Technische Universität Braunschweig

Sicherheitskonzept

Betrieb fahrerloser Fahrzeuge

unicaragil

Sicherheitsaspekte

- **Verhaltenssicherheit:** Nach außen sichtbares Verhalten des Systems im Straßenverkehr
- **Funktionale Sicherheit** (insbesondere ISO 26262)
- **Gebrauchssicherheit**
- **IT-Security**
- **Passive Sicherheit**

(Vgl. Waymo (2018). Waymo Safety Report – On the Road to Fully Self-Driving)

Sicherheitsaktivitäten in UNICAR*agil*

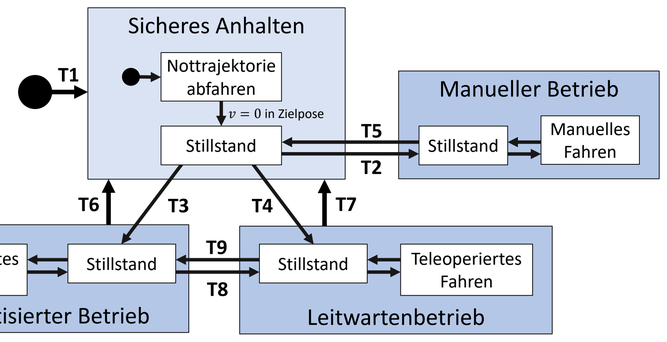
- Realisierung ganzheitlicher Konzepte durch Aufteilung relevanter Sicherheitsschwerpunkte im Projekt, z.B.:
  - RWTH Aachen: **Fail-safe Dynamik-Module**, Simulative Strukturvalidierung
  - TU Darmstadt: **Modulare Absicherung**, **Sicheres Anhalten** und **fähigkeitenbasierte Streckenfreigabe**
  - Universität Stuttgart: Funktional **sicheres Fahrzeug-netzwerk** (Energie & Daten), **ausfallsicheres Stammhirn**
  - Universität Passau: **IT-Security**

TU Braunschweig: **Sicherheitskonzept für das Gesamtfahrzeug**

- Sicherheitsanalysen für den Betrieb der Fahrzeuge
  - Städtische Umgebung & Vielzahl möglicher Strecken
  - Abbildung vorliegender Unsicherheiten in Anforderungen an Hardware und Software
  - Synergien zwischen Anwendungsfällen durch gemeinsame Fahrfunktion und weitere geteilte Komponenten
- Dokumentation in der Entwicklung und in den Prototypen umgesetzter Anforderungen und Sicherheitsmechanismen

Item Definition der Fahrfunktion

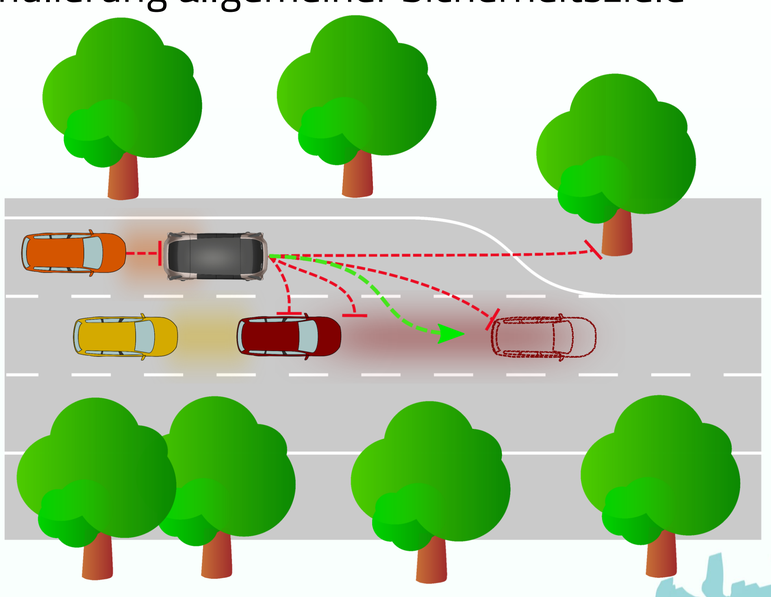
- Fahrfunktion in großem Maße sicherheitsrelevant: Übergang der Verantwortung vom Menschen auf das technische System
- Beschreibung der Betriebsmodi und Funktionsgrenzen



- Festlegung der erwarteten Einsatzumgebung
- Vorstellung abgestimmter besonders relevanter Betriebsszenarien für anschließende Sicherheitsanalysen

Gefährdungsanalysen

- **Technologieunabhängige Gefährdungsidentifikation:** Betrachtung generischen Fehlerverhaltens in repräsentativen Betriebsszenarien
- Bewertung der Risiken
- Formulierung allgemeiner Sicherheitsziele



Kontakt

Robert Graubohm, Torben Stolte & Markus Maurer
Technische Universität Braunschweig, Institut für Regelungstechnik
{graubohm,stolte,maurer}@ifr.ing.tu-bs.de

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung