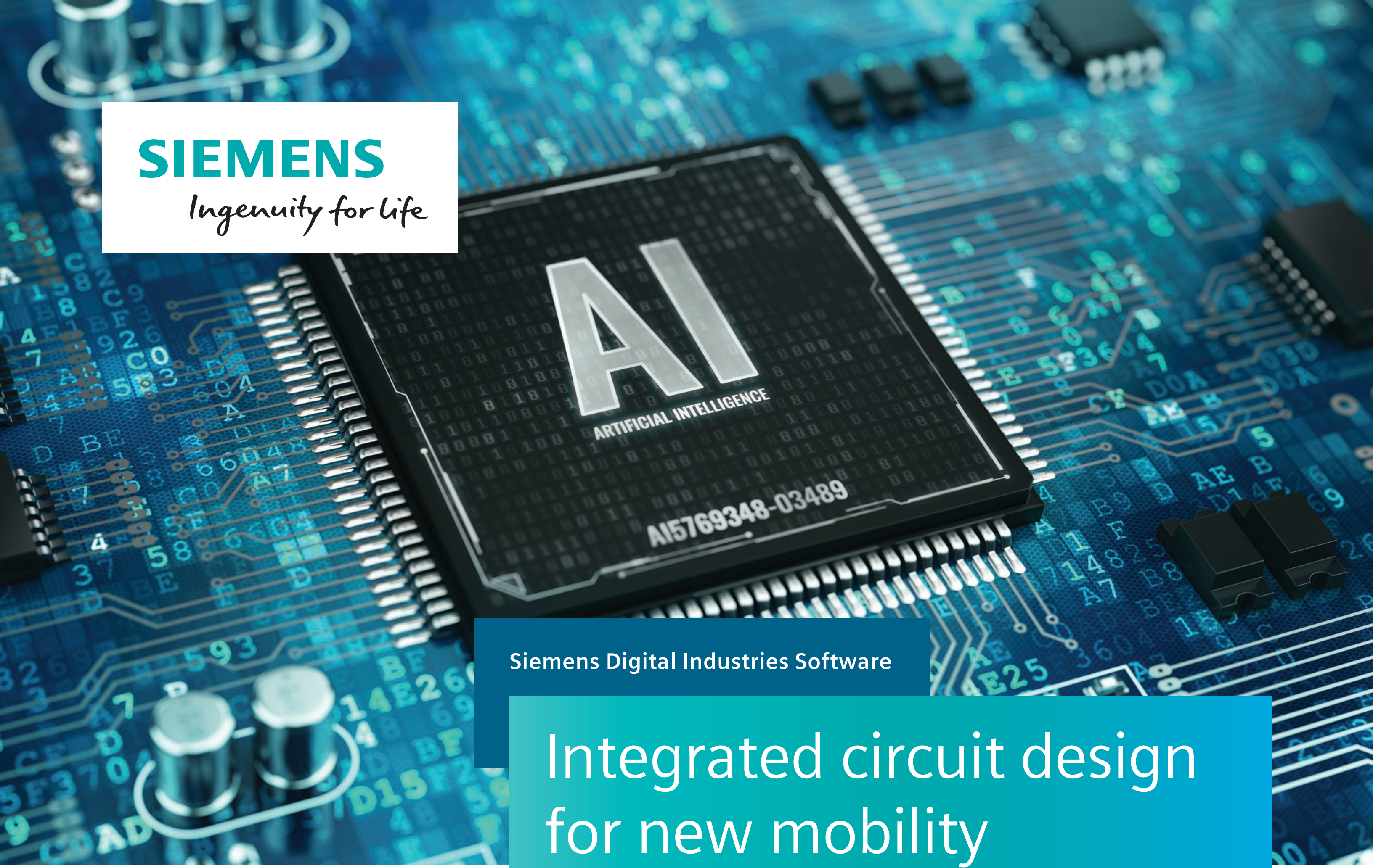
SIEMENS

Ingenuity for life



Siemens Digital Industries Software

Integrated circuit design for new mobility

Executive summary

The success of autonomous vehicles hinges on the ability of a system of advanced sensors and powerful chips to perceive and process an immense amount of data in real-time. These chips will require never-before-seen architectures to meet the power, performance and area required for automated driving, while surviving the harsh environmental conditions inside a vehicle. As automotive startups, established OEMs and systems companies vie to create these advanced systems, they will need a portfolio of advanced design automation and lifecycle management tools. Among the requirements of such tools in the years ahead – accelerating the creation of bespoke designs; enabling work across previously disparate technical disciplines; and providing access, via APIs and ongoing integration, to open platforms and technology-based ecosystems.

Andrew Macleod
Director of automotive marketing for the Mentor portfolio
Siemens Digital Industries Software

New mobility demands new technology

New mobility refers to a group of technologies that are disrupting traditional means of moving humans and goods from one place to another. Today, this includes ride-sharing services, city-wide bike sharing programs, electric scooters and of course, connected, autonomous and electric vehicles. The latter have garnered innumerable hours of public, corporate and media attention due to the large-scale industry and societal changes they will cause. Siemens is perhaps unique in the world as a chip-to-city supplier to nearly all of this era's current and would-be transportation providers – carmakers and tier 1 suppliers, tech companies, mobility service providers and cities.

