SAFETY CONSIDERATIONS FOR A CLOUD SERVICE FOR AUTOMATED DRIVING

OUR COMPETENCIES AND SOLUTIONS

- Safety analyses and safety concept development
- Safety standards and initiatives for the development of such standards
- safeTbox – tool framework of Fraunhofer IESE providing support in phases of safety-critical systems development and certification

THE CUSTOMER BENEFIT

- External view on cloud services for vehicles with higher levels of automation
- Transfer of the results of current discussions in research and industry as well as future safety standards into the customer’s process

WHAT IT IS ALL ABOUT

In the future, automated driving will be increasingly supported by cloud services: A vehicle’s sensor system only has a limited range and is expensive, which is why in the future, vehicles will be supplied with information through the cloud. This information may stem from other vehicles, but also from other sources such as weather service providers.

This project with Bosch was also about a cloud service: This service informs the highway pilot about the road conditions and the static friction coefficient of the road surface. Highway pilots are dependent on this information, as their range of use and their driving behavior depend on this friction. Developing a safety concept for this cloud service – despite the lack of standards regarding safety issues in the automotive field – was the challenge for the experts of Fraunhofer IESE.
THE CHALLENGE

To date, no standard exists yet that would explain how to develop cloud services for highway pilots. The safety standard ISO 26262 and the Safety-Of-The-Intended-Functionality (SOTIF) standard ISO PAS 21448 relate to vehicles, but their application is not easily transferable to cloud services. IT safety standards do address cloud services, but not the safety issues from the automotive field.

However, just because there is no standard does not mean that you can develop such services any way you want. One should still adhere to the state of the art, even if this is not found in one single standard.

THE SUPPORT

The researchers of Fraunhofer IESE are familiar with the state of the art as well as with current developments in the area of safety and automated driving. Based on this background knowledge, they put together relevant requirements from standards in this project with Bosch and demonstrated how to implement these methodologically.

In addition, Fraunhofer IESE supported Bosch in the methodological implementation. In close cooperation with the domain experts from Bosch, they developed a functional architecture that represents the entire information processing. Next, the team analyzed individual processing steps with component fault trees. They also performed a safety analysis of the cloud platform on which the software developed by Bosch is running. Based on the results of this analysis, the Fraunhofer experts derived a safety concept and developed a safety argumentation using the Goal Structuring Notation (GSN). They modeled all artifacts with safeTbox, the tool framework developed by Fraunhofer IESE for support in phases of safety-critical systems development and certification. Due to their modular nature, the modeled artifacts can be easily adapted to different customer demands.

THE RESULT

As the result of this project, Bosch received a comprehensive safety concept for its dedicated cloud service. However, the approach and the methods and tools used are easily transferable to other cloud services. Hence, the project also yielded a model-based safety engineering approach for cloud services and forms the foundation for a standard that is still missing as yet.

Contact

Dr.-Ing. Rasmus Adler
Program Manager Autonomous Systems
Phone +49 631 6800-2172
rasmus.adler@iese.fraunhofer.de
www.iese.fraunhofer.de
www.bosch.de

The cooperation with Fraunhofer IESE was groundbreaking for us in terms of the safety engineering of our cloud services. The model-based analysis techniques enabled us to systematically examine the entire chain of action from the sensors via different cloud systems right up to the vehicles, and to derive a comprehensive safety concept from this.

Erik Lesser
Chief Product Owner
Robert Bosch GmbH

Name: Robert Bosch GmbH
Domain: Electronics and Information Technology
Headquarters: Gerlingen, Germany
Number of Employees: 410,000 (2018)