SIEMENS
Ingenuity for life

Siemens PLM Software

Safety first – On meeting the only self-driving requirement that really matters

Automotive

Andrew Macleod
Director of automotive marketing for Mentor product suite

Introduction

All of a sudden the autonomous future is looking a bit more uncertain, which is somewhat surprising given what tech and auto boosters have been saying for years now – namely, that self-driving cars are "just around the corner." (Google that phrase to see just how often they've been saying it.) The proximate cause of the change in outlook is that accidents have started to happen, including several involving fatalities. And that is shifting the public conversation, perhaps for the foreseeable future, to a focus on safety and trust, whether the topic is the design of chips and sensors or the fates of nameplates and entire fleets. Innovating in this environment of public and press skepticism, and mounting attention from governments, may get harder. Certainly there will be a new premium on testing of all types. What should the Silicon Valley, the world's auto capitals and the sprawling global auto supply chain do to respond?

Consider that even a few years ago, the self-driving storyline was nearly entirely positive. Autonomous vehicles were going to do everything from curbing noxious traffic and carbon emissions to helping the elderly and disabled to streamlining the cumbersome accident claims process. And of course self-driving cars would save vast numbers of lives. New developments and prototype vehicles with no steering wheels or pedals were covered with "gee whiz" earnestness even by the most jaundiced of news outlets and journalists. And the technologists and execs pushing the vehicles were more often than not lauded as tech heroes.

What a difference a few years makes. Now the only white knights are the regulatory veterans hired to clean up safety programs among the newly chastened self-driving elite. And the overall tone is now one of skepticism or downright hostility. To be sure, at least some of this shift can be explained by the general tumult in tech, no longer seen as an unvarnished force for good but instead as an opened Pandora's box of powerful and entirely mixed blessings. (Example: autonomous delivery vehicles should dramatically cut costs and boost efficiency though may also put millions of drivers out of work.) But part of the increasingly dark mood about self-driving tech is due to that still very small number of well-publicized fatal accidents, a phenomenon that all agree is sure to continue even if no one wants to talk about it.

Here it's important to reiterate what the traffic safety engineers have told us all along. The toll taken by human drivers is unacceptably high and the main point of shepherding this new technology into existence is to reduce the carnage, which by the way is getting worse. Fact: after years of decline, road deaths are now increasing, passing the 40,000 killed mark in the United States in 2017, up from 36,000 the year before. All the more reason, it would seem, to get humans out of the decision-making and driving loop as soon as possible. However, given the unique place of driving in culture and the vagaries of human psychology, self-driving technology will likely need to be dramatically safer than the alternative before it's deployed en masse. Elon Musk famously said he won't remove the beta label from Tesla's Autopilot system until it's 10 times safer than the U.S. vehicle average. Others have said demonstrated safety levels will need to be orders of magnitude higher still.

Figure 1: NTSB employees examine an Uber autonomous car involved in a fatal crash in Tempe, Arizona.

For the automotive industry to make this a reality, it needs to develop smart and safe systems that, through simulation and testing, can convince the wary public, regulators and governments. Any such development process will require not only physical testing, but also physics-based simulation. Physical testing is required to verify and demonstrate that physical products comply with specific requirements and quality standards related to functional safety, like ISO 26262. On the other hand, simulation is needed to make quick and cost-effective design iterations, and validate that the system can handle all possible real-life use cases in an environment that is reproducible and safe. A robust methodology that focuses on a complete validation and verification framework is key to help the industry move quicker towards complete solutions that lead to faster automated vehicle development.

The methodology

Similar to agile software development, this methodology emphasizes an iterative, incremental and systematic approach with very short feedback loops and adaptation cycles. Two main requirements underpin the approach:

1. Internal and external guidelines set by manufacturers, regulatory bodies and the consumer.
2. A digital twin of the "problem-solution space." This consists of not only detailed vehicle models including sensors and algorithms, but also 3-D depictions of physical space, including models of roads, traffic, occupants and weather.