Connected, electric and autonomous vehicles will alter how cars are evaluated and used. In particular, the value of electric and autonomous vehicles is increasingly found in the electronics, and not the mechanical aspects of the vehicle. In the new age of mobility, companies that are able to own and optimize the design of the critical electronics will capture more of the profit available. This fact is bringing traditional automotive manufacturers into the electronics business, and simultaneously attracting tech companies like Google and Facebook into the automotive industry.

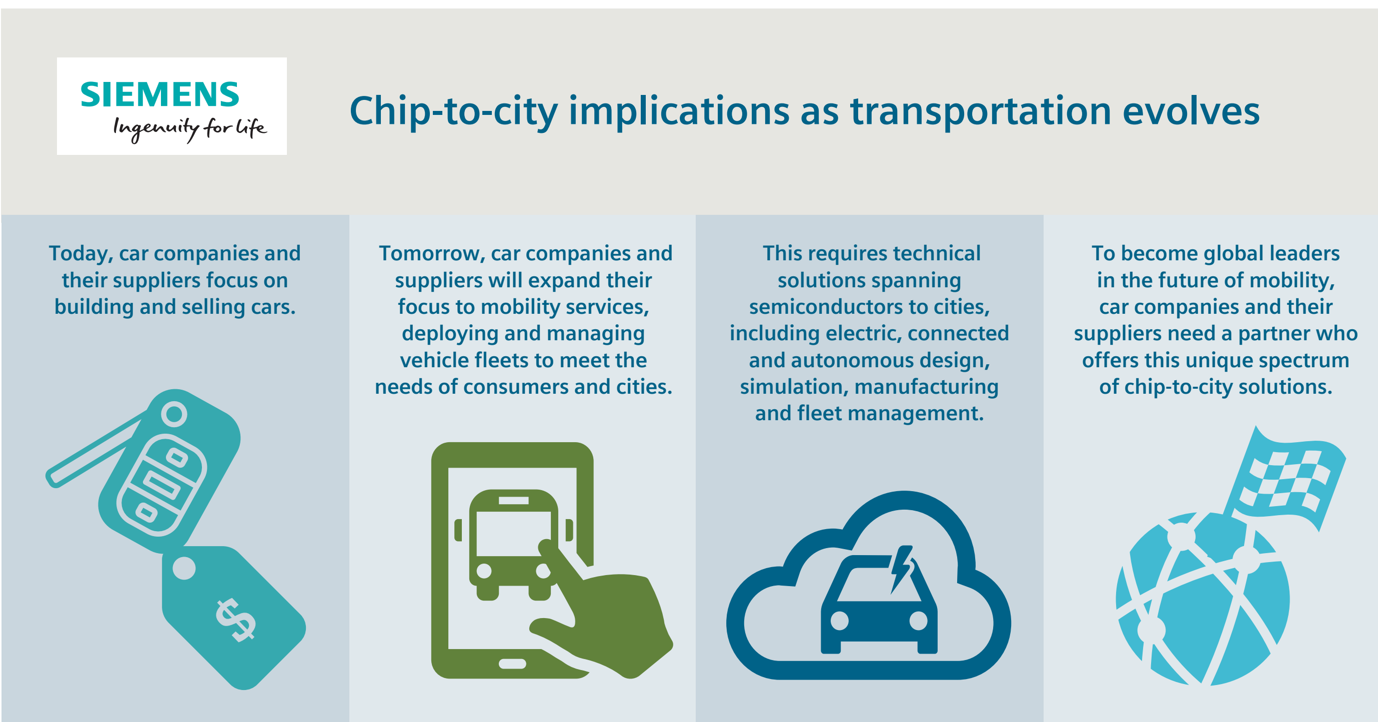
Consider the electronic content of an autonomous vehicle. The Society of Automotive Engineers (SAE) defines six levels of sophistication for autonomous vehicles, from zero to five. A level five autonomous vehicle will use a network of fifty or more advanced sensors to perceive the driving environment. This

New mobility technologies such as autonomous cars and ride-sharing will disrupt our usual methods of transportation.

network will link LiDAR, radar, camera and other sensors to detect key features of the vehicle's environment such as road lines, traffic signs and signals, other vehicles and pedestrians. Next, a set of integrated circuits (IC) will process the gigabits of sensor data being gathered every second, process it and decide on a response.

This architecture will converge, with larger and more powerful domain controller systems-on-chips (SoCs) connected to a centralized processing unit, all implementing artificial intelligence. To date, many autonomous vehicle programs have used CPUs and GPUs, designed for data center or personal computing applications, as these domain controllers and central processors. These solutions worked well for early testing and development tasks, but are not equipped to meet the power, performance and area requirements of a true autonomous vehicle SoC. Chip designers are discovering that meeting these requirements will require new silicon and system architectures, developed around artificial intelligence, machine learning and information processing.

