cadence®

Meeting Functional Safety Requirements Efficiently Via Electronic Design Tools and Techniques

By Philippe Roche, STMicroelectronics, and Adam Sherer, Cadence Design Systems

In an intelligent electronic system, unexpected errors can lead to unplanned, unexpected behavior. This can be a potentially dangerous proposition for, say, an automotive manufacturer, as well as a costly occurrence for consumer product developers. Compliance to the latest safety standards can be a laborious, time-consuming process. Fortunately, there are now technologies available that can automate the process of meeting functional safety requirements. This paper examines these functional safety solutions, showing how these technologies and tools can help engineers efficiently and effectively create safe, reliable products.

Contents

Introduction

Intelligent electronics are everywhere these days, from smartphones to cars, airplanes, trains, power plants, pacemakers, and even refrigerators. This intelligence fuels powerful products with simple interfaces built on top of sophisticated electronics. However, as design complexity grows, the risk that unexpected errors will lead to unplanned, unexpected behavior grows. While the risk of personal injury for errors in, say, automotive designs may be obvious, we also cannot overlook the risk of financial loss associated with a fickle consumer who throws away the smart watch that freezes every time an alpha particle hits it during a sunny summer run.

Compliance to safety standards takes considerable effort, from staying up-to-date on the latest standards to managing data in spreadsheets and documents and refactoring the verification environment to fit the traditional tool flow. While forgoing safety is clearly not an option, there are technologies available now that automate the process of meeting functional safety requirements, making the process more efficient than before. Efficiency is, after all, more desirable than ever in this environment of increasing system complexity.

This paper will discuss design and verification tools that can provide the assurance that systems on chip (SoCs) are functionally safe at the IC and system levels. While functional safety is pertinent to an array of application areas, we will focus our discussion on the automotive space. Automotive applications, guided by a clear set of standards, provide a good illustration of the concerns and requirements around functional safety.

Why is Functional Safety Important?

Functional safety refers to the concept that an overall system will remain dependable and function as intended even in the event of an unplanned or unexpected occurrence. Moreover, the system is assured to avoid unacceptable risk of physical injury or damage.

For SoCs, especially as we move deeper into the submicrons, susceptibility to errors becomes greater. For example, phenomena that we cannot really see—from radiation sources to large magnetic fields and internal wear (common cause failure) —can be highly disruptive to advanced node SoCs. Imagine the repercussions if the most significant bit flips (single event upset) in a chip that controls the transmission of the car you're driving down the highway, causing your vehicle to drop into a different gear.

It's not just lives at risk—it could be as simple as a company's brand image if their device constantly reboots. On a more positive note, having a higher degree of safety can differentiate your product, as well as consumers' perceptions of it. As basic design requirements go, dependable design is becoming as critical a criterion as meeting power, performance, and area (PPA) specifications.

What Does Functional Safety Require?

The design of safety systems involves the following:

- Redundancy, which provides multiple processing paths to limit the risk that any one error will upset the system; the tradeoff here is that redundant systems do consume IC area that could otherwise be used for additional functionality
- Checkers, which monitor the systems and trigger error response and recovery features when necessary; the tradeoff here is that while checkers don't consume too much area, they may provide only partial recovery

Safety engineers must implement requirements tracing from the system to components, and ensure their development flow aligns with tool confidence level (TCL). Quality measurement involves functional verification at all levels of abstraction and for all system elements, as well as safety verification, which measures response of systems to undesired/unplanned events. Finally, it is important to record and report functional safety measures in order to have a verified system.

From a process standpoint, to achieve safety verification, safety engineers need to be able to take their functional verification environment and essentially replay pieces of it while injecting errors (faults) into their system. Redundant logic can "vote" on the correct data to eliminate errors, maintaining continuous operation. Checkers monitor for erroneous data within specified time periods and apply error corrections. As an example, consider the pressure sensors in the power windows of cars. When operating correctly, pressure sensors prevent power windows from, for example, closing on the fingers of a curious child who's playing with the window's up/down switch. Imagine what might be missed if the checker on these sensors samples only every five seconds vs. every quarter of a second.

