NEW FuSa methodology for safety-critical semiconductors

By: Nick Palmen

Functional safety cannot be an afterthought and needs to be addressed right at the beginning of the SoC (system on a chip) architecture design phase. The same is true for safety analysis and verification—the earlier, the better to avoid expensive late changes in the development cycle.

Automotive is one of the most challenging vertical market segments because suppliers need to meet high standards for quality, reliability, and safety. Particularly with the development of autonomous cars, functional safety is becoming even more important to ensure a safe ride in all kinds of traffic situations, during all weather conditions, regardless of whether it is day or night.

Meeting the market needs by developing safety-critical semiconductors to meet the ISO 26262 standard is a complex and compute-intensive task.

AI: Automotive Industries (AI) asked Robert Schweiger, Director of Automotive Solutions at Cadence, how the company is meeting the requirements.

Robert Schweiger, Director of Automotive Solutions at Cadence.

Schweiger: What most people don't know is that we introduced our first fault simulator, Verifault-XL, back in 1999. The ISO 26262 standard for functional safety of electrical and/or electronic systems for road vehicles was first published in 2011 and revised in 2018 to include semiconductors and IP.

In 2014, we announced the Incisive Functional Safety Simulator and other tools to specifically address the ISO 26262 requirements. Since then, we've been developing and enhancing our tools and flows to provide to our customers with a highly automated safety solution that helps them to achieve faster certification for their automotive and industrial products. Given this long history, Cadence is probably an EDA pioneer in functional safety.

AI: Cadence just launched a new comprehensive safety solution. What challenges is Cadence looking to solve with this new solution?

Schweiger: Today, many car companies are working on fully autonomous vehicles (AV) where the driver becomes a passenger, giving the control to a machine/computer. AVs require more advanced electronics and software to fully control and automate the vehicle.

So, OEMs and their suppliers need to make sure that their complex ADAS and autonomous driving systems are working as specified and there is no risk not only for the AV's driver and passengers but also for other road users.

With our new holistic safety solution, we provide a design flow that enables our customers to automate the design and validation of their electronic systems according to functional safety standards, like ISO 26262 for automotive but also IEC 61508 for industrial applications. In addition, by leveraging our solution, users can automatically generate safety reports and safety manuals to speed up the certification process for their end products according to these standards.

AI: What are the benefits of the Cadence Midas Safety Platform?

Schweiger: Advanced electronic systems of AVs are typically based on highly integrated circuits (ICs) aka systems on chip (SoCs). One of the key methods to analyze functional safety is a Failure Mode Effect and Diagnostic Analysis (FMEDA). However, traditional FMEDA tools are not integrated with the IC design flows to leverage native chip design data.

The Midas Safety Platform, which includes FMEDA, is fully integrated with the Cadence Safety Solution to enable a FMEDA-driven safety methodology, including safety analysis, verification and implementation for analog, digital and mixed-signal design. Hence the Midas platform has full access to the chip design database, including the number of transistors or gates and area.

Failure rate estimations rely on this data to predict failure rates as accurately as possible early in the design cycle, which the Midas platform can leverage to calculate the hardware safety metrics. Based on this, the safety architect can refine the safety architecture, including safety mechanisms, to detect failures in the system and take certain measures to mitigate or tolerate faults and report them when faults have been detected.

AI: Please tell our readers more about the different engines and flows for advanced safety design and verification built into the Midas platform.

Schweiger: In order to provide a holistic safety design and verification solution, we have significantly enhanced our analog, mixed-signal and digital verification flows.

The Midas Safety Platform sits on top of all Cadence flows and acts like a cockpit that guides the safety engineers through the development process. vManager Safety, which is our unified safety verification environment, controls all digital verification engines like Xcelium Safety and Jasper FSV, as well as the Spectre Simulation Platform, which is an optimized engine for analog/mixed-signal safety verification.

With more than 80% of field failures caused by the analog or mixed-signal portion of products, the integration of Cadence Legato Reliability into an automated safety solution was key. It provides a new analog fault simulation approach based on the concept of defect-oriented test (DOT) to measure and maximize the diagnostic coverage. The advantage of safety verification is to provide a much more accurate approach to determine the diagnostic coverage (DC), back-annotate the results to the Midas platform and recalculate the hardware safety metrics of the chip or system.

AI: What about implementation?

Schweiger: Of course, a holistic safety methodology doesn't stop with safety verification. We've also significantly enhanced our digital flow to support automated safety-aware digital implementation. Safety-critical automotive designs require some special implementation features like triple voting flop insertion or safety island generation to enable automated safety-aware P&R, including automated safety mechanism insertion in the Genus Synthesis Solution, our digital synthesis tool.

The Innovus Implementation System can then, for example, automatically control the creation, shape and routing of the safety islands for a dual-core lock step controller to the meet highest ASIL requirements. The Conformal Equivalence Checker can be used for signoff to ensure that the logic, including the dedicated safety structures implemented with Innovus Implementation, are functionally equivalent to the original RTL code synthesized by Genus Synthesis.

AI: Are there any moves to create a functional safety standard?

Schweiger: Both Accellera and IEEE have picked up the ball and have formed dedicated functional safety working groups focusing on different safety aspects.

The Accellera Systems Initiative is currently developing a standard that will specify a data model, language or format to exchange data seamlessly within safety-aware design flows and even the supply chain. The goal is to improve automation, interoperability, traceability and retargeting.

IEEE is focusing on the analog/mixed-signal safety design and has been developing the concept of DOT. The IEEE P2427 Working Group has standardized the definitions of manufacturing defects on the circuit by providing dedicated defect models, such as DC short, DC open and AC coupling, which are a prerequisite for analog defect simulation to analyze the analog test coverage.

The illustrations are self-captioning

As a member, Cadence is actively contributing to these standards with the goal to automate "design for safety" and enable a faster certification of safety-critical automotive and industrial designs.

AI: Where should a customer get started with safety?

Schweiger: Depending on the customer's end product, whether it's a pure digital SoC or more analog will define the flow that they need to focus on. Either way, they should first set up the Midas Safety Platform to create an architectural FMEDA of the technical safety concept of the SoC.

In the case of an existing Cadence design environment, they can start augmenting their functional verification flow to a safety verification flow. Due to testbench compatibility, they can reuse the functional verification testbenches for safety verification, which saves a lot of time. Last, but not least, they should set up a safety implementation flow, however this doesn't need to happen at once and can be done in different phases. AI