Developing bespoke SoCs to meet these exacting requirements is one of the most difficult, and critical challenges that autonomous vehicle programs must overcome to achieve commercial success. The ability of these chips to navigate a vehicle safely and reliably through an environment will be a key differentiator in the autonomous vehicle market. The safest and most reliable system will garner the greatest public trust, and thus the most favor in the marketplace. Advanced IC design and verification solutions can help companies realize their SoC designs, verify them, maximize their post-manufacturing yield and ensure their reliability over long lifetimes.



Accelerating automotive IC design cycles

To meet the high-performance and low-power requirements of autonomous vehicles, SoC designers will need to create bespoke silicon architectures optimized for artificial intelligence algorithms. Using traditional design methodologies will take far too long, as the complexity of designs increases and verification time rises. To lower the investment in time and manpower, many companies are looking for a proven solution that can increase their productivity and design quality, while accelerating their time-to-market. This explains the increasing interest in high-level synthesis (HLS).

HLS takes high-level descriptions of the design functionality in SystemC or C++ and synthesizes them into RTL. Designing at a higher level of abstraction accelerates the completion of initial designs by separating the specification of the chip functionality from the implementation (figure 1). Designers must only describe what the chip needs to do, without delving into how it accomplishes such functionality. Then, the HLS tool automatically generates RTL to implement the described functionality.

Using HLS to design at a higher level of abstraction can reduce design times to a few months, and requires half as much code as a traditional RTL flow. Late functional changes, new features, or even a migration between technology nodes or from FPGA to ASIC can be incorporated without impacting the design schedule. HLS also enables the design team to explore hundreds of design variants to optimize the power, performance and area of the chip. Design space exploration results in higher quality designs compared to hand-coded RTL.

Incorporating emulation into this flow enables the design team to further accelerate design. The RTL generated from HLS can be instantiated in an emulator, providing the software team a platform to test their software before any chip hardware is available. Meanwhile, synthesized sensor and mechatronic system data can be integrated to create a virtual environment that provides realistic feedback to help optimize hardware and software designs.

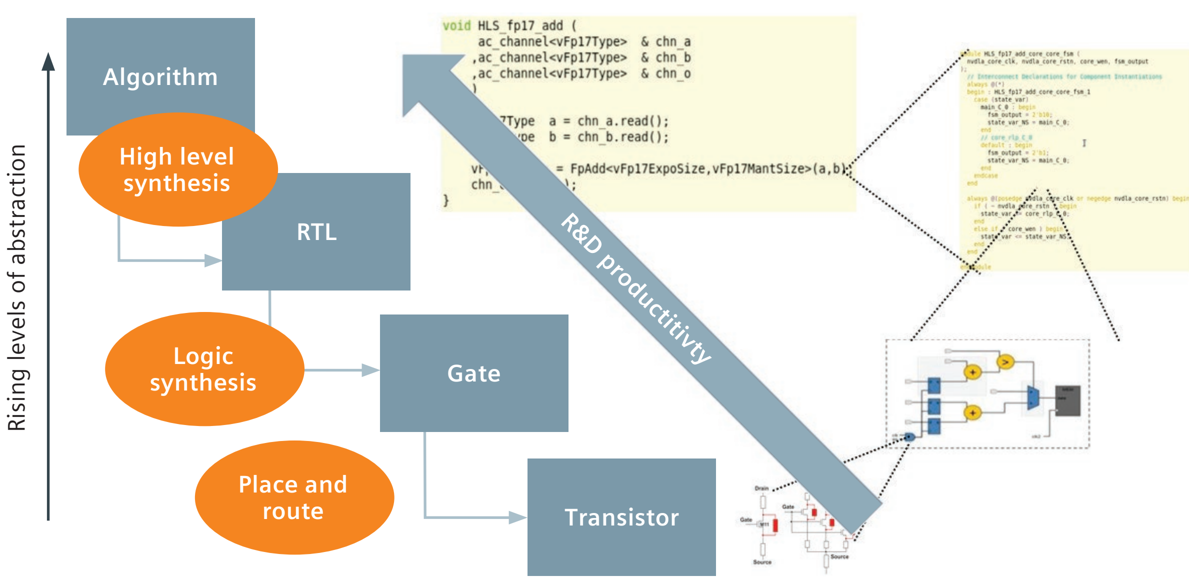


Figure 1: HLS rises the design abstraction level to improve design productivity.

Finally, advanced HLS solutions can conduct robust verification of the designs to remove bugs and errors before the designers commit to RTL (figure 2). HLS verification capabilities include automatic formal checks of the C++ or SystemC code, simulation based C-to-RTL verification and formal equivalence verification to find bugs and errors before synthesizing to RTL.