Key Safety Standards: IEC 61508 and ISO 26262

The foundation functional safety standard is IEC 61508, which addresses the assessment and reduction of the risk that unexpected errors will lead to unplanned behavior. It defines assessment methods for requirements tracing, functional safety, and TCL, culminating in an audited safety integrity level (SIL, ASIL for automotive). A variety of industrial standards are derived from IEC 61508, including the automotive safety standard, ISO 26262.

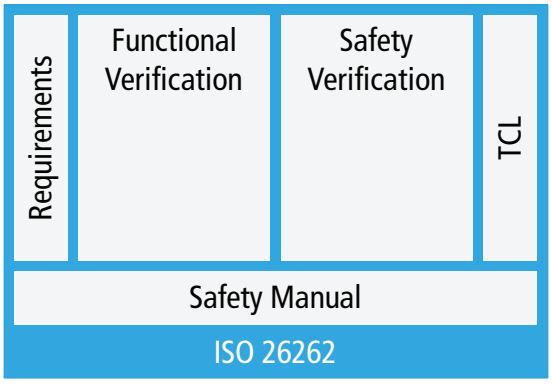

Figure 1: Elements of ISO 26262 from a verification perspective

All of these standards have one thing in common – the massive amount of data collection and analysis needed to achieve the safety integrity level. Massive can mean tens of person-years in the development cycle for a product line, translating into millions of dollars in added development expense. With an increasing number of OEMs and tier 1 integrators requiring an audited ASIL certificate, the challenge is to find immediate solutions that can evolve as your product grows in complexity.

Safety Needs to Address Now

Requirements tracing, functional safety assessment, and TCL for digital designs are the core requirements that have to be met today. The design and test teams start by identifying potential safety issues, along with the checking and error correction systems that can detect those faults. Those requirements are captured in a safety plan that augments the functional verification plan. These metric-driven verification plans monitor sets of metadata through both the functional and safety verification flows. For the functional flow, the metadata includes well-known coverage, test completion, and other metrics using conventional verification flows. While the functional safety flow adds a new technology for fault injection and detection, it needs to integrate seamlessly with the conventional flows for two critical reasons – efficiency and tool confidence. Safety verification is a complex task so the teams need to reuse the environments already created in the conventional flow. Along these lines, achieving a TCL1 for the flow is dependent on both a well-known flow and redundant tooling. By fitting the fault injection and requirements tracing within the conventional flow, a TCL1 assessment for the flow is justified.

As simulation provides a means for functional verification of systems, fault injection allows for functional safety assessment by simulating the behavior of the system under various error conditions by momentarily or permanently changing the values seen in a given simulation. Faults models include manufacturing-time stuck-at-0 and stuck-at-1 faults, as well as single event upset faults and transient faults that can occur while the ICs are functioning in the system. Given this, fault simulation helps safety verification engineers cover a wide range of possible system malfunctions.

While the TCL assessment is important, the efficiency of fitting in the conventional functional verification flow is equally important. Part of the safety assessment requires fault analysis at the gate level, which can be achieved with a fault injection using a well-proven gate-level simulator. However, the temporal faults can require longer simulations with more of the SoC context. This context can include both analog circuits and software, implying the need for mixed-signal and hardware-based verification. Moreover, the gate-level simulation can be exceedingly long, so safety engineers need to develop the safety verification at higher levels of abstraction, develop the RTL for the immediate need, and then replay the verification at the gate level as needed for, say, a ISO 26262 audit in the automotive space. Therefore, the fault injection technology and requirements tracing must work well with conventional verification flows.

Safety Requirements on the Horizon

While digital functional safety simulation is the critical starting point, it is not sufficient to demonstrate safety only in the complex SoCs being deployed in vehicles. The systems throughout the vehicle, especially powertrain, safety (i.e. braking), and chassis systems that require Automotive Safety Integrity Level D (ASIL D) certification, involve digital, analog, design for test (DFT), AUTOSAR-based software components, and design and verification IP.

Functional safety solutions must expand to have analog/mixed-signal verification that matches that for digital, including requirements tracing, fault injection, and metrics collection. Doing so will allow both internally developed and commercially accessed design IP and verification IP to be assessed in the complete system. As these systems become increasingly large and dependent on software, hardware-based verification systems will be needed to run enough cycles to inject faults in the running system and measure the combined digital, analog, and software system response.

