Fraunhofer IESE

HITACHI
Inspire the Next

SAFETY ENGINEERING FÜR FAHRZEUGE MIT HÖHEREM AUTOMATISIERUNGS-GRAD

UNSERE KOMPETENZEN UND LÖSUNGEN

- Safety Engineering und Safety-Architekturen
- Sicherheitsnormen und Initiativen zur Schaffung solcher Normen
- safeTbox

DER KUNDENNUTZEN

- Externe Betrachtung Ihres gegenwärtigen Safety-Engineering-Prozesses für Fahrzeuge mit höherem Automatisierungsgrad
- Transfer der Ergebnisse aktueller Diskussionen in Wissenschaft und Industrie sowie künftiger Sicherheitsnormen in Ihren Prozess

UM WAS ES GEHT

Bevor sicherheitskritische Systeme in Verkehr gebracht werden können muss gewährleistet werden, dass das mit ihnen assoziierte Risiko ein akzeptables Maß nicht übersteigt. Sicherheitsnormen machen entsprechende Vorgaben und repräsentieren den Stand der Praxis bezüglich der Absicherung. Bei Fahrzeugen mit hohen Automatisierungsgraden ist es jedoch so, dass die etablierten Normen, Techniken und Methoden nicht ohne weiteres anwendbar sind beziehungsweise nicht ausreichen. Es werden entsprechend sowohl neue und erweiterte Normen als auch neue und erweiterte Techniken und Methoden des Safety Engineering benötigt. Deshalb entschloss sich Hitachi dazu, auf die Expertise des Fraunhofer-Instituts für Experimentelles Software Engineering IESE zu vertrauen. Das Institut verfügt über Kompetenzen und Projekterfahrung im Bereich Safety Engineering für Fahrzeuge mit höherem Automatisierungsgrad. Außerdem ist das Fraunhofer IESE in laufenden Normungsinitiativen in diesem Bereich involviert.

Die Kooperation mit dem Fraunhofer IESE bezüglich einer multiaspektuellen Safety-Engineering-Methode mit safeTbox hat zu erheblichem Erfolg für Hitachis F&E geführt. Wir haben die Entwurfsmethode der funktionalen Architektur für autonom fahrende Systeme umgesetzt und gleichzeitig den Sicherheitsaspekt analysiert.
Vielen Dank für die Arbeit.

Dr. Shiro Yamaoka
Abteilungsleiter
Abteilung Control Platform Research Center for Technology Innovation - Controls Hitachi, Ltd. Research & Development Group

DIE HERAUSFORDERUNG

Die relevante Norm hinsichtlich der Gewährleistung der funktionalen Sicherheit von Fahrzeugen ist die ISO 26262. Diese wurde jedoch im Hinblick auf klassische nicht automatisierte Fahrzeuge erstellt und reicht daher nicht aus, um ein adäquates Safety Engineering für hochautomatisierte oder gar autonome Fahrzeuge umzusetzen. Künftige Normen wie die Initiative Safety-Of-The-Intended-Functionality (SOTIF) ISO PAS 21448 machen den Versuch, diese Lücke zwischen dem derzeit von Sicherheitsnormen unterstützten Safety Engineering und dem für die Zulassung von Fahrzeugen mit höherem Automatisierungsgrad erforderlichen Safety Engineering zu schließen. Allerdings ist weder gewährleistet, dass der Umfang von SOTIF für die Schließung dieser Lücke ausreichend sein wird, noch gibt es aktuell einen Safety-Engineering-Prozess, der die notwendigen Sicherheitsüberlegungen für Fahrzeuge mit höherem Automatisierungsgrad enthält.

DIE UNTERSTÜTZUNG

In einer gemeinsamen Forschungskooperation haben Forscher von Hitachi und Fraunhofer IESE den erforderlichen Umfang für zukünftiges Safety Engineering erforscht und untersucht, wie aktuelle Sicherheitsnormen und Initiativen zur Schaffung solcher Normen diesen adressieren. Basierend auf den Ergebnissen dieser Untersuchung wurden ein erster Prozess und eine Methodik für multiaspektuelles Safety Engineering mit Werkzeugunterstützung durch unser Tool safeTbox entwickelt. Die Resultate dieses Projekts wurden 2018 im Rahmen eines Vortrags bei der International Conference on Computer Safety, Reliability & Security (SafeComp) – einer der wichtigsten Konferenzen in der Safety Engineering Community – in Schweden präsentiert. Der Austausch der Ergebnisse mit der Forschungsgemeinschaft ermöglichte eine kritische Reflexion über diese und trug zur Schärfung des Bewusstseins für den vollen Problembereich des Safety Engineering für Fahrzeuge mit höherem Automatisierungsgrad bei.

DAS ERGEBNIS

Dank der gemeinsamen Forschungsaktivitäten können Hitachi und Fraunhofer IESE nun die Inhalte künftiger Sicherheitsnormen im Bereich automatisierter Fahrzeuge vorhersagen und diese mithilfe einer werkzeuggestützten Methodik adressieren.

Name: Hitachi Ltd.

Website: hitachi.com

Branche: Elektronik und Informationstechnologie

Zentrale: Tokio, Japan

Anzahl Mitarbeiter: 35.631 (2017)

Kontakt

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

www.iese.fraunhofer.de