Understanding Automotive Reliability and ISO 26262 for Safety Critical Systems

Matthew Hogan, Mentor Graphics
Automotive electronics are playing a rapidly expanding role in automotive platforms tied to safety systems. Not content with the more traditional electronic systems such as airbag controllers, anti-lock breaking systems, engine control units, and the like, integrated circuit (IC) manufacturers have been expanding into advanced driver assistance systems (ADAS) and other automotive electronics to great effect, benefitting both drivers and occupants. Ensuring reliable design and verification of the ICs used in these systems, including compliance with industry standards like ISO 26262 [1], is critical for success in this highly competitive market.

**UNDERSTANDING THE RAPIDLY EXPANDING ROLE OF AUTOMOTIVE ELECTRONICS**

Automotive electronic systems such as rear back-up cameras have been used for some time now, providing increased convenience to the driver while also improving operational safety. In March, 2014, the United States’ National Highway Traffic Safety Administration (NHTSA) announced their final ruling making back-up camera systems mandatory for new vehicles in the US, “…all vehicles under 10,000 pounds, including buses and trucks, manufactured on or after May 1, 2018, to come equipped with rear visibility technology that expands the field of view to enable the driver of a motor vehicle to detect areas behind the vehicle to reduce death and injury resulting from backover incidents” [2]. While this requirement in and of itself presents an enticing incentive for those IC manufacturers in the image sensor (camera) industry to focus efforts in this area (if they are not already), there are also efforts to expand image sensor use for other automotive applications.

For example, even though ADAS does not rely heavily on image sensor technology today, a recently developed microcamera module [3] (Figure 1) may change the way automotive vision systems are deployed, and expand their range of uses. Leveraging this technology and other areas of “organic” growth provides opportunities for new entrants and new applications.

Other plans for US-based vehicles aimed at improving operational safety require complex systems to interact not only within a single vehicle, but also in concert with the surrounding traffic. One such application is the upcoming requirement of the US Department of Transport (DOT) that mandates vehicle-to-vehicle (V2V) communications [4] [5] (Figure 2). Many positioning pieces have been written on this topic, both for and against [6] [7] [8], with opponents expressing not only privacy concerns, but also technical challenges involving product feasibility and successful implementation within the proposed timeframes. However, a number of established automotive partners have already begun research in this area [9] [10], working in tandem with the US government.

While these new systems offer great opportunities for new entrants into the automotive market, the high standard for safety that must be established may be a stumbling block for those companies not familiar with or entrenched in the culture of automotive safety.
STANDARDS COMPLIANCE AND FUNCTIONAL SAFETY

The standard ISO 26262 is an adaptation of the Functional Safety standard IEC 61508 for Automotive Electric/Electronic Systems. ISO 26262 defines functional safety for automotive equipment applicable throughout the lifecycle of all automotive electronic and electrical safety-related systems. These functional safety features form an integral part of each automotive product development phase, ranging from the specification to design, implementation, integration, verification, validation, and production release [11].

Many established automotive Tier 2 semiconductor vendors have been developing their chips in compliance with the ISO 26262 defined process. This standard includes both the hardware and software development process.

Freescale has been particularly active in this space, having a “SafeAssure” functional safety program to educate their customers on the merits of standards compliance. They also have a rather elegant description of functional safety:

“Functional safety is achieved when there is the absence of unreasonable risk due to hazards caused by the malfunctioning of electrical/electronic systems. Industries impose functional safety standards as a way to ensure that safety-related systems will offer the necessary risk reduction required to achieve safety for the equipment. The functional safety standards include IEC 61508, which covers functional safety for the general industry, and ISO 26262, which covers functional safety for road vehicles.” [12]

Other IC vendors, like Infineon, are also promoting their products with ISO 26262 compliance [13].

The importance of these safety standards is amplified by the changes in the automotive electronic landscape. Some of these changes are being driven by an increase in the number of safety and critical systems controlled by electronic control units (ECUs) [14], while others are from the upsurge in vehicle infotainment systems. Back in 2009, it was estimated that even low-end cars had 30-50 ECUs [15], magnifying not only the complexity of the underlying hardware platform, but also that of the software used to control complex user interactions.

