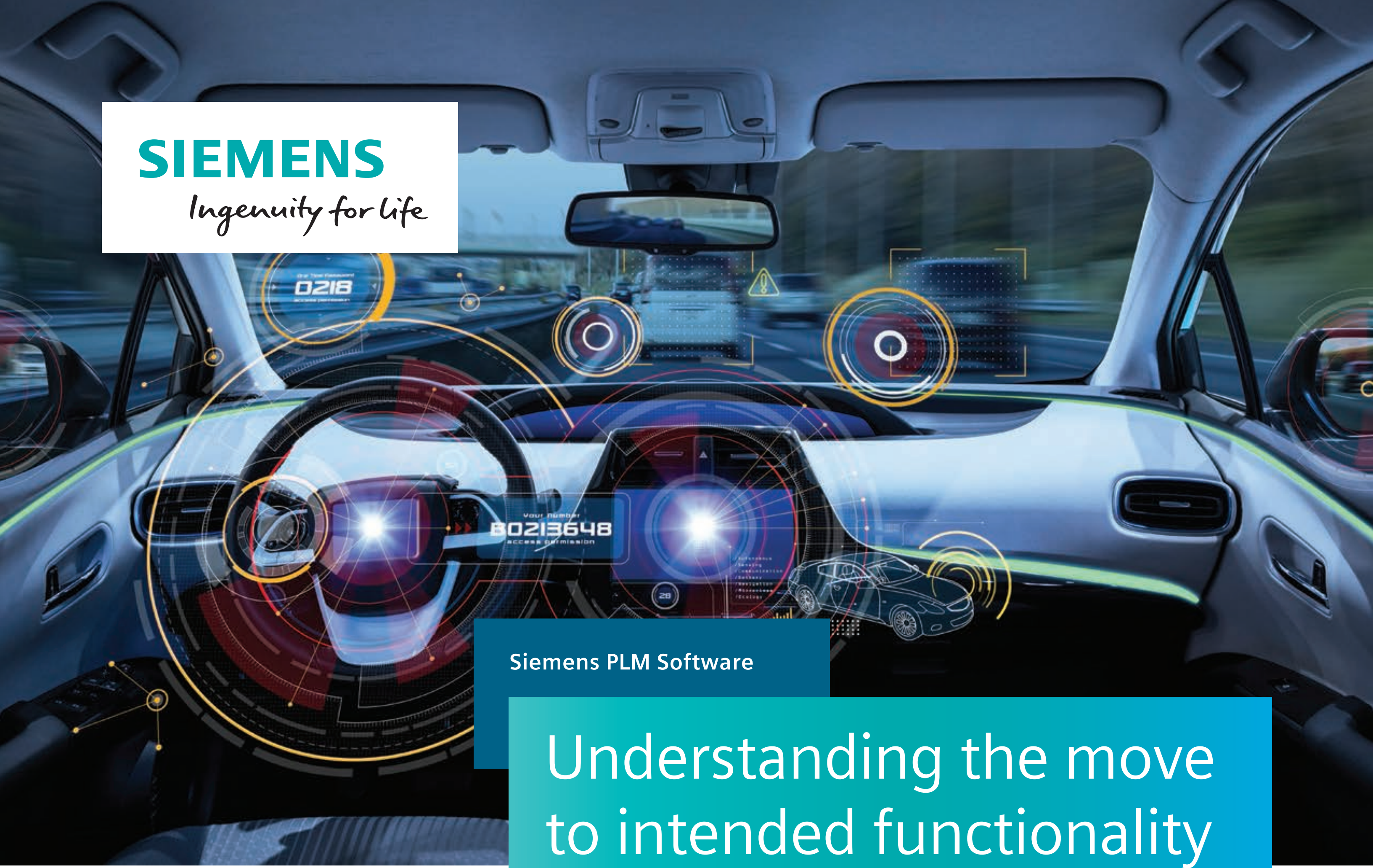


Siemens PLM Software

Understanding the move to intended functionality in autonomy

Executive summary

The autonomous revolution is disrupting the automotive market and bringing new opportunities to a range of actors, from automotive and tech companies to local and national governments. However, major challenges loom, including the certification of the safety of cars that increasingly think and act for themselves, even as they are more connected than ever to the internet. This paper briefly surveys the responses to these challenges from the global technical and regulatory communities. The paper was prepared for a September 2018 workshop convened by the Centre of Excellence for Testing and Research of Autonomous Vehicles – Nanyang Technological University (CETRAN), the Singapore Manufacturing Federation – Standards Development Organisation (SMF-SDO) and the Land Transport Authority of Singapore (LTA).

Joseph Dailey