Ultimately, the goal is to put automated vehicles on the road. To achieve this, automated driving technology, ranging from system-on-a-chip design, sensor development, data fusion and system integration, to full vehicle performance evaluation and traffic impact analysis, must prove to be safe and reliable. Our proposed methodology includes three different validation and verification (V&V) environments that use advanced simulation environments as well as physical testing facilities to help OEMs, Tier 1 suppliers, and other solution providers to demonstrate that the autonomous systems they build are certified and good enough to be put on the road.


EE Times Connecting the Global Electronics Community

NEWS & ANALYSIS: Robo-Uber: What Went Wrong

designlines AUTOMOTIVE

News & Analysis

Robocar Testing: It's Simulation, Stupid!

You can still miss the ground truth even with millions of miles of test drives on the road

Junko Yoshida

3/27/2018 08:00 AM EDT

6 comments

NO RATINGS
LOGIN TO RATE

Like 6 Tweet Share G+

After the latest Uber debacle, in which the company's robocar killed a woman crossing a street late at night, here's the million-dollar question: Will the autonomous vehicle development community be talking more about their simulations instead of miles of real-world test drives that they racked up on public roads?

Figure 2: *EE Times'* coverage of Siemens autonomous driving system simulation offering announced in 2018.

The first V&V environment is performed via simulation tools that are applied in model-in-the-loop (MIL), software-in-the-loop (SIL) and cluster applications. In this environment, the idea is to cover as many scenarios as possible (millions of scenarios) in a controlled environment that offers a quick turnaround and allows variation to be applied with relative ease. The Siemens autonomous driving solution announced[1] in March 2018 and covered enthusiastically by various trade publications, including *EE Times*, is one example of this approach.

The second V&V environment combines software and hardware to do hardware-in-the- loop (HIL), vehicle-in-the loop (VIL) and driver-in-the-loop (DIL) testing. In this environment, the amount of scenarios needed is lower (from thousands to hundreds of thousands), concentrating on a subset of the most critical scenarios that need to be validated.

The third and final V&V environment is done in emulated environments that represent a subset of real-life use cases. In this environment only a few dozens or hundreds of scenarios are tested, typically based on requirements set by regulatory bodies. When this final environment provides desired results, then vehicles should be ready to go on the road.

During each of the V&V environments, iterations will be done to gather results that are then used to apply design adaptations in software and hardware until requirements can be met. This covers the complete life-cycle development needed to have a streamlined, robust and fast automated vehicle development process.

Simulation

For the methodology to be successful, simulation must be scalable to handle millions of scenarios that are ultimately representative of reality. Simulation tools need to be able to provide the following:

- Realistic sensor simulation
- Realistic static and dynamic world models with annotated data
- Realistic occupant models
- Realistic vehicle models
- Robust cluster and test automation capabilities

At Siemens PLM we are working to provide an integrated tool-suite which encompasses all of the above mentioned items. Our autonomous solution announced this spring, part of the Simcenter portfolio, starts with TASS' PreScan simulation environment, which produces highly realistic, physics-based simulated raw sensor data for an unlimited number of potential driving scenarios, traffic situations and other parameters. The data from PreScan's simulated LiDAR, radar and camera sensors is then fed into Mentor's DRS360 platform, where it is fused in real time to create a high-resolution model of the vehicle's environment and driving conditions. Customers can then leverage the DRS360 platform's superior perception resolution and high-performance processing to test and refine proprietary algorithms for critical tasks such as object recognition and driving policy.

Ultimately, this tool-suite will also be coupled to product lifecycle management (PLM) environments (such as Teamcenter) and requirement management tools (such as Polarion).

Also important is that any design tools should be flexible enough to do simulation at different levels. Physics-based sensor simulation is absolutely critical to help advance the capabilities of automated vehicles, but a higher realism of sensor modelling results in an increase of computational effort. That is why our tools also provide more idealistic sensors that can be used when doing complete system tests in hard real-time HIL setups. Over time, with advances in graphic cards, artificial intelligence and general computing power, technology will become both accurate enough and fast enough to be used in all the necessary V&V environments.