Established automotive manufacturers, startups and chip companies alike will need to develop brand new silicon architectures optimized for neural computing and computer vision to make autonomous vehicles possible. Existing design methodologies cannot scale to meet this demand. SoC designs for autonomous vehicles are too complex to design efficiently by hand-coding RTL. Additionally, verification times are escalating out of control, making it necessary to verify designs as early as possible. HLS can deliver higher quality SoC designs faster and more efficiently than hand-coded RTL. New HLS solutions further enhance this advantage with automatic C-to-RTL verification. In sum, HLS can provide productivity gains up to 10X, and help designs get to market four times as fast.

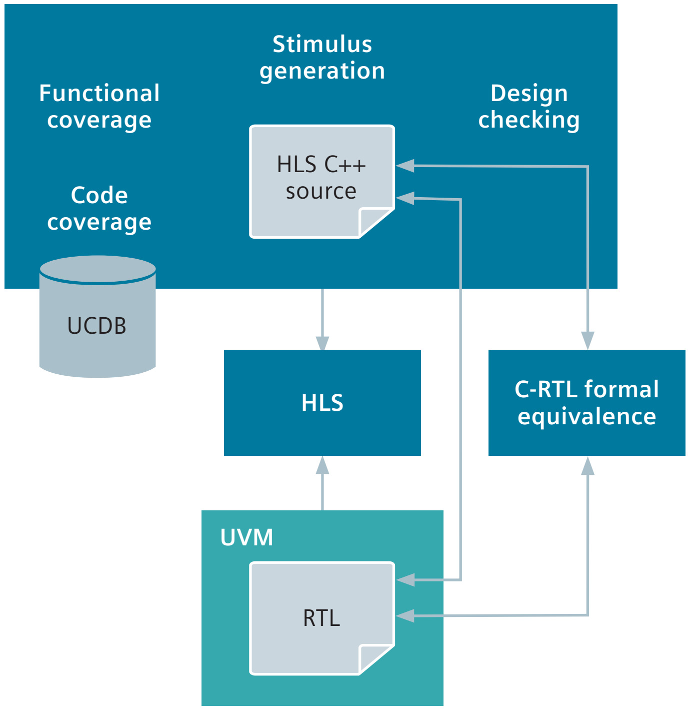


Figure 2: Advanced HLS flows HLS can perform C-to-RTL verification to remove bugs and errors before committing to RTL.

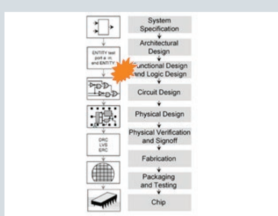
Functional safety, verification and design for safety

Despite the numerous challenges involved in designing SoCs for AVs, the most substantial obstacle to the success of AVs is earning the trust of the public. One way AV manufacturers can establish this trust is to demonstrate the safety and reliability their platform through safety standards and certification. To that end, the automotive industry has established a set of procedures and standards focused on the safety of electrical and electronic systems, known as functional safety. Functional safety is the reduction of the risk of electrical and electronic components malfunctioning due to failures. In the automotive industry, these procedures and requirements have been formalized in the ISO 26262 standard. ISO 26262 requires that electronics be tested for random hardware failures and systematic faults (figure 3).

Systematic faults are those that prevent an integrated circuit from operating correctly according to the product specifications. These could be design bugs, hardware/software interface problems, misinterpreted or incomplete specifications and so forth. The goal is to eliminate systematic faults through robust design procedures, qualified EDA tools and formal requirements.

On the other hand, random hardware faults occur over time as the IC operates. Random hardware faults can be caused by electromagnetic interference (EMI), electro-migration and other electrical phenomena. Some of these faults are transient, and will disappear with time, while others are permanent. In either case, a random hardware failure in a mission-critical autonomous IC has potentially catastrophic consequences. Therefore, ISO 26262 requires that chips continue to operate, or fail safely, in the event of a random hardware fault.

Systematic faults



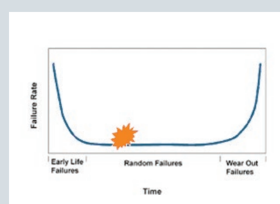
- Incomplete specs
- Misinterpreted specs
- Bad RTL
- HW/SW interface problems

Challenges

- Process and requirements
- IC complexity
- Exhaustive and efficient

ISO 26262 and IEC 61508

Random faults



- EMI
- Electro-migration
- Permanent or transient
- Latent

Challenges

- Emerging requirement
- Manual > automation
- Scale with IC complexity

Figure 3: ISO 26262 requires that electronics are tested for systematic and random faults.

There are four key processes in a complete functional safety flow (figure 4).