Global Functional Safety Manager, Mentor product suite

Gwen Van Vught
Director of the Mobility Center, TASS International, a Siemens Business

Ajinkya Bhave
Engineering Manager, Siemens Industry Software

www.siemens.com/simcenter

Vehicles are famously morphing from purely mechanical horseless carriages to software-driven computers on wheels. As electronics have taken on an outsized role in designing and building cars, the engineering community has responded as it always does, by adopting standards, including ISO 26262, 21448, 21434 and J3061. All of these are regular fare in articles and op-eds in the industry trade press. "With specs like ISO 26262,...a big burden goes onto you developers to show that what you've created is safe," wrote Bryon Moyer, in an August 27, 2018 article in *Electronic Engineering Journal*, in effect summarizing the demands of most standards grappling with autonomy.

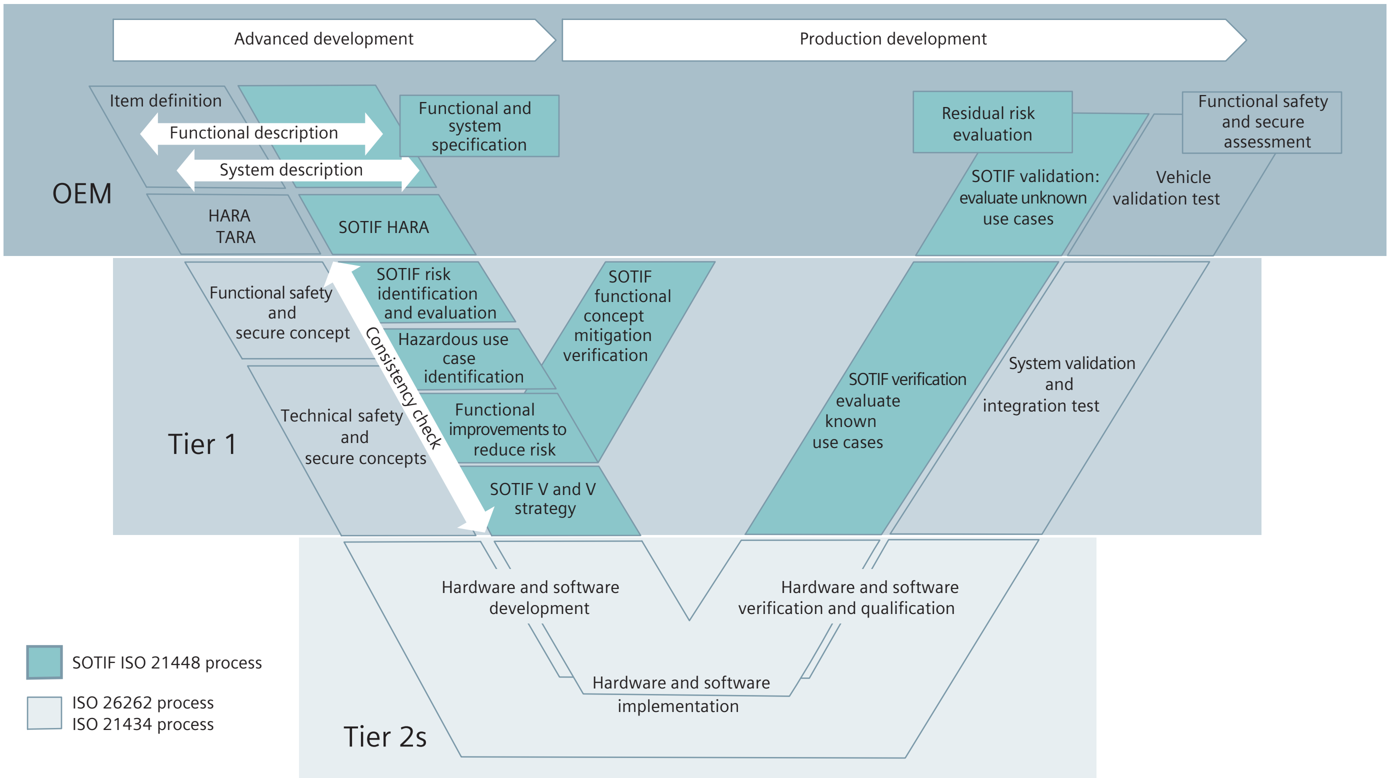
For the uninitiated, here is a brief summary of these standards.

