THE HANSEN REPORT
ON AUTOMOTIVE ELECTRONICS

This article first appeared in the February 2017 issue of The Hansen Report.

Standardization Efforts on Autonomous Driving Safety Barely Under Way

How Safe Is Safe Enough?

Among all of the topics I cover for the *Hansen Report*, none is as widely discussed as autonomous driving, a hugely challenging requirement that is likely to upend today's E/E architectures, if not the automotive industry, as new players such as **Waymo**, **Apple** and **Uber** enter the market. As cars take over the driving, first on highways and in controlled, low-speed settings, and some years later in unrestricted urban settings, the liability for injury and death resulting from accidents will increasingly fall on carmakers and ride-service providers. Carmakers are thinking long and hard about how best to build safety-critical systems that are sufficiently robust. They have to be fault tolerant, meaning they don't fail completely but continue at a reduced level. And when they fail they "fail operational," meaning the system continues to operate to bring the vehicle to a safe stop.

"Robust design methods are not at all new to automotive electrical engineering," said Scott Morrison, engineering group manager at **General Motors**. "Airbag designs, drive-by-wire solutions, electronically controlled steering and braking all must be fault tolerant and robust. But now as we journey to full autonomous, more and more systems will have functional safety requirements."

And while GM is addressing these functional safety matters on its own, Mr. Morrison is supportive of efforts to collectively address the safety risks associated with autonomous driving, "whether it's process standards like ISO 26262, or generating common test standards or pushing the industry forward in a harmonious fashion. This will give all of us a common foundation on which we can work. We can differentiate on top of that."

Still, according to Kai Barbehön, vice president of product offering, E/E and software architecture at **BMW**, there will be limits to how much

carmakers will be willing to work collaboratively. “With PEGASUS we are looking at concepts for requirements and validation methods. On the other hand, we see that it will be a competitive advantage if someone can offer autonomous systems faster than others. Not everyone is open to getting into common discussion about how it should work.”

Here is a roundup of some of the collective efforts under way.

PEGASUS

In January 2016, the German OEMs began the PEGASUS research project, a 34.5 million euro, 149 man-year project to answer two main questions about automated vehicles: “How safe is safe enough? Then, how can we prove that our technology fulfills that requirement?” explained Thomas Form, who is responsible within **Volkswagen Group Research** for electronics in the vehicle, which includes everything except powertrain. He is one of two coordinators of the project.

To consider the question how safe is safe enough, Dr. Form cited a presentation at CES 2017 by Gill Pratt, who heads the **Toyota Research Institute**. As reported by *Automotive News*:

> [Dr. Pratt] noted that while human beings, tolerant of human error, have come to accept the 35,000 traffic deaths every year in the United States, he went on to ask if people could accept even half that number of deaths caused by robotic automobiles. “Emotionally, we don’t think so,” said Pratt. “People have zero tolerance for deaths caused by a machine.”

“We asked this question in Germany two years ago,” said Dr. Form, “and realized that we, the automotive industry, did not have an answer and that we have to bring together all stakeholders from ministries, transport organizations, OEMs, tier ones and test authorities to find a suitable answer, because there will not be a 100% perfect system on the road in the future.”

Proving that technology is safe enough is not a simple matter. “On German highways you can drive well above 200 million kilometers between two accidents with fatalities. To provide proof that a robot can at least drive better than a human driver you would need billions of test kilometers. It would take thousands of vehicles dozens of years to do this,” explained Dr. Form. “So we must find an acceptable process using

hardware in the loop and software in the loop simulation and verification that could be accepted as proof that the technology for autonomous driving is safe."

The project has established automatic driving on the highway as the functional example it will research. The next step, determining the typical capabilities of human drivers on highways, will be complete next month. From there the project will derive the requirements needed for an autonomous vehicle that at least drives as well as a very good human driver. The project is also trying to create a framework of simulation test scenarios which can in the future be used to prove this capability.

The PEGASUS project is scheduled for completion on June 30, 2019. The Germans are already thinking about creating a successor project that would be based on the available results of PEGASUS and look into autonomous driving in the urban environment. That project would start in 2018.

Dr. Form is hopeful that projects similar to PEGASUS will be set up in the U.S., Asia and elsewhere in Europe, "because in the end we should have a standard set of requirements accepted worldwide." A workshop is scheduled for October 19-20, 2017, at a location yet to be determined. Elmar Frickenstein, senior vice president for fully automated driving and driver assistance at **BMW**, noted, "The need for an international collaboration should be discussed within this PEGASUS international workshop."

ISO 26262 Next Editions

Work on the second edition of ISO 26262, the Road Vehicle Functional Safety Standard, has been underway since 2015. A draft of the standard is now publicly available, but it doesn't address the fault tolerance and fail operational requirements associated with SAE Level 4 or Level 5 automation. And further, it only partially addresses Level 3, which calls on the human driver to intervene as needed.

Riccardo Vincelli, manager of **Renesas**' Functional Safety Competence Center, has been personally contributing to ISO 26262 since 2005. "The second edition covers only the technical issues associated with the system's availability. It doesn't cover controllability, which is a human issue. How quickly can the driver react? There is also the question of attendant liability. Who takes on liability if the driver doesn't react quickly enough?"

The ISO work group is on a path to consider autonomous driving and the fail operational requirement, but the real work won't start until after the second edition is completed in 2018 or early 2019. "The third edition won't be done until 2022 or 2023," cautioned Mr. Vincelli.

"The current ISO 26262 second edition is far away from adequately dealing with the fail operational and fault tolerance topics," concluded Christof Ebert, managing director for **Vector Consulting Services**.

Renesas' Mr. Vincelli provided a list of some other ongoing standardization activities.

- SOTIF (Safety of the Intended Function) is a workgroup under ISO. Its specification is expected to be published toward the end of 2018. Nicolas Becker from PSA leads the workgroup, which includes considerable representation from several international companies.

- IEEE P2020 Standard for Automotive System Image Quality Working Group started at the end of 2016. Its goal is to define a standardized suite of objective and subjective test methods for measuring automotive camera image quality attributes for ADAS. More information is available from the IEEE Standards Association.

- The SAE Functional Safety Committee wrote Recommended Practice J2980, *Considerations for ISO 26262 ASIL Hazard Classification*. The group is now looking at what further work is required and meets regularly, a few times per year.

- The SAE Automotive Internet of Things Steering Committee started last year with some initial discussions. Activities are expected to resume this year. This committee could become relevant for autonomous driving. ◆