Fraunhofer IESE

HITACHI
Inspire the Next

SAFETY ENGINEERING FOR VEHICLES OF HIGHER AUTOMATION LEVELS

OUT COMPETENCIES AND SOLUTIONS

- Safety engineering and safety architectures
- Safety standards and standard creation initiatives
- safeTbox

YOUR BENEFITS

- External reflection on your current safety engineering process for vehicles of higher automation levels
- Transfer of the results of current scientific and industry discussions and upcoming safety standards into your process

WHAT IT IS ABOUT

Before safety-critical systems can be released on the market, it must be guaranteed that the risk associated with them does not exceed an acceptable level. Safety standards provide appropriate specifications and represent the state of the practice in terms of assurance. However, in vehicles of higher automation levels, the established standards, techniques, and methods are not readily applicable or inadequate. Accordingly, both new and extended standards as well as new and extended safety engineering techniques and methods are required. Hitachi has therefore decided to rely on the expertise of the Fraunhofer Institute for Experimental Software Engineering IESE. The institute has competencies and project experience in the field of Safety Engineering for Vehicles of Higher Automation Levels. Furthermore, IESE is involved in and connected to ongoing standardization initiatives in this field.

The cooperation with Fraunhofer IESE regarding a multi-aspect safety engineering method with safeTbox brought about substantial success for Hitachi R&D. We implemented the design method of the functional architecture for autonomous driving systems and analyzed the safety aspect simultaneously.
Many thanks for the effort.

Dr. Shiro Yamaoka
Department Manager
Control Platform Research Dept.
Center for Technology Innovation
- Controls Hitachi, Ltd. Research & Development Group

THE CHALLENGE

The relevant standard for the assurance of functional safety in vehicles is ISO 26262. However, this standard was created with conventional, not with automated vehicles in mind, and is therefore not sufficient for implementing adequate safety engineering for highly automated or even autonomous vehicles. Upcoming standards such as the Safety-Of-The-Intended-Functionality (SOTIF) ISO PAS 21448 initiative attempt to close the gap between the safety engineering currently supported by safety standards and the safety engineering needed for the release of vehicles of higher automation levels. However, it is neither guaranteed that the scope of SOTIF will be sufficient to close that gap nor does a safety engineering process currently exist that includes the necessary safety considerations for vehicles of higher automation levels.

THE SUPPORT

In a joint research cooperation, researchers of Hitachi and Fraunhofer IESE have investigated the necessary scope for future safety engineering and how current safety standards and standard creation initiatives address this necessary scope. Based on the results of this investigation, an initial process and methodology for multi-aspect safety engineering with tool support from our safeTbox tool was developed. The results of this project were presented at the International Conference on Computer Safety, Reliability & Security (SafeComp) – one of the most important conferences in the safety engineering community – in Sweden in 2018. Sharing the results with the research community enabled critical reflection on them and contributed to building awareness for the full problem scope of Safety Engineering for Vehicles of Higher Automation Levels.

THE RESULT

The joint research activity enables Hitachi and Fraunhofer IESE to anticipate the contents of upcoming safety standards in the field of automated vehicles and to address these contents with a tool-supported methodology.

Name: Hitachi Ltd.

Website: hitachi.com

Industry: Electronics and Information Technology

Headquarters: Tokyo, Japan

Number of Employees: 35,631 (2017)

Contact

Dr. Daniel Schneider
Department Head Embedded Systems
Quality Assurance (ESQ)
Phone +49 631 6800-2187
daniel.schneider@iese.fraunhofer.de

www.iese.fraunhofer.de