1. Lifecycle management covers the functional safety lifecycle from planning to compliance. This includes design changes, requirements, quality assurance and audit or compliance management.
2. Next, safety analysis uses failure modes, effects and diagnostics analysis (FMEDA) to understand potential failure modes of the design due to random hardware faults. FMEDA automatically computes the failure in time (FIT) rate of the design, and estimates the single-point and latent fault metrics (SPFM/LFM). A fault list is also generated to use during the safety verification process.
3. Third, design for safety attempts to enhance or modify the design to mitigate potential failures from random hardware faults. This is achieved by inserting safety mechanisms into the design that detect and correct faulty behavior, ensuring the design behaves and fails safely. Some toolsets can even perform this insertion automatically.
4. Fourth, safety verification proves that the design is safe using fault injection to test the behavior of the design and safety mechanisms during a random hardware failure. The results of safety verification are compared to the FIT rate, SPFM/LFM and the diagnostic coverage (DC).

In the past, SoC designers and engineers had to call in experts, who performed these critical tasks with painstaking manual procedures. Relying on experts creates a bottleneck in the SoC development process, and prevents the experts from focusing on unique and challenging problems requiring of their skill. Today, advanced portfolios of solutions, such as Mentor Safe IC, are able to achieve rigorous functional safety standards while automating lifecycle management, safety analysis, design for safety and safety verification processes. This accelerates the verification of functional safety for compliance with industry standards such as ISO 26262.

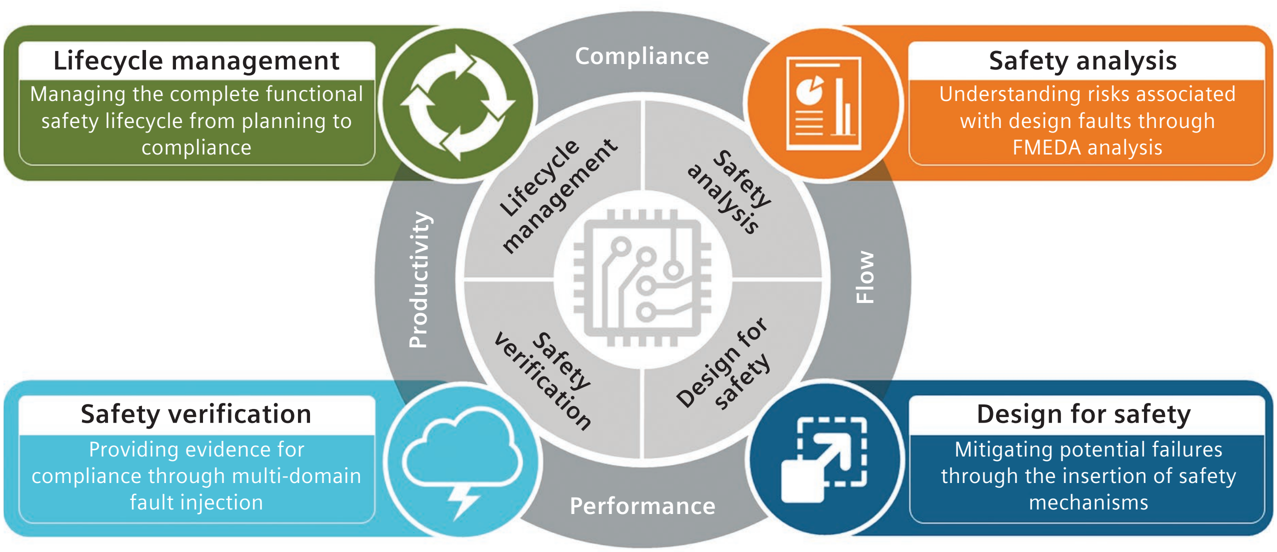


Figure 4: The four key processes in functional safety include lifecycle management, safety analysis, safety verification and design for safety.

Emulation's role in verification

In the process of verifying complex autonomous vehicle chips for functionality and functional safety, engineers will conduct hundreds of thousands of complex tests on the chip design. Hardware simulation cannot provide the speed and throughput necessary to complete this verification in a timely matter on its own. Hardware emulation is a necessary augmentation to verify the millions of scenarios needed to ensure the safety and functionality of an autonomous vehicle. Hardware emulation executes tests in the hardware design at megahertz (MHz) speeds. This enables system verification to begin before the chip design is implemented in silicon and provides full visibility into the hardware design for efficient debug. Furthermore, emulation supports fault injection, monitoring and results analysis for safety-critical automotive applications.

Emulation provides unparalleled flexibility for collaboration throughout the supply chain without altering the design flow. An emulator can run specific pieces of IP, or the entire SoC design long before any silicon is ready. Therefore, engineers can begin writing software and testing it with the evolving SoC design on which it will be implemented. Engineers can then feed the emulation with synthetic sensor data, and output to an environment that models the vehicle's behavior to test how the IP and software respond to stimuli. With emulation, each level of the supply chain will be able to begin development earlier while testing within a model of the entire system.

It is not feasible to test every possible safety scenario in the real world. As vehicles progress from level 1 to level 5 automation, the number of potential scenarios that must be investigated to properly validate a vehicle explodes into the millions. As a result, estimates predict that it will require more than eight billion miles to fully test and verify the safety and functionality of an autonomous car. The only way to achieve this amount of verification is with a virtual testing environment employed early in the design process.