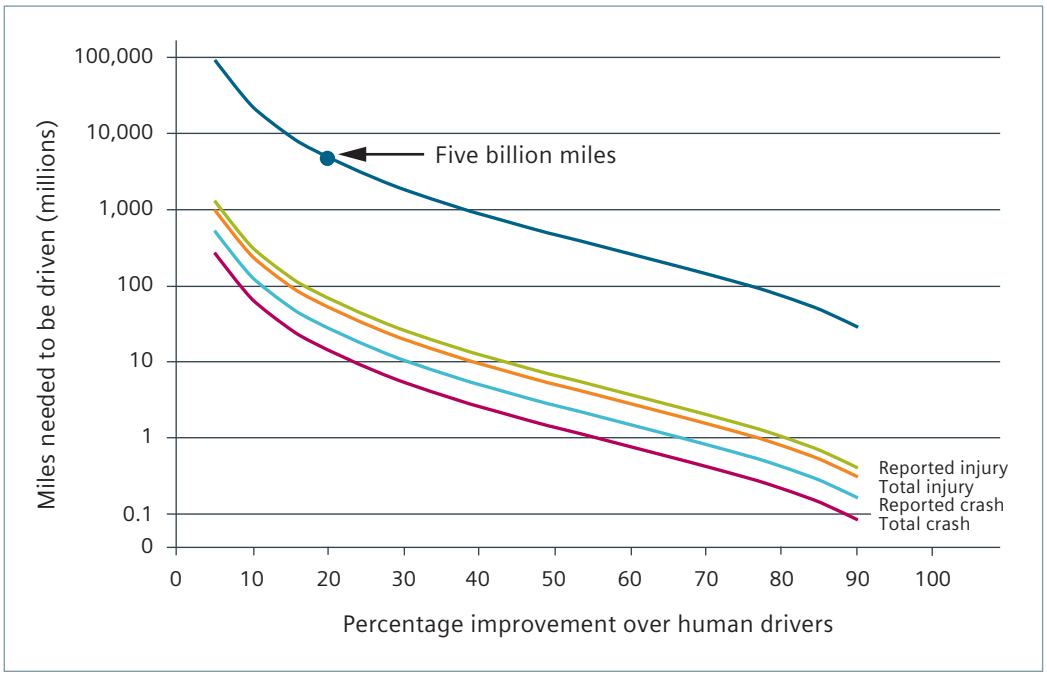

Figure 3: Data from a 2016 Rand Corporation report[2] showing the miles needed to demonstrate with 95 percent confidence that autonomous vehicle failure rate is lower than with human drivers.

Figure 4: PreScan screenshot; tool uses ray tracing to model a one-lane-change evasive maneuver.

Testing

Next, we come to testing. Despite the growing importance of simulation in the automated vehicle development cycle, this work will never be complete until a vehicle can prove its worth in real-life conditions in a real-world environment. We believe that this last step is highly complementary of simulation as is demonstrated by our various UNECE/EuroNCAP accreditations for verification and certification of ADAS and occupant safety systems. We use simulation before going to a test track, but at the same time, we use the results of our test track testing to improve the way that our simulation tools work. We believe that this testing philosophy will optimize the amount of time that vehicles need to be tested on the road while increasing overall test coverage. Additionally, virtual certification will be integrated into this process in the near future and become an integral part of testing for automated vehicles.

