pruned" from the fault list. This technique can be used for other logic, for example a stuck-at-0 on the input of an AND gate means that the output will also be stuck-at-0. However, a stuck-at-1 on the input cannot be represented on the output of the AND gate, which may still fluctuate based on the other input.

Hard Error Fault Analysis

Once the Fault List is established, it is possible to perform an analysis to understand the fault coverage of the Safety Mechanisms and produce a list of Single Point Faults,

which are considered dangerous. The impact of these Single Point Faults on the design must be understood to decide if they can be tolerated without too much impact to the ASIL categorization, or if further remedial action needs to be taken. The typical Hard Error Analysis process is shown in Figure 5.

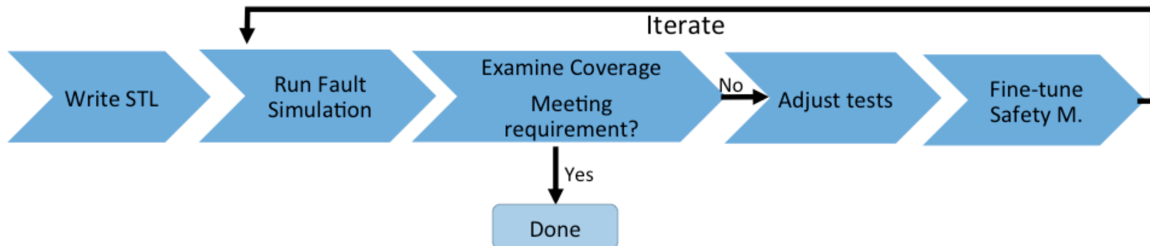

Figure 5: Hard Error Analysis Process

First an effective Software Test Library (STL), i.e. simulation stimulus, must be written that, when executed in the simulator, will provide a high level of fault coverage. For many large blocks this is a non-trivial exercise, and several iterations on the test set will be required to improve coverage to a tolerable level for the ASIL categorization (>99% for ASIL-D).

Once a base STL has been created, Fault Simulation is executed using the fault list from the Structural Analysis phase of the process and a report is generated to demonstrate areas of the design that have been covered, which faults have been exercised, and dangerous Single Point Faults that remain. As previously noted, Fault Simulation performance is a key bottleneck in this process.

Based on the report, the STL may be adjusted to increase simulation coverage, the fault list may be re-inspected to ensure all faults are correctly analyzed, and the design itself may be updated such that more faults may be handled by the SMs.

Understanding how to improve coverage efficiently is both time-consuming and error prone. Automated methods to examine the design and highlight areas where coverage may be improved are also becoming available, and this coverage boosting technology can save fault simulation iterations and a significant level of manual effort.

The Optima CoverageMaximizer™ Approach uses several factors to indicate areas where coverage may be increased and the accompanying tests.

Soft Error Iterative Hardening Analysis

Soft Errors refer to Transient or Intermittent Faults, and in critical locations these are eliminated using special "hardened" flips flops, an example of which is shown in Figure 6.

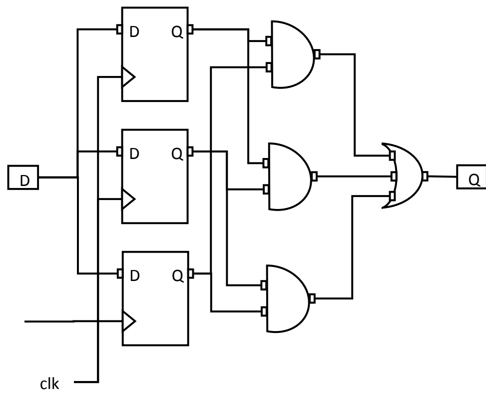

Figure 6: Hardened TMR Flip-flop

This TMR flip-flop design removes transient faults by comparing the two flip-flop states of a master slave flip-flop pair. The instability reducing Master Slave flip-flop pairs operate from inverted clocks such that they latch the input signal and eliminate instability at different times. The output is then run through a simple comparator and further instability eliminator.

This arrangement will eliminate many transient fault types but it requires a lot more silicon area and power consumption, a hot commodity for these automotive designs. If all the flip-flops in a design are "hardened" by replacing them with these special flip-flops, the power consumption increase is generally prohibitive.

However, it can be observed that the state of many flip-flops in a typical design is rarely changed (e.g. a control register) and other flip-flops may often change to the same state. As such, a transient fault in many flip-flops is unlikely to have a significant effect. It is possible to run analysis, using fault simulation, to understand a minimal set of flip-flops that do need to be hardened to provide a specific level of coverage against Soft Errors.