Hardware emulation supports model, software and hardware in-the-loop verification. It provides an environment to test, program and debug an IC or an entire autonomous vehicle platform before any chip or vehicle hardware is available. This testing environment merges three data types (figure 5). First is sensor data. To generate this data without sensor hardware, advanced physics-based sensor simulations feed the hardware emulation with simulated LiDAR, radar, camera and other sensor data. Second is compute data that is provided by the emulator running the autonomous drive IC. Third, a mechatronic simulator provides actuator data from steering, braking and drivetrain systems. Advanced sensor simulators can also generate traffic patterns and simulate V2X communications to fully test the capabilities of an autonomous vehicle platform.

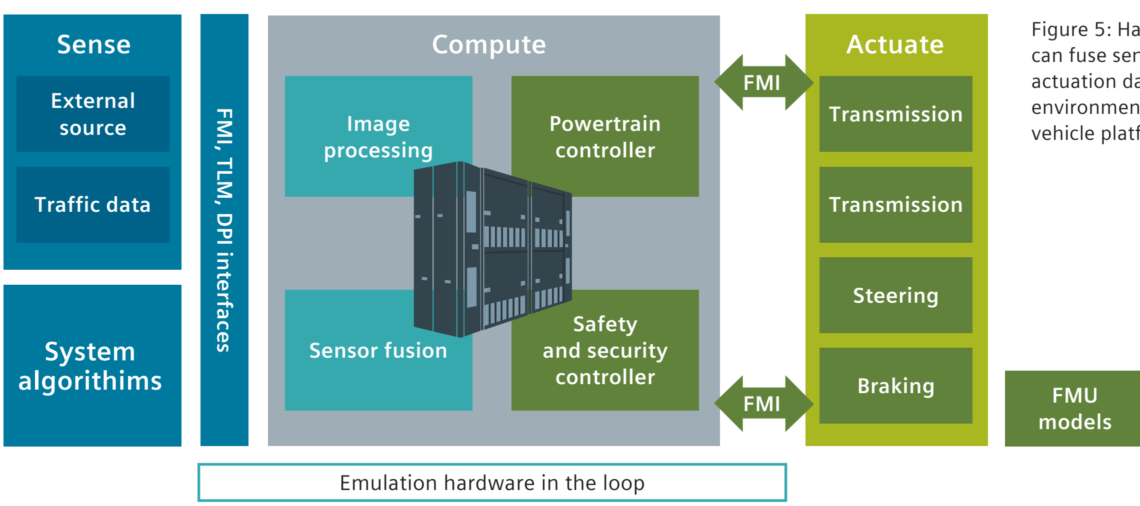


Figure 5: Hardware emulation can fuse sensor, compute and actuation data to create a testing environment for autonomous vehicle platforms.

Physical reliability verification

Now, the SoC design team has optimized the chip through rapid iteration enabled by HLS, verified for its functionality and functional safety, and even tested it in a realistic virtual driving environment with simulated sensor and mechatronic data. Next, the physical reliability of the design must be verified to ensure that the design will survive the manufacturing process with sufficient yield, and will operate as intended in the real-world. The hand-off from design to manufacturing is a critical juncture in the IC design process; it is where the rubber meets the road.

Understanding the reliability needs of autonomous vehicle ICs can be challenging, particularly for companies just entering this market. Typical automotive ICs are expected to function for up to thirty years in temperatures that can range from -40° C to 150° C, and electrical loads into the hundreds of volts. The harsh driving environment that automotive electronics must operate in, combined with the high reliability requirements for verification of these ICs, creates design and verification challenges that are not commonly encountered when developing ICs used in less demanding settings. Design standards will mandate acceptable criteria for electrostatic discharge (ESD) or electrical overstress (EOS) compliance, but they cannot articulate the design trade-offs or best practices needed to meet such criteria.

The traditional IC physical verification tools of design rule checking (DRC), layout versus schematic (LVS) comparison and electrical rule checking (ERC) can efficiently identify and solve very specific layout and circuitry issues within your IC design. But they cannot understand the holistic impact of device implementation in the context of a larger circuit. Standard physical verification tools struggle to consider the net connectivity and the physical layout of a device in the same framework.

Fortunately, a new class of IC reliability verification tool 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, these tools allow focused analysis on how circuits are implemented from both a circuit topology and layout perspective. 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), 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.

Next, designers must optimize the physical layout of the chip for successful manufacturing. Design for manufacturing (DFM) solutions can help designers by automatically performing layout optimizations, simulating manufacturing processes, or managing lithographic hotspots before tape-out. DFM solutions automatically measure changes in yield that result from proposed layout modifications. This gives designers the ability to select layout modifications that will maximize manufacturing yield and reliability of the chips.

When digital and analog collide

The complex digital processor and controller SoCs of an autonomous car will interact with the analog world through a variety of sensor systems. Some of these systems will require powerful chips of their own to manage advanced sensors like LiDAR, Radar and computer vision systems. These advanced sensor systems, however, would be at a loss without the many smaller smart sensor systems that perform specific, but critical tasks.