ISO 26262, which covers the functional safety of vehicle electrical and electronic systems, dates to November 2011. The standard covers all parts of the product lifecycle, from requirements management and planning through manufacturing and testing. It also has transformed organizational safety cultures, which now often require that everyone from company president to line engineer participate in ISO 26262 training. While it defines how to conduct critical analysis and helps establish engineering best practices, ISO 26262 of late has run into challenges thanks to the rise of nondeterministic, artificial intelligence (AI) systems. In such systems, with underlying algorithms that teach themselves, the straight-through line from input (such as vehicle sensor data) to output (like a given driving decision), is broken – a major hurdle to the if/then-type testing at the heart of ISO 26262 and indeed most engineering testing practices.

Other standards relevant to autonomy concern cybersecurity, a major topic for all connected devices. The global cost of cybercrime is now $600 billion annually or 0.8 percent of global GDP, according to cybersecurity firm McAfee. In announcing the Mcity Threat Identification Model in early 2018, University of Michigan mechanical engineering professor Huei Peng said: "Without robust, fool-proof cybersecurity for autonomous vehicles, systems and infrastructure, a viable mass market for these vehicles simply won't come into being."

The standards to watch here are J3061, a guidebook of best practices from SAE International published in 2012, and the in-development ISO/SAE 21434, which will include a list of specifications and requirements for

The ideal remains to approach fully autonomous Level 5 driving that is hands-free in all scenarios.



How the SOTIF ISO 21448 might enhance the v-cycle of hardware and software development and verification.

cybersecurity components and interfaces, and govern activities such as engineering, production, operation, maintenance and even decommissioning of connected components. A final version is expected in late 2019.

A major question today is how to combine existing best design practices and simultaneously adopt new design and testing techniques required to build ever more advanced autonomous vehicles. One response to this question is ISO 21448, currently under development. ISO 21448 attempts to outline how to deal with Safety of the Intended Functionality (SOTIF) of the electronic guts of self-driving cars. The standards committee is trying to cast a wide net – the better to deal with all the electrical and mechanical systems coming from an increasingly diverse supply chain. The standard will outline a long list of scenes, scenarios and triggers that in some combination invoke a human and AI response “behind the wheel.” It is very much a work in progress and even when the standard is eventually published, ISO 21448 won’t answer all or even most of the safety questions about AI-powered vehicles. However, it will provide a defined roadmap to get to a Level 2 autonomy.

Of course, the ideal remains to approach fully autonomous Level 5 driving that is hands-free in all scenarios. Getting there requires innovation at each stage of the product lifecycle, from concept to design to manufacturing to testing. And most of all, its hinges on establishing trust with the public at large that a vehicle can truly think and react like a human – or rather, that a vehicle can respond 10 to 100 times better than a human in all circumstances.

