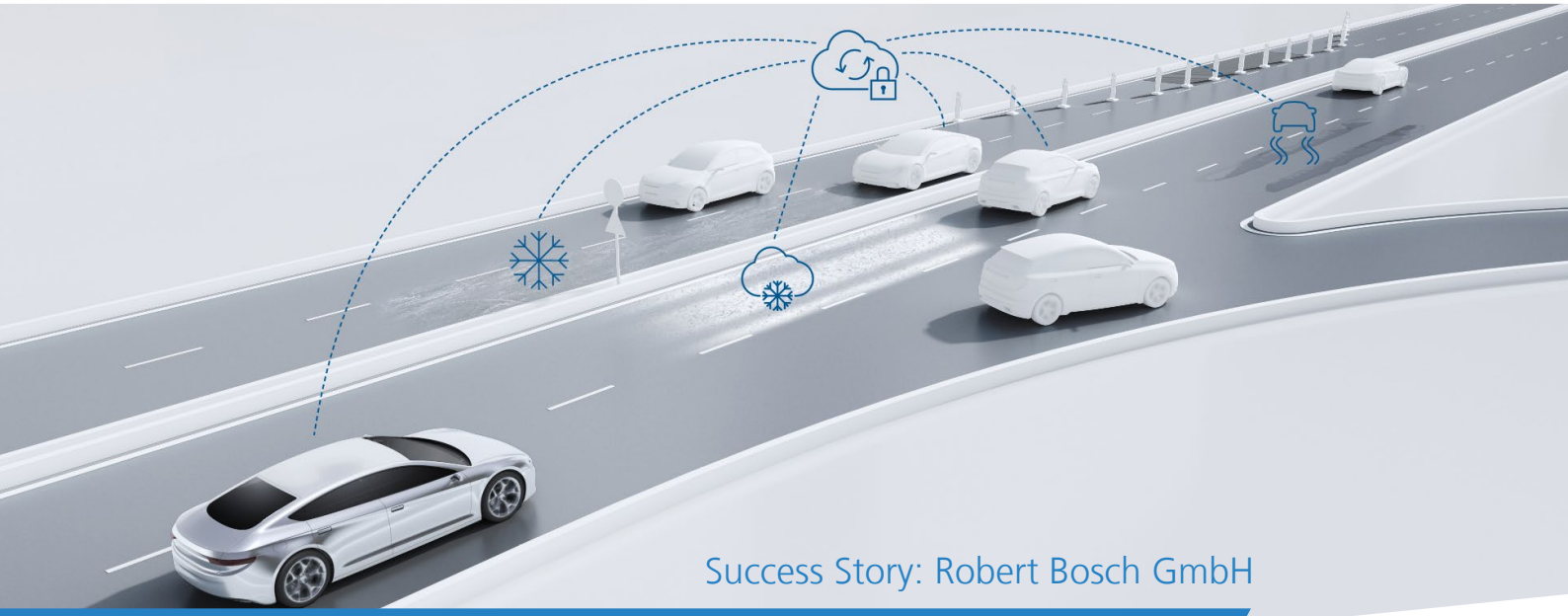
Fraunhofer IESE

BOSCH



Success Story: Robert Bosch GmbH

SAFETY-BETRACHTUNGEN EINES CLOUD-DIENSTES FÜR AUTOMATISIERTES FAHREN

UNSERE KOMPETENZEN UND LÖSUNGEN

- Safety-Analysen und Safety-Konzeptentwicklung
- Sicherheitsnormen und Initiativen zur Schaffung solcher Normen
- safeTbox – Werkzeugrahmenwerk des Fraunhofer IESE zur Unterstützung in Phasen der Entwicklung und Zertifizierung von sicherheitskritischen Systemen

DER KUNDENNUTZEN

- Externe Betrachtung von Cloud-Diensten für Fahrzeuge mit höherem Automatisierungsgrad
- Transfer der Ergebnisse aktueller Diskussionen in Wissenschaft und Industrie sowie künftiger Sicherheitsnormen in den Prozess des Kunden

UM WAS ES GEHT

In Zukunft wird das automatisierte Fahren zunehmend durch Cloud-Dienste unterstützt: Die Sensorik eines Fahrzeugs hat nur eine begrenzte Reichweite und ist teuer, weshalb zukünftig Fahrzeuge über die Cloud mit Informationen versorgt werden. Diese Informationen können von anderen Fahrzeugen kommen, aber auch von anderen Quellen wie Wetteranbietern.