Many companies develop custom ICs to enable their smart sensor systems. Micro-electro-mechanical systems (MEMS) are commonly used for the sensing device, with the rest of the circuitry as an analog/mixed-signal (AMS) design implemented in a CMOS technology (figure 6). Creating a custom IC design enables companies to reduce the cost, size and power consumption of the IC compared to creating the system with off-the-shelf components. But, AMS design is challenging due to the multiple design domains at play. The MEMS design must interface effectively with the analog circuitry, which in turn must integrate with the analog to digital converter and digital logic.

Automotive AMS ICs must also operate with extreme reliability for many years, and often under harsh environmental conditions. To manage, designers will need an integrated design and verification solution that can bridge analog, digital and MEMS to create the single-purpose smart sensor systems critical to autonomous vehicles.

Aging simulations are important in automotive applications because the devices must operate reliably over ten years or more. Automotive applications have stressful bias and thermal conditions which cause circuit degradation over time. Using simulation, potential reliability issues can be detected early and rectified at the design level. Next, electrothermal simulation helps account for circuit problems caused by self-heating and mutual heating, which are a result of high power dissipation. Finally, safe operating area (SOA) simulations detect dangerous situations that may occur over the life of a component.

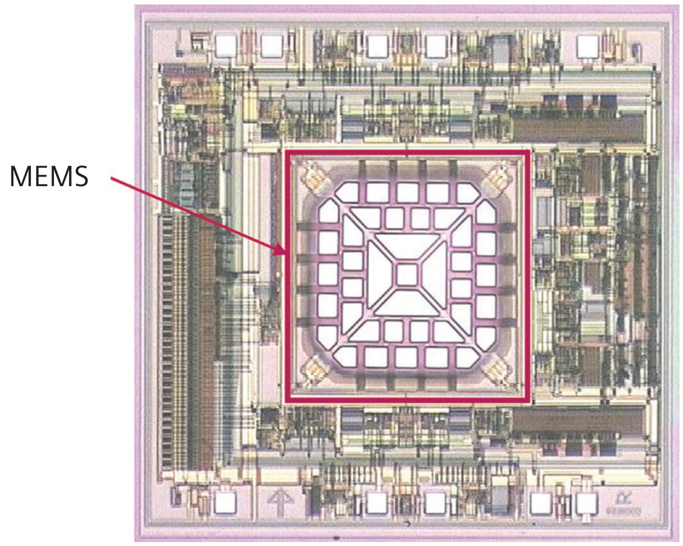


Figure 6: A MEMS device integrated on a CMOS IC. (Source: MEMSIC)

Furthermore, mixed-signal verification is traditionally a divide-and-conquer approach in which digital and analog blocks are verified individually. Even the relatively simple smart sensor ICs are growing too complex for this approach. While digital verification techniques have evolved over the years, mixed-signal verification is still catching up. Modern analog modeling approaches are developed, but the need for accuracy still takes top priority when it comes to analog verification.

Additionally, the analog and digital design environments and verification use models are different, making it challenging to integrate the IC for full mixed-signal verification. To address these challenges, mixed-signal simulation solutions need to be fast, accurate, easy to use and seamlessly integrate into existing analog and digital verification flows.

Ensuring safety over a lifetime

The unique challenges for producing automotive ICs do not end with design and verification. Automotive ICs must meet very high bars for quality and reliability, and do so at the bleeding edge of performance, power and area. To address these concerns, integrated circuits are tested rigorously after fabrication. IC testing consists of supplying a device under test (DUT) with an electrical signal, and checking the output against the expected values to see if they match. IC testing methods have evolved to limit the time and cost incurred during testing. However, the complexity and safety requirements of autonomous ICs are increasing test time and cost again.

Traditional DFT fault models and test methodologies consider faults that arise from cell-level inputs and outputs, and only some faults that occur on interconnect lines between cells. This level of abstraction is no longer suitable for the small device geometries needed to meet automotive power, performance and area requirements.

New, automotive-grade, ATPG technologies have been developed that target defects at the transistor and gate level. These new methodologies rely on cell-aware test (CAT), which uses fault models that specifically target defects internal to each cell. Mentor's CellModelGen fault model extraction uses layout-annotated Spice representations of the cells to identify the location of possible transistor, bridge, open and port defects. The cell layout is analyzed for potential bridge defects by calculating the critical area of each potential defect and its related defect probability. This analysis generates a model that ensures the highest possible defect detection, minimizes pattern count and preserves required information for diagnosis. Capturing these otherwise undetectable defects helps the makers of digital ICs meet the ISO 26262 goal of zero defective parts per billion (DPPB).

Automotive-grade ATPG has been instrumental in increasing the quality of testing to meet the rigorous standards of ISO 26262. But, ATPG and standard test procedures only cover the chip after manufacturing. Periodically testing these chips during operation is a crucial step to ensuring their reliability, especially over the long service life of an automotive chip.

