Operational Safe Systems for Automated Driving

From Fail-Safe to fail-operational

As the automotive industry advances in the field of autonomous driving, it is simultaneously encountering a rising number of safety and security related challenges. Without an existing and reliable way to test and prove the safety levels of autonomous vehicles prior to their entering roads, both manufacturers and researchers are currently facing functional, legal and ethical issues. And if operational safety of a system behind an autonomous vehicle is imperfect, the key question that needs answering becomes:

If 100% perfection is currently impossible to achieve, which level of safety is acceptable for autonomous cars to engage in on-road traffic?

In addition to that, the sophistication of security systems is being brought to a new level – one that has a strong impact on the safety of these vehicles. Consequently, previously mentioned challenges must be united with those that accompany the correlation between security and safety. This introduces a second set of issues that the autonomous driving industry is facing today: *How connected is safety to security and should these two components be treated simultaneously?*

Operational safety for autonomous driving

Operational safety intends a status of failure-free operation of all elements included. An introduction of risk-reducing measures to the existing system components directly influences the level of operational safety of an autonomous vehicle. Key components involved in this process include mechanical, electrical and software safety. The goal of manufacturing, testing and releasing onto the road a self-driving vehicle that is perfectly safe has proven to be a rather utopian one for the time being.

Here is why. To prove that such a car is fully independent of the human factor while fulfilling rigorous safety requirements when on the road, manufacturers would have to spend decades collecting the billions of miles necessary for such a proof. Current testing methods, such as extensive test-drives in real traffic, testing in partial simulation and functional safety standards like ISO 26262 cannot provide enough proof of the vehicles' safety. On the other hand, placing an imperfect vehicle on the road would pose serious liability issues in case it causes harm to its driver, passengers or other collateral victims. The third question in the quest for a safe-enough autonomous vehicle then becomes: *Is it possible to create a robust design for autonomous vehicles that would satisfy the rigorous safety requirements for urban settings?*

Car manufactures are getting closer to developing safety-critical systems that would provide a level of safety with a satisfying level of robustness. Failing of operational systems inside these vehicles must be controlled to a certain extent, which is the main principle behind the "fail operational" function that enables the vehicle to continue operating safely until it has reached a full stop. Most safety related components of today, such as air-bags and braking systems,

satisfy the required level of robustness. However, as car manufacturers continue advancing towards the development of fully autonomously-operated vehicles, more systems are being added to the list of functional safety requirements. This is why, in an effort to provide a standard for safety features, the automotive industry has developed the ISO 26262 Road Vehicles Functional Safety Standard based on IEC 61508. The certification of those systems ensures compliance with the relevant regulations and helps protect the public from harm should the safety system fail to perform.

With a particular focus on the automotive development cycle, ISO 26262 is a multi-part standard that defines requirements and provides guidelines for achieving functional safety in E/E systems installed in series production passenger cars. The standard ISO 26262 is considered a best practice framework for achieving automotive functional safety. However, the compliance process tends to take a long time, given that employees need to undergo thorough training processes to develop the expected competences.

The current ISO 26262 standard, widely used throughout the automotive industry, is today facing challenges in an effort to keep up with the advancements in the development of a fully autonomous operating vehicle. The second edition of ISO 26262 has already been drafted and is available to the public. However, it is yet to address controllability and how it correlates with the human factor, as it still only addresses the technical issues of the system's availability.

Recent developments in the autonomous driving safety and security regulations are priority in the automotive industry, and The German Federal Ministry for Economic Affairs and Energy has been supporting the PEGASUS research project since 2016. The project involves experts from both the automotive industry as well as top research institutes.

The main goal of this joint research is to provide advancements in the safety systems of autonomous cars, ultimately improving satisfactory rates related to safety systems. Scheduled to be over by the end of June 2019, the program aims at answering all the key questions related to the acceptable levels of safety and the systems used to determine these requirements. Should the project run successfully, it is expected to set in motion the release of highly-automated driving functions, which should further improve their safety on the road.

Collaboration as the key to success

Developing robust systems behind autonomous vehicles is a complicated task. The PEGASUS project is therefore divided into four subprojects that are being rolled out in parallel. From predicting and simulating potential scenarios that would trigger safety measures, through developing new testing processes that would shine a light on the specifics behind the human-machine interaction in driving conditions, the actual testing phase and, finally, to the revision and embedding phase. These four subprojects would ensure that the processes developed within the PEGASUS project are safe for implementing to higher levels of automation within car manufacturing companies.

This project is expected to be followed by a successor-project, currently in its planning stage. Meanwhile, PEGASUS is planned to widen its scope, as it is introduced to Asian, US and other European markets. Involving all major research institutes as well as car manufacturers, this project is based on full collaboration with the aim of optimal results achievement.

It must also be noted that, although potentially eliminating the competitive advantage of car manufacturers, the collaboration between manufacturers and researchers will provide the fastest and most efficient method for achieving safety related goals in autonomous driving systems. Pioneering robust safety systems is a valuable advantage for car companies, but the priority is elsewhere. If safety comes first, then all industry relevant experts must join forces to ensure a safe and secure future of autonomous driving.

The correlation between safety and security

As technology matures and creates sophisticated features, such as hands-free voice communication systems, cars are becoming smarter and more connected than ever. As digital technology steps deeper inside the automotive industry, it opens the door for possible hacks and malware. Consequently, security in connected cars, whether autonomous or not, has been gaining more recognition over the last years.

Security has become a key element in keeping cars safe from hacks and viruses, but the impact it has on the car's safety shouldn't be neglected either. As more responsibilities are handed over to these smart controls, more risk inevitably follows. Failure of a security feature can cause major safety issues. Security and safety must therefore be treated, researched, tested and improved together as they have a direct impact on the security and safety of the driver and passengers respectively.

To help bridge this gap and support innovation in all stages of the lifecycle of autonomous vehicles, the upcoming Operational safety and security event taking place in Berlin on September 25 – 27, 2018. is focusing on the topics of safety and security, as well as how they are connected in the overall safety systems inside autonomous vehicles. Introducing the latest addition – a full day dedicated to the topic of semiconductors with focus on safety and security challenges of semiconductor components.

As innovation within the automotive industry advances, the need for complex semiconductor devices increases. However, these devices are currently only available in consumer grade quality. To accelerate AE technology, the entire automotive value chain must work together to reach this goal. Cooperation is the key element required to develop systems for smart mobility and infrastructure, ultimately resulting in a smarter, safer and more secure future for the car industry.

With support from leading OEMS like BMW, Audi, Daimler, Tier Ones such as Bosch, Continental, ZF and Hella as well as renowned research institutes, we bring the right people together to unlock expert knowledge exchange and support safety and security systems

advancements. For more details visit https://www.operational-safe-systems.com/ or send an email to klaudia.malowitz@intrepid-delta.com