Deutsches Forschungszentrum für Künstliche Intelligenz GmbH

SATISFY

Validierung von Safety- und Security-Anforderungen in autonomen Fahrzeugen

Motivation

Eine zentrale Herausforderung des autonomen Fahrens ist die Gewährleistung der Sicherheit aller Beteiligter. Dies betrifft sowohl den Schutz der Umgebung vor Fehlverhalten des Fahrzeugs (Safety) als auch der Schutz des Fahrzeugs vor unbefugten Manipulationen von außen (Security). Beide Aspekte sind nicht unabhängig voneinander, sondern sind häufig miteinander eng verzahnt: Manipulationen im Fahrzeug können zum Ausfall einzelner Komponenten und damit zum Fehlverhalten des Fahrzeugs führen; umgekehrt können auftretende Fehler in Programmkomponenten dem Angreifer erst die Möglichkeit eröffnen, Manipulationen im Fahrzeug vorzunehmen.

Vorhaben

Der Standort Bremen (CPS) arbeitet im Rahmen des BMBF-Verbundprojekts SATiSFy an Methoden und Techniken, um bereits im Entwicklungsstadium Safety- und Security-Anforderungen sowohl auf Hardware- als auch auf Softwareebene gesamtheitlich erfassen und formal überprüfen zu können, um vor einer finalen Systemintegration eine verlässliche Sicherheits-aussage für die gesamte Entwicklung treffen zu können.

Hierbei wird ein Rahmenwerk für sicherheitsrelevante IT-Architekturen entwickelt, um die verschiedenartigen Sicherheitsanforderungen entweder frühzeitig beim Entwurfsprozess oder auch dynamisch zur Systemlaufzeit überprüfen zu können. In manchen Fällen müssen Sicherheitsanforderungen zunächst auch in Einzelanforderungen dekomponiert werden, um dann einzeln statisch oder dynamisch verifiziert zu werden. Existierende Sicherheitsarchitekturen werden dahingehend modifiziert und in den Gesamtkontext des Rahmenwerks integriert, dass über sie durch formale Argumente und Komposition eine hinreichende Aussage über die erreichte Sicherheit, Resilienz bzw. das Restrisiko gegenüber absichtlichen Angriffen und unabsichtlichen Einwirkungen getroffen werden kann.

Projektlaufzeit: 05/2018 – 04/2021

Partner:

BOSCH

KASPER OSWALD
Ingenieure für innovative Sicherheitslösungen

HOOD GROUP

EBERHARD KARLS UNIVERSITÄT TÜBINGEN

Gefördert durch:

Bundesministerium für Bildung und Forschung

Kontakt:
DFKI GmbH
Cyber-Physical Systems

Projektleiter: Dr. Daniel Große
Telefon: +49 421 218 63935
E-Mail: daniel.grosse@dfki.de
Internet: www.dfki.de