Two metrics are important for this analysis:

- The AVF (Architectural Vulnerability Factor) for each flip-flop
  The AVF is a measure of how vulnerable certain parts or the whole design is to various faults. For an individual flip-flop the AVF is defined as the probability that when a bit flip happens on the flip-flop, that the error will propagate and reach a safety-goal output. This is dependent on such factors as the logical masking of the flip-flop, the likelihood of its change having an overall impact, etc., and may be measured using fault simulation.

- The FiT (Failure in Time) Rate
  The FiT Rate is defined as 1 fault in 1 billion hours of operation * the specified rate. For example a design with a FiT of 1000 would be 1 fault in one million hours of operation. It may be shown that the FiT rate of all the flip-flops in a design are equivalent to:

  $$\sum k = (AVF(k) * fit_hard) + \sum i = (AVF(i) * fit_unhard)$$

  where k and i are the hardened and unhardened flip-flops and fit_hard and fit_unhard are the FiT rates of a hardened and regular individual flip-flop.

The Selective Hardening Process operates as shown in Figure 7. The FiT rate of the design block is measured using fault simulation, together with the Fault List and representative tests. Depending on the outcome, it is decided if hardening is

required. Selected flips-flops with a high individual AVF are hardened and the fault simulator is rerun to calculate the resulting new device FiT rate. By iteratively selecting different flip-flop sets, as hardening one flip-flop will effect the transient faults applied to surrounding flip-flops, a minimal set of flip-flops requiring hardening may be derived.

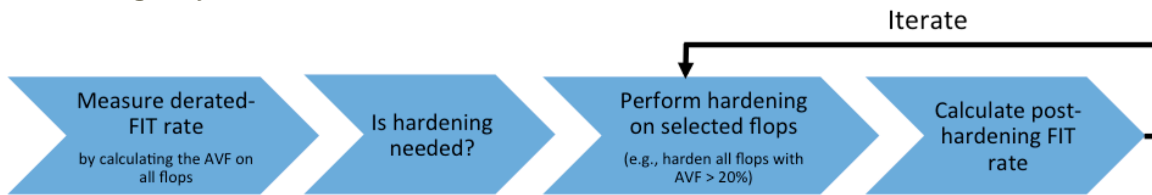

Figure 7: The Selective Hardening Iterative Process

This process requires a significant amount of Fault Simulation, and is clearly hard to execute unless the simulation process is extremely fast. Only now has it been possible to automate this process to arrive at optimal FiT ratings versus power consumption, improving overall design performance dramatically.

Optima Next Generation FMEDA

The Hard and Soft Error Analysis, as well as the Structural Analysis, processes described above are encompassed by new technology produced by Optima Design Automation. Optima-DA has produced a next generation Fault Injection Engine (FIE) that executed orders of magnitude faster than traditional fault simulation. This has been used as a platform for "Apps" that provide the automated capability described in the previous sections, see Figure 8.

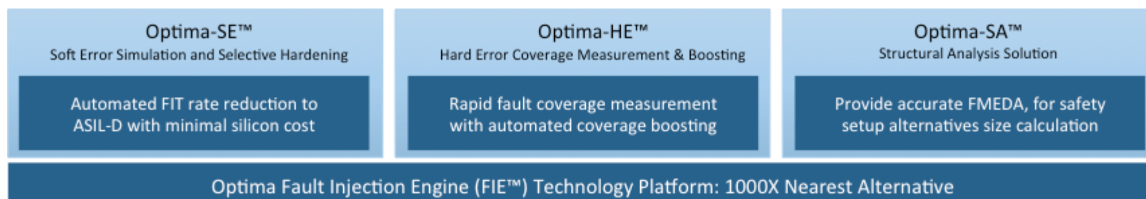

Figure 8: Optima Design Automation Product Line

Optima's next generation product line is already in use at leading automotive semiconductor companies.

Summary

As required by the ISO 26262 standard, fault analysis is critical to ensure the safety of automotive semiconductors is within tolerable ranges based on their purpose. Performing this fault analysis has proven difficult using traditional EDA tools and methods, namely fault simulation. However, a next generation Fault Injection Engine (FIE) technology is set to change this dynamic, accelerating the fault analysis process from weeks to hours, thereby enabling advanced solutions for critical problems. Optima Design Automation is delivering a suite of solutions that are accelerating real design flows at automotive semiconductor leaders. Hard Error and

Soft Error analysis is now possible in a reasonable amount of time, allowing for exhaustive ASIL analysis rather than statistical guesses while meeting stringent time-to-market constraints.

References

[1] An ISO 26262 Automotive Safety Standard Primer, Optima Design Automation, August 2019. www.Optima-DA.com