Long Term View of Safety

In the full view, the safety of the vehicle depends on more than the individual ICs. It depends on the interaction of those ICs in the electronic control unit (ECU). This implies that level analysis is needed to develop fault models for board-level signal and power integrity on the traces between the ICs. It also implies that safety monitoring needs to be designed at higher levels of abstraction, suggesting the need for fault analysis in the earliest phase of design where the modeling is abstracted using algorithmic and untimed design models. These systems then need to be traced through implementation and final verification, completing the system view of functional safety.

Tools and Technologies that Address Functional Safety

Cadence has been in the fault simulation business for more than 25 years. It is now expanding to provide an end-to-end functional safety solution, based on its proven Incisive® functional verification platform, that reduces the automotive ISO 26262 certification effort by 50%. The solution accomplishes this efficiency gain by automating what is otherwise a time-consuming manual verification process of fault injection and result analysis for IP, SoC, and system designs. For safety requirements tracing, the solution integrates permanent and transient fault simulation.

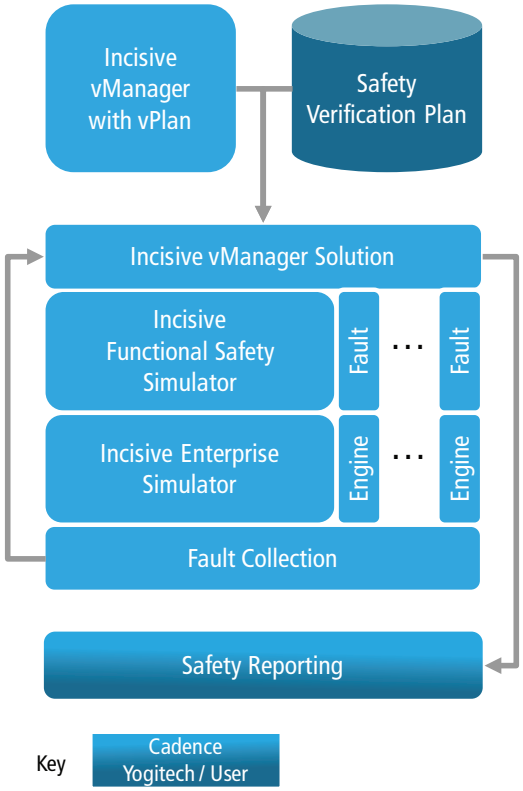

Figure 2: A functional safety verification flow

Fulfilling the traceability, safety verification, and TCL requirements of ISO 26262, Cadence's functional safety solution includes the Incisive Functional Safety Simulator and a functional safety regression capability in the Incisive vManager™ solution.

Incisive Functional Safety Simulator offers seamless reuse of functional and mixed-signal verification environments to accelerate the time to develop safety verification. The simulator provides 10X the runtime performance compared to the interpreted Incisive Verifault-XL engine traditionally used in functional safety simulation. With the simulator, users benefit from fault identification during elaboration and the ability to reuse their SystemVerilog, Universal Verification Methodology (UVM), and ***e*** functional verification environments unchanged. The solution simulates the unaltered design under test (DUT); faults are injected during simulation and can propagate through SystemC, analog transistor or behavioral models, and assertions. The simulator also supports multiple fault types, including single event upset, stuck-at-0/stuck-at-1, and single event transient.

The functional safety analysis capability in the Incisive vManager solution automatically generates a safety verification regression from the fault dictionary created by the simulator. The Incisive vManager solution can then track millions of detected, potentially detected, and undetected faults introduced into simulation to verify the safety systems in a design. The capability also highlights potential and undetected fault runs for further debugging.

Both of these technologies will be available in the Cadence® System Development Suite. Incisive vManager solution has already been used in production by several US and European automotive IC suppliers. In fact, the first ISO 26262-certified chip used the Cadence solution with a requirements management tool. Cadence is continuing to expand its functional safety solution to encompass more hardware, software, and IP components.

