OPERATIONAL SAFE SYSTEMS

September 25-27, 2018
Berlin, Germany

THE STATE OF FUNCTIONAL SAFETY

2018 REPORT

INTREPID DELTA

2018 SURVEY REPORT

THE STATE OF FUNCTIONAL SAFETY

Survey by Intrepid Delta | www.intrepid-delta.com

68%

says it's acceptable that machines make mistakes as long as it's not life threatening.

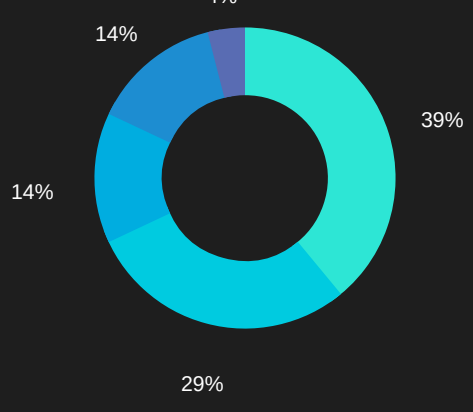
64%

believes even if autonomous cars aren't perfect, they should be allowed on the road.

25%

still believes we should put autonomous cars on the road to enable improvement, even if they perform worse than the average human driver.

There is currently no proven way to test autonomous vehicles safety prior to being on the road. In your opinion what is the most promising method?



39% Existing functional safety standards (ISO 26262) can provide assurances of safety together with further adjustments

29% Testing in Partial Simulation: Hardware and sensors will operate in shadow mode

14% Extensive test drives in real traffic

14% Real-World Driving Experience: this approach enables autonomous vehicle performance

4% Other

96% Thinks that security of safety is very important and it should be treated together.

93% Considers the question of liability as a challenge for the automotive industry.

Where do you see the main challenges with regards to realizing safety?

Semiconductors, cyber security and safety measures in autonomous driving

From Fail-Safe to Fail-Operational

The most exciting and promising aspect of the automotive industry today is without a doubt autonomous driving. With an extremely complex combination of sensors and actuators, sophisticated algorithms and powerful processors to execute software, the industry continues making dramatic improvements in bringing self-driving cars closer to entering roads in the near future.

IF 100% PERFECTION IS CURRENTLY IMPOSSIBLE TO ACHIEVE, WHICH LEVEL OF SAFETY IS ACCEPTABLE FOR AUTONOMOUS CARS TO ENGAGE IN ON-ROAD TRAFFIC?

If we look at statistics, the automotive industry has, in the last two years, moved up to become the most important market for semiconductors. With advanced features added to cars yearly, electronic components that are necessary for the safety, comfort and convenience of these features have been on the rise. As the focus of the industry shifts towards autonomous vehicles, vehicle-to-infrastructure communications and on-board safety, the demand for electronic systems required for these systems to function safely has brought along an equal increase in the need of semiconductors per vehicle.

In fact, the demand for semiconductors in cars has become so high, that it has slowly pushed out computers as the industry that has been the biggest market for chips for so long. Today, market research studies show that, starting in 2016, the automotive industry will stay on top of this list as the strongest market for semiconductors all through 2021, with a CAGR (Compound Annual Growth Rate) of 5.4% per year.

THE STATE OF FUNCTIONAL SAFETY

Systems safety, monitoring control and autonomous driving are currently causing the highest demand for semiconductors in the automotive industry to date. According to IC Insights, the recent focus turning towards autonomous driving and all related components required for its life cycle will bring the automotive IC market to a record in the last three years, reaching $32.3 billion in 2018. The momentum is forecasted to run through 2021, with an annual growth rate of 12.5%, ultimately reaching $43.6 billion in 2021.

However, despite all the progress we have witnessed so far, the major point of concern remains in the field of safety. Focus has been steadily turning towards determining strict guidelines that will encompass both hardware and software components throughout the life cycle of autonomous vehicles. Providing experts with a strict set or safety regulations, ISO 26262 standard is guiding the way, yet the fact that it needs constant updating to make sure it keeps up with all the latest developments has raised some important questions regarding software safety and cyber security.

As a result, this year's Operational Safe Systems is dedicating an entire day to the topic of semiconductor safety and reliability. ISO 26262 standard has been the industry's main guideline in an effort to avoid malfunctions that could compromise safety and performance of self-driving vehicles. Aimed at providing a strict list of requirements needed to build chips that meet the rigorous standards and guarantee fault-proof systems, ISO 26262 relies on a ranking scheme called ASIL.

The ISO 26262 standard is constantly updated, and we have dedicated the first talk of the day to the review of the latest version and its current status. The standard's overview will be followed by a discussion on system-on-chip development, HW and SW components design requirements, verification, validation and testing, as well as FIT rate calculation. In addition to that, we will demonstrate a framework for the development of ad-hoc, native solutions for the enablement of high coverage, ASIL compatible STL, with the goal of providing support for reaching HW architectural metrics targets in accordance with ISO 26262.

We will also take a closer look at challenges in the field of safety analysis for semiconductor components, such as pros and cons of performing safety analysis at concept vs implementation levels and implications when targeting different ASILs. From there we will move on to discuss diversity as a commonly used tool in functional safety, observing it as part of an ASIL decomposition or as redundancy at the algorithm level to improve SOTIF. Ultimately, the conference will focus on the inevitable question of: How much diversity is enough?

Moving into computing architecture, another important topic that will be addressed is rooted in determining the best architecture for the autonomous car observed from the perspective of functional safety. With cloud infrastructure becoming one of the key parts of the entire process, the importance of cyber security has joined the safety related concerns as one of its key points of concern.

Cloud infrastructure remains potentially vulnerable to hackers, opening new gateways for compromising safety of sophisticated car features, potentially disrupting the system that controls the entire vehicle. We recognize the importance of cybersecurity and its relation to semiconductors, which is why we are dedicating the last talk of the day to the topic of automotive cybersecurity considerations for semiconductors.

For more information visit www.operational-safe-systems.com or send an email to klaudia.malowitz@intrepid-delta.com.