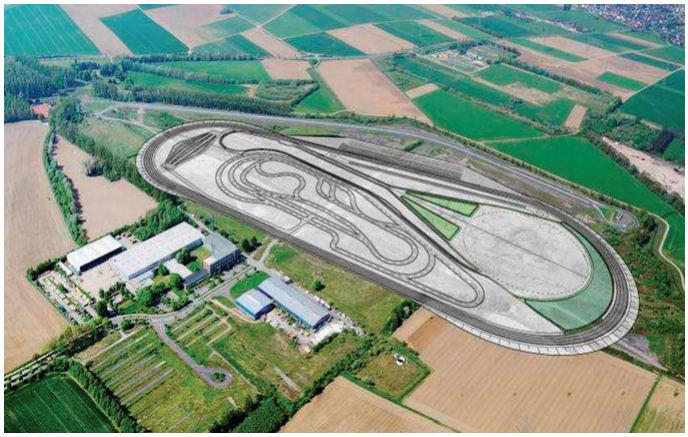

Figure 5: Aldenhoven Testing Center of RWTH Aachen University in Germany where TASS performs its ADAS tests.

ISO 26262

Any methodology for creating safe self-driving cars and systems will hinge on software, which as we all know is eating the world, according to Marc Andreessen, or at least firmly establishing itself as the most important input (besides the brains of the engineers) in the development process. So it's no surprise that there's not only pressure to deliver ISO 26262-compliant chips and systems, but also to demonstrate that the software tools used to create these electronic brains and sensory organs also meet the standard's requirement.

There's much noise in the IC electronic design automation (EDA) industry when it comes to functional safety programs and ISO 26262 compliance. We offer the follow three bits of advice when it comes to evaluating these claims.

1. Beware of EDA functional safety programs focused on the qualification of flows instead of individual tools Why? Simply put, EDA software is fundamentally a point solution market and functional safety programs based on ISO 26262 qualified flows can disguise weaknesses in the reliability of individual tools. The vast majority of chipmakers develop their own flows comprised of specific tools from different EDA vendors. So when EDA functional safety programs prioritize the qualification of flows consisting only of their tools, vs. qualifying each individual tool on its own merit, they are ignoring the reality of how chipmakers design their products with EDA software. Like a house of cards, removing even a single tool from a qualified flow can render a certified flow ISO 26262 non-compliant – unless a chipmaker adopts wholesale only one EDA firm's tools (which almost never happens). Better to stick to EDA vendors offering a tools-centric approach to ISO 26262, which allows chip designers to select the best tools for their design, with the confidence that each qualified tool can comply with safety standards on their own and without reliance on the larger flow.
2. This one is related, and it involves the term "Tool Confidence Level" (TCL). Despite rampant chest-beating in EDA press releases around TCL ratings, it's important to remember two key things (1) the goal of a software tool qualification is qualification – not TCL. TCL is merely a metric toward qualification. And (2) the ability for a tool to stand alone and be qualified as TCL2 or TCL3 – entirely independent of any other flows or tools in those chains – is what's key. Oftentimes a tool that's in a TCL 1 flow, is in fact, not a TCL 1 tool when extracted from a specific flow...again collapsing the house of cards. An alternative approach, and one recommended here, is to look for tools capable of standing alone, outside any flow, and supporting ISO 26262 compliance.
3. Be sure the EDA vendor stands behind its documentation. With each qualification of ISO 26262 compliance, the EDA vendor produces a software tool qualification report, including an executive summary of the classification and validation process, the results, recommendations, project-specific process measures and detailed information about the use of the tool. This documentation provides the EDA vendor's supporting evidence that that all necessary and required steps to secure ISO 26262 compliance have been met. This information is invaluable to chip designers, because it provides step-by-step instructions on exactly how their tools can be used to establish safety-qualified end products. But here's the thing: a careful reading of the "fine print" for too many EDA tool qualification reports reveals that in fact the customer is responsible for ensuring the evidence is accurate. The lesson here: read the fine print on qualification reports...if the EDA vendor doesn't have the confidence to stand behind its documentation and "show the work," consider walking away.

Beware of EDA functional safety programs focused on the qualification of flows instead of individual tools. Why? Simply put, EDA software is fundamentally a point solution market and functional safety programs based on ISO 26262 qualified flows can disguise weaknesses in the reliability of individual tools.