Implications of AI

The quest for full AI control may well redefine who sits atop the auto industry. “Automakers always owned the ‘secret sauce’ of the vehicle,” says Tom Mayor, Industrial Manufacturing Strategy Practice Leader at KPMG, in a November 2016 report. “But with deep learning, somebody else has it, and for car companies to control the algorithms driving the vehicle, they will need the people who design them. The problem is, deep learning specialists are not exactly flocking to the auto industry.”

Indeed, talent is the new arms race, for startups, global companies and even governments. The reality is there are precious few people capable of building advanced AI systems. In the auto industry, the major effort today is how to combine deep reinforcement learning systems, AI and real-world data in closed-loop simulations. For now, this is about creating a list of discrete, small-scale scenarios and responses by hand, then running these through a neural network, which learns the correct response. Once this learning is complete, the network can be given more complicated scenarios requiring more sophisticated decision-making.

Eventually, the goal is to go beyond vehicle subsystem and full-vehicle simulation to bring in even city-scale data, which is possible given the ongoing effort to instrument and digitize everything. The algorithms can be optimized for this more robust dataset, corresponding both in closer detail and at a larger scales to the real world. Then the systems will get smarter still by tweaking parameters of all this real-world data to begin simulating and learning about unexpected corner-case events. At Siemens and elsewhere, researchers are not only extracting data into scenario databases, but also starting to perform statistical analysis of parameters to begin testing these unknown scenarios in a disciplined, mathematical way. Completing such a testing regime on test tracks and public roadways would take many billions of miles and likely permanently forestall the development of truly hands-free driving.

"Automakers always owned the 'secret sauce' of the vehicle. But with deep learning, somebody else has it, and for car companies to control the algorithms driving the vehicle, they will need the people who design them. The problem is, deep learning specialists are not exactly flocking to the auto industry."

Tom Mayor, Industrial Manufacturing Strategy Practice Leader at KPMG

Singapore at night. The city-state made news in summer 2018 for building a dedicated town for testing self-driving buses. Today's wide-open regulatory environment presents an opportunity for many jurisdictions and countries, but this will not last long.

Screenshot from the 2018 Siemens on-demand webinar, "Designing autonomous vehicles for series production." See https://youtu.be/fdifp6G38ak.

Even in the most optimistic scenarios, roadways with Level 5 autonomous vehicles in large numbers are still far in the future. The likely reality will be a decades-long interregnum where humans and machines share the driving task. The AI-to-human handoff is fraught, though the outlines of the new mode of driving are already apparent today. AI will drive the vehicle until encountering a situation beyond its ken, then will give control to the human driver, maybe after a deterministic safety layer slows down the vehicle and pulls over to the side of the road. This is good news from the testing point of view, as the rigid if/then safety layer conforms nicely to the traditional verification approach in automotive, which has proven remarkably effective through the years in boosting vehicle safety. Look for methodologies that comprehend this reality – AI systems switching to a highly deterministic mode that executes a safe action when specific safety scenarios are encountered.

Regulations (or lack thereof)

How will the industry certify the safety of these systems to governments? This is a huge topic today. Just because a company reports some combination of millions of actual and billions of simulated miles, that doesn't guarantee the safety of their vehicles. It seems inevitable that there will be varying requirements for confined operational design domains (ODDs). And each set of these requirements likely will require loads of data around disengagements, much as are reported today in the California DMV's disengagement reports, which are pored over by the press. Part of such a hypothetical requirement could be that the system is not deemed safe if it exceeds one disengagement per 10,000 miles in a given ODD. In the California data, currently Waymo has the lowest rate at 0.18 disengagement per thousand miles, while the next closest is Cruise Automation at 0.8 disengagements per thousand miles.