However, while in-vehicle infotainment (IVI) systems need high-reliability IC designs for marketability and brand perception, out-of-specification performance for these ICs results primarily in customer inconvenience. Although failure can lead to a significant negative market reaction, it is nowhere near the degree of concern and accountability incurred if an air-bag controller, brake sensor, or other safety critical IC fails.

Presently, the automotive market seems very attractive, with high growth and IC requirements for multiple new application areas. However, automotive safety systems involve increasingly complex ICs and the need for exceptional reliability. Understanding the reliability needs of these ICs can be challenging, particularly for companies just entering this market. The harsh environment present in automotive electronics operation [16] combined with the high reliability requirements for verification of these ICs [17] provides design and verification challenges that are not commonly encountered when designing and developing ICs used in less-demanding settings. While questions like which electrostatic discharge (ESD) or EOS compliance standards need to be met are often answered in industry standards documents, what’s not exposed are the challenges, design trade-offs, and best practices used to achieve compliance with these standards.
LEVERAGING IC VERIFICATION TOOLS FOR ISO 26262 COMPLIANCE

The traditional IC verification tools of design rule checking (DRC), layout vs. schematic (LVS) comparison, and electrical rule checking (ERC) can efficiently identify and solve very specific layout and circuitry issues within your IC design. Understanding the holistic impact of device implementation in the context of a larger circuit is not one of these. Being able to consider not only the net connectivity, but also the physical layout of the design within the same framework is something that traditional IC verification tools struggle with. Complex design constraints, device matching rules, and other implementation details that must be evaluated as part of a reliability design and verification flow are not within the scope of these tools.

Fortunately, a new class of IC reliability verification tool, such as Calibre® PERC™, is able to consider these problematic realms in a cohesive environment. Created out of the need to improve the coverage of IC reliability verification in a circuit aware context, Calibre PERC allows focused analysis on how circuits are implemented from both a circuit topology and layout perspective [18]. As part of this analysis, external constraints can be leveraged to direct the intent of checks and help determine which circuits are out of compliance. A reliability verification tool that can understand and assess those constraints is essential to identifying reliability issues and ensuring compliance with reliability requirements and industry standards.

One common example is protection and verification against time-dependent dielectric breakdown (TDDB) in interconnects (often called voltage-aware DRC [19]), where reliability verification in electrical overstress (EOS) environments plays a critical role. This issue requires larger design areas to avoid failure, but is critical to mitigate in high reliability IC designs. Figure 3 shows voltage-aware DRC checking using the Calibre® PERC™ tool. The verification occurs entirely within the Calibre PERC environment.

Much of the additional reliability verification performed on designs is to ensure robust operation over an extended operating period. To what levels you must go for the extra validation of design robustness is a measure of how critical correct device operation over time is to your market. Are point-to-point resistance, current density, and electromigration simulations on your “must do” list? What about hot gate identification [20] or device orientation matching [21] (Figure 4)? These and other reliability checks are important for the long-term reliability of your designs.
Understanding Automotive Reliability and ISO 26262 for Safety-Critical Systems

Calibre PERC can utilize a constraint file that contains the complete constraint documentation, as required by ISO 26262 [22]. This feature, combined with Calibre PERC’s unique capability to identify device interactions in the context of the overall circuit, provides a compelling reliability verification solution for IC vendors looking to produce ISO 26262 compliant chips.

SUMMARY

This is a time of incredible change and growth in the electronic systems and number of ICs used in automotive vehicles. New entrants to the automotive Tier 2 marketplace, together with new expectations of how cars are designed, built, and driven, provide burgeoning opportunities for semiconductor vendors to develop new chips in compliance with the ISO 26262 defined process. Leveraging EDA tools like Calibre PERC to ensure accurate reliability verification while achieving compliance with industry standards can provide IC vendors and their customers with valuable product confidence.

To learn more about Calibre PERC’s full range of capabilities, visit our website at:

http://www.mentor.com/perc

REFERENCES:


Growing number of ecus forces new approach to cars electrical architecture, http://www.newelectronics.co.uk/electronics-technology/growing-number-of-ecus-forces-new-approach-to-car-electrical-architecture/45039

This Car Runs on Code, http://spectrum.ieee.org/transportation/systems/this-car-runs-on-code


Thanks for reading.

**Additional Calibre PERC information that may be of interest:**

- [Improving Design Reliability By Avoiding EOS](#)
- [Improve Reliability With Accurate Voltage-Aware DRC](#)