Conclusion

A robust V&V methodology and a smart approach to ISO 26262 compliance are key to the creation of L4/L5 automated vehicles, still an inevitability, despite the uncertainty of the current moment. Auto history buffs like to note that, despite dire warnings about government crackdowns and public revolt, when the first automobile fatalities started happening in the 1890s, nothing much happened. Speed limits were raised and for a time abolished, and even though the death toll climbed, innovation and sales accelerated faster still, transforming cities, economies and our way of life. There are any number of ways to interpret this basic reality, but one is that the utility and benefit of personal transportation is so great that society at large continues to make the calculation that trading away small bits of safety is worth it for the extraordinary advantages that horseless carriages or Teslas confer. (And it bears noting, too, that though the traffic fatality statistics today are sobering and unreasonably high, contemporary vehicles are also extraordinarily safe. In the United States, there is just over one death per 100 million vehicle miles – dozens of lifetimes of driving for most people.)

We believe that a V&V and test methodology needs to take into account requirements from various stakeholders while using a framework that allows the creation of a digital twin of the vehicle and the real world in advanced physics based simulated environments. Our goal is to make real the creation and adoption of L4/L5 automated vehicles by using this methodology. Through our existing validation and certification services, and our software tools, we believe that we can achieve this goal and accomplish our mission "to make real what matters." We're all excited about the future of automated vehicles, the dramatic reduction of traffic accidents, and the new opportunities that this automation will bring to society across the globe.

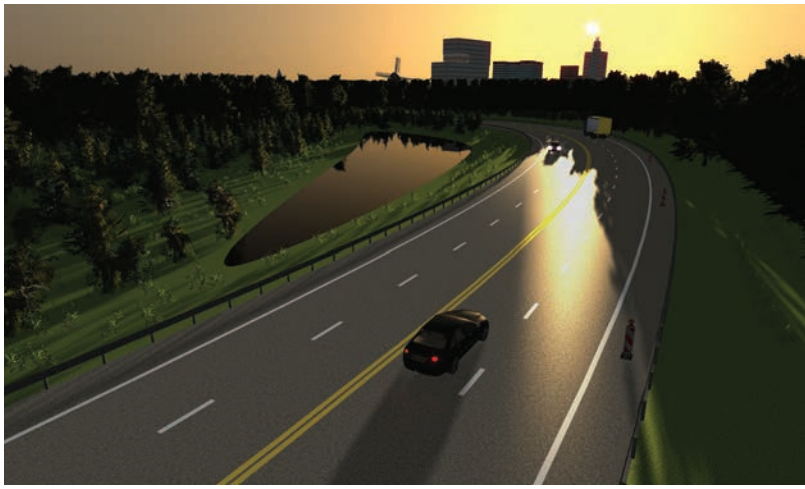

Figure 6: The American Center for Mobility in Willow Run, Michigan, as modeled in PreScan.

References

1. https://www.plm.automation.siemens.com/en/about_us/newsroom/press/press_release.cfm?Component=260639
2. https://www.rand.org/pubs/research_reports/RR1478.html

Siemens PLM 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
Suites 4301-4302, 43/F
AIA Kowloon Tower,
Landmark East
100 How Ming Street
Kwun Tong, Kowloon
Hong Kong
+852 2230 3308

About Siemens PLM Software

Siemens PLM Software, a business unit of the Siemens Digital Factory Division, 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, Siemens PLM Software works 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 Siemens PLM Software products and services, visit www.siemens.com/plm.

About the author

Andrew Macleod is director of automotive marketing at Siemens, focusing on the Mentor product suite. He has more than 15 years of experience in the automotive software and semiconductor industry, with expertise in new product development and introduction, product management and global strategy, including a focus on the Chinese auto industry. He earned a 1st class honors engineering degree from the University of Paisley in the UK, and lives in Austin, Texas. His previous whitepaper, "Being a Player in the Automotive IC Market," is available here: http://go.mentor.com/4ZlWv.
Follow him on Twitter@AndyMacleod_MG.

www.siemens.com/plm

70971-A8 7/18 C