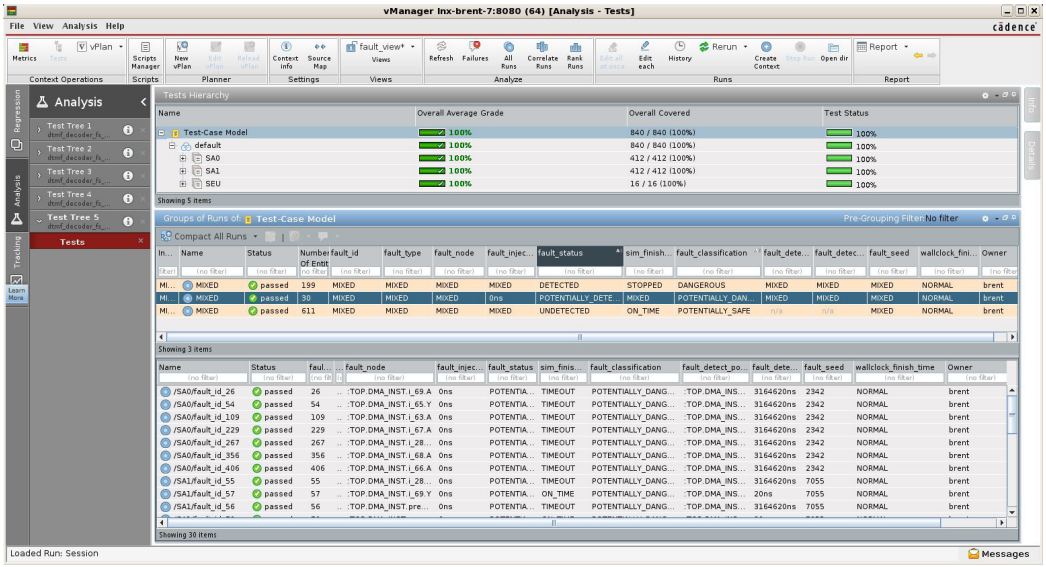

Figure 3: Leveraging metric-driven verification to provide a comprehensive functional safety regression analysis

Summary

As discussed in this paper, meeting functional safety in automotive designs is only the beginning. Safety requirements touch a multitude of application areas, from medical devices to industrial equipment to military systems and much more. Complying with safety specifications can be laborious and time-consuming. However, electronic design tools, technologies, and methodologies—such as those offered by Cadence—can automate the process. By doing so, these tools and techniques can make it faster and more efficient for SoC designers to ensure that their chips will function as intended once inside the end products, even in the face of errors or other unplanned or unexpected circumstances.

References

1. P. Roche, G.Gasiot, "SEE on advanced CMOS BULK, FinFET and UTTB SOI technologies", short course, Nuclear Space Radiation Effects Conferences, NSREC/RADECS conferences, Paris, July 2014

2. P.Roche, "Changing the radiation paradigm with sub-28nm CMOS technologies", tutorial, International Reliability Physics Symposium, IRPS, Hawaii, April 2014

3. P. Roche, "Technology Downscaling Worsening Radiation Effects", Invited talk, SEMATECH Reliability Council, Dresden, Germany, July 2013

4. P. Roche, J.L. Autran, G. Gasiot, D. Munteanu, "Technology Downscaling Worsening Radiation Effects in Bulk: SOI to the Rescue", Invited talk, IEDM conference, Washington DC, USA, December, December 2013

5. P. Roche, J.L. Autran, G. Gasiot, D. Munteanu, "Addendum to the Anthology of the Development of Radiation Transport Tools as Applied to Single Event Effects", Invited contribution, IEEE Trans. on Nuclear Sciences, Special Issue, December 2013.

6. P. Roche, Gilles Gasiot, Sylvain Clerc, Jean-Marc Daveau, Cyril Bottoni, Maximilien Glorieux, Vincent Huard, §Laurent Dugoujon, "A 65nm CMOS Platform for Space Applications: Qualification Test Results on Rad-Hard Microprocessors", submitted to IEEE Transactions on Nuclear Science, December 2013

For Further Information

Learn more about Cadence's functional safety solution at: http://www.cadence.com/cadence/newsroom/features/Pages/fusa.aspx

Learn more about the Cadence System Development Suite at: http://www.cadence.com/solutions/system_to_silicon_verification/pages/default.aspx

Learn more about the Incisive verification platform here: http://www.cadence.com/products/fv/enterprise_simulator/pages/default.aspx

Learn more about Incisive vManager solution here: http://www.cadence.com/products/fv/vmanager/pages/default.aspx

cadence®

Cadence Design Systems enables global electronic design innovation and plays an essential role in the creation of today's electronics. Customers use Cadence software, hardware, IP, and expertise to design and verify today's mobile, cloud and connectivity applications. www.cadence.com www.cadence.com