The disengagement data is just one example of how the industry is attempting to regulate itself while innovating, a dance unfolding against a backdrop of uncertain but sure-to-come government regulations. One of the signal issues in recent years was the 2016 decision of the U.S. National Highway Traffic Safety Administration to declare that the computers controlling an autonomous vehicle are the same as a human driver. The announcement generated headlines globally and also perhaps created more questions than it answered.

Notably, it was an endorsement, explicit or otherwise, of Google's proposal to create a human-out-of-the-loop self-driving car without controls like a steering wheel, brake or accelerator.

"At this point, researchers admit that they do not completely understand how the deep learning networks make decisions."

John Markoff, New York Times science and technology reporter

In covering the story, veteran New York Times science and technology reporter John Markoff outlined the ongoing uncertainty, which if anything is more pronounced today, due to ongoing advances of hardware and software technology:

> The legal challenges that artificial intelligence will pose have become more complex as technology has advanced. It was once fashionable to say that the machines would only do exactly what they were programmed to do. And if the human programmer made an error, such as misplacing a decimal point, that would be expressed in some incorrect behavior on the machine's part.
>
> However, recent progress in artificial intelligence has largely been made with so-called deep learning algorithms. This is a branch of machine learning that is based on software composed of multiple processing layers, each with its own complex structure. The programs are "trained" by exposing them to large data sets. They are then able to perform humanlike tasks, such as categorizing visual objects and understanding speech.
>
> At this point, researchers admit that they do not completely understand how the deep learning networks make decisions.

Governments, and indeed all of us, should keep in mind lessons from the airline industry, which has moved to almost complete fly-by-wire systems. When automation appeared on the horizon in aerospace, there was a concerted effort to certify as much as possible about the new systems. Safety eventually did improve, yet along the way there were many near-misses and a handful of well-publicized crashes as everyone, engineers to pilots, learned the reality of the new systems. Even one unnecessary death is too many, though inevitably lives will be lost as new forms of vehicle automation take hold. Given the current data on vehicle accidents globally (1.3 million deaths annually, and as many as 50 million people injured or permanently disabled), the key is remembering the potential to save vastly more lives.

As autonomous development continues apace, safety is everyone's utmost concern. Ongoing work to bring multiple standards together must account for the eventual ascendance of nondeterministic AI algorithms that in the near term will be buttressed by highly deterministic (and thus more easily verified) safety layers. And yes, eventually the industry will be constrained by mandatory government regulations. At present, today's wide-open regulatory environment presents an opportunity for many jurisdictions and countries, but this will not last long. Playing an outsized role in spurring development of what will be one of the most transformative technologies of the last 100 years means chip- to city- and even country-scale considerations for everyone, engineers and government officials alike.

As complexity mounts, so do the stakes for carmakers and their suppliers to bring functionally safe hardware and software components together across a product lifecycle and supply chain. Despite the promise of autonomy, no population (and thus no government), will accept even the perception of an unsafe self-driving car, let alone the reality of one.

References

Siemens report (July 2018), "Cities in the Driving Seat Connected and Autonomous Vehicles in Urban Development," https://sie.ag/2Mb29VT

Rosenberger, Peter (July 9, 2018), "Singapore: The world's smartest nation by 2030?," The Magazine (a Siemens publication), https://sie.ag/2NUxIEV

Lauzun, Dave (June 28, 2018), "Designing Autonomous Vehicles for Series Production: On-demand webinar," https://youtu.be/fdifp6G38ak

Goncalves, Manny (November 22, 2016). "Deep Learning & Autonomy Will Accelerate The Birth Of A New $1 Trillion Autonomous Mobility Services Market: KPMG Report" (Press release.) KPMG http://bit.ly/2Qamj5j

Markoff, John (February 10, 2016), "Google Car Exposes Regulatory Divide on Computers as Drivers," New York Times (https://nyti.ms/1XjkX5u)

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
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 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.

www.siemens.com/plm

73863-A7 9/18 C