In diesem Projekt mit Bosch ging es ebenfalls um einen Cloud-Dienst: Dieser informiert den Autobahnpiloten über die Straßenwetterverhältnisse und den Haftreibwert der Straße. Autobahnpiloten sind auf diese Information angewiesen, da ihr Einsatzbereich und ihr Fahrverhalten von der Reibung abhängen. Für diesen Cloud-Dienst ein Sicherheitskonzept zu entwickeln – trotz fehlender Normen für Safety-Belange im Automotive-Bereich – war die Herausforderung für die Experten des Fraunhofer IESE.

Die Kooperation mit dem Fraunhofer IESE war für uns wegweisend für das Safety Engineering unserer Cloud-Dienste. Die modellbasierten Analysetechniken haben es uns ermöglicht, die komplette Wirkkette von Sensoren über verschiedene Cloud-Systeme bis in die Fahrzeuge hinein systematisch zu untersuchen und daraus ein umfassendes Sicherheitskonzept abzuleiten.

Erik Lesser
Chief Product Owner
Robert Bosch GmbH

DIE HERAUSFORDERUNG

Es gibt bislang noch keine Norm, die erklärt, wie Cloud-Dienste für Autobahnpiloten zu entwickeln sind. Die Sicherheitsnorm ISO 26262 und der Safety-Of-The-Intended-Functionality (SOTIF) Standard ISO PAS 21448 beziehen sich auf Fahrzeuge, doch ihre Anwendung ist nicht ohne Weiteres auf Cloud-Dienste übertragbar. Normen aus der IT-Sicherheit adressieren zwar Cloud-Dienste, aber nicht die Safety-Belange aus dem Automotive-Bereich.

Nur weil es keine Norm gibt, heißt dies aber nicht, dass man solche Dienste entwickeln kann, wie man möchte. Man sollte sich trotzdem an den Stand der Technik halten, auch wenn dieser nicht in einer einzigen Norm zu finden ist.

DIE UNTERSTÜTZUNG

Die Forscher des Fraunhofer IESE kennen den Stand der Technik sowie aktuelle Entwicklungen im Bereich Safety und automatisiertes Fahren. Basierend auf diesem Hintergrundwissen stellten sie im Projekt mit Bosch relevante Anforderungen aus Normen zusammen und zeigten auf, wie man diese methodisch umsetzen kann.

Weiterhin unterstützte das Fraunhofer IESE Bosch bei der methodischen Umsetzung. In enger Kooperation mit den Domänenexperten von Bosch entwickelten sie eine funktionale Architektur, welche die komplette Informationsverarbeitung darstellt. Anschließend analysierte das Team die einzelnen Verarbeitungsschritte mit Komponentenfehlerbäumen. Außerdem führten sie eine Sicherheitsanalyse bezüglich der Cloud-Plattform durch, auf dem die von Bosch entwickelte Software läuft. Basierend auf den Analyseergebnissen leiteten die Fraunhofer-Experten ein Sicherheitskonzept ab und erstellten eine Sicherheitsargumentation mit der Goal Structuring Notation (GSN). Alle Artefakte modellierten sie mit safeTbox, dem vom Fraunhofer IESE entwickelten Werkzeugrahmenwerk zur Unterstützung in Phasen der Entwicklung und Zertifizierung von sicherheitskritischen Systemen. Die modellierten Artefakte lassen sich aufgrund ihres modularen Charakters leicht an verschiedene Kundenwünsche anpassen.

DAS ERGEBNIS

Als Projektergebnis erhielt Bosch ein umfassendes Sicherheitskonzept für seinen speziellen Cloud-Dienst. Die Vorgehensweise sowie die angewendeten Methoden und Tools sind aber ohne Weiteres auf andere Cloud-Dienste übertragbar. Somit liefert das Projekt auch einen modellbasierten Safety-Engineering-Ansatz für Cloud-Dienste und den Grundstein für einen bisher fehlenden Standard.

Name:
Robert Bosch GmbH

Website:
https://www.bosch-mobility-solutions.com/en/products-and-services/passenger-cars-and-light-commercial-vehicles/automated-driving/predictive-road-condition-services/

Branche:
Elektronik und Informationstechnologie

Zentrale:
Gerlingen, Deutschland

Anzahl Mitarbeiter:
410 000 (2018)

Kontakt

Dr.-Ing. Rasmus Adler
Programm-Manager Autonome Systeme
Telefon +49 631 6800-2172
rasmus.adler@iese.fraunhofer.de
www.iese.fraunhofer.de
www.bosch.de