Built-in self-test (BIST) is test IP that is inserted into the chip for testing digital logic or memory in the field. Logic BIST involves the on-chip generation of pseudo-random test patterns that are applied to the chip's circuitry. Traditional BIST technologies test the chip at power-on, to prevent the test process from affecting the chip's performance. Advanced testing solutions can perform tests during the chip's operation without affecting its performance. In addition, ATPG compression can be integrated with BIST for manufacturing-quality test that can be performed for both power-on and in-systems testing.

On the cutting edge, on-chip test controllers can interface with any and all test IP that has been inserted into a chip. This provides a variety of users, up to the OEM and dealer, with the capability to reconfigure test IP for post-manufacturing use cases (figure 7). Tier 1 suppliers can use this capability to retarget existing test IP to test ECUs and other control units, and to check application specific functions. At the OEM level, test IP can be reconfigured to perform in-system test runs to ensure the chip functions correctly as a part of an entire vehicle. Finally, the dealer can access the test IP to diagnose and repair chip functions, and perform firmware – over-the-air (FOTA) updates.

DFT instrument access and debug-specific test	FOTA, diagnosis and repair	**Dealer**
In-system test run	Vehicle	**OEM**
DFT intrument access and re-use	Application/AUTOSTAR	**Tier 1**
Test retargeting and re-use	ECU/xCU	**Tier 1**
DFT insertion and test development	Hardware chip	**Tier 2**
DFT instrument insertion	Hardware IP	**Tier 3**

Figure 7: Advanced test controllers enable test IP reuse at all levels of the supply chain.

Conclusion

The success of autonomous vehicles hinges on the ability of a system of advanced sensors and powerful chips to perceive and process an immense amount of data in real-time. As a result, these chips will require never-before-seen architectures to meet the power, performance and area required for autonomous drive. Furthermore, autonomous ICs will need to function with near flawless reliability and accuracy, despite harsh environmental conditions, for extended periods of time, much longer than ICs in traditional consumer electronics.

Designing these chips is just the beginning. Autonomous vehicle IC designs must be proven to operate correctly and fail safely in the event of a random hardware failure. Functional safety standards like ISO 26262 are necessarily rigorous, targeting zero defective parts per billion (DPPM) for safety-critical ICs. Ensuring this level of quality in astonishingly complex autonomous ICs will require a new flow that combines simulation and emulation to “left-shift” verification in the design process. The ICs must also be validated within the system, a task that cannot wait until real-world testing.

The physical reliability of the chips must also be verified and proven to comply with functional safety standards and manufacturing requirements. Physical verification tools are necessary to ensure that designs meet the specifications provided by the foundry, that the layout and schematic representations match, and that electrical phenomenon will not lead to random hardware failures. Additionally, the mixed-signal ICs that power the many supporting sensors come with their own design and verification challenges. The interactions between digital and analog logic can be particularly troublesome, requiring solutions tailored specifically to those challenges. After manufacturing, the ICs will need to be tested time and time again to ensure proper functionality off the fab floor, and while in the field.

As automotive startups, established OEMs and systems companies vie to be the first to market, they will need a portfolio of advanced design automation and lifecycle management tools. Siemens Digital Industries Software is uniquely positioned to provide such tools, with leading solutions in HLS, functional safety and verification, emulation, physical reliability verification, AMS design, mixed-signal verification and IC test.

More information

Jim McGregor, "AV Simulation Extends to Silicon," TIRIAS Research, May 2019

Junko Yoshida, "Robocar SoCs: Designers' Worst Nightmare | Siemens takes on challenges of AV/ADAS chip design and validation," EE Times, May 17, 2019

"David Fritz and Jim McGregor on Chips For Autonomous Vehicles," The Autonocast podcast, Episode #144, May 22, 2019

Siemens Digital Industries Software

Headquarters
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 972 987 3000

Americas
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 314 264 8499

Europe
Stephenson House
Sir William Siemens Square
Frimley, Camberley
Surrey, GU16 8QD
+44 (0) 1276 413200

Asia-Pacific
Unit 901-902, 9/F
Tower B, Manulife Financial Centre
223-231 Wai Yip Street, Kwun Tong
Kowloon, Hong Kong
+852 2230 3333

About Siemens Digital Industries Software

Siemens Digital Industries Software, a business unit of Siemens Digital Industries, is a leading global provider of software solutions to drive the digital transformation of industry, creating new opportunities for manufacturers to realize innovation. With headquarters in Plano, Texas, and over 140,000 customers worldwide, we work with companies of all sizes to transform the way ideas come to life, the way products are realized, and the way products and assets in operation are used and understood. For more information on our products and services, visit siemens.com/plm.

About the author

Andrew Macleod is director of automotive marketing for the Mentor portfolio at Siemens Digital Industries Software, based in Austin, Texas. Read his blog post "Cars, mobility, chip-to-city design and the iPhone 4" here. Follow him on Twitter@AndyMacleod_MG.

siemens.com/plm

78104-C5 7/19 C