FORSCHUNG KOMPAKT

Mehr Sicherheit beim autonomen Fahren

Vertrauen in automatisierte Systeme

Autos autonom fahren lassen? Den im Auto verbauten Sensoren erlauben, Daten über den aktuellen Gesundheitszustand des Fahrers zu sammeln? Die meisten Menschen sind hier sehr zögerlich. Im Projekt SECREDAS erhöht ein Forscherkonsortium, darunter das Fraunhofer-Institut für Experimentelles Software Engineering IESE, die Sicherheit solcher Systeme – um auf diesem Weg das allgemeine Vertrauen in die Technik zu stärken.

Bei der Akzeptanz neuer Technologien wie selbstfahrender Autos ist noch viel Überzeugungsarbeit zu leisten: Lebendigen Fahrern traut man üblicherweise bessere Entscheidungen im Straßenverkehr zu als einer Software. Das Vertrauen in solche vernetzten automatisierten Systeme in Mobilität und Medizin zu stärken – sei es in puncto Sicherheit oder hinsichtlich des Datenschutzes – und europäische Erstausrüster wettbewerbsfähig zu halten, hat sich das Konsortium des Projekts »Product security for cross domain reliable dependable automated systems SECREDAS« zum Ziel gesetzt. Insgesamt 69 Partner aus 16 europäischen Ländern beteiligen sich an dem Projekt, darunter auch das Fraunhofer-Institut für Experimentelles Software Engineering IESE. Die EU finanziert das Projekt mit rund 15 Millionen Euro, das Gesamtvolumen des Projekts beträgt 51,6 Millionen Euro.

Sicherheit selbstfahrender Autos erhöhen

Bei autonom fahrenden Autos spielen neuronale Netze bei der Steuerung und Situationserkennung eine immer größere Rolle. Ist die Ampel rot? Kreuzt ein anderes Fahrzeug den geplanten Fahrweg? Die Schwierigkeit dabei: Auf welche Art und Weise die neuronalen Netze ihre Entscheidungen treffen, lässt sich nicht bis ins Detail nachvollziehen. »Wir entwickeln daher einen Safety Supervisor, der die Entscheidungen des neuronalen Netzes live überwacht, sodass auf Basis dieser Bewertungen notfalls regulierend eingegriffen werden kann«, sagt Mohammed Naveed Akram, Wissenschaftler am Fraunhofer IESE. »Dieser Supervisor basiert auf Algorithmen, die sich klassische Ansätze zunutze machen. Über diese erfassen wir nicht die Gesamtsituation wie die neuronalen Netze, sondern kritische Eckpunkte. Im Rahmen des SECREDAS-Projekts beschäftigen wir uns vor allem mit der Frage nach geeigneten Metriken; die Einleitung geeigneter Gegenmaßnahmen zur Kontrolle des Risikos ist Gegenstand weiterführender Arbeiten.«

Wie das genau vonstattengeht, lässt sich am besten an einem Beispiel erklären, etwa an einer Kreuzung. Das neuronale Netz ist darauf ausgelegt, die Gesamtsituation zu

Kontakt
Janis Eitner | Fraunhofer-Gesellschaft, München | Kommunikation | Telefon +49 89 1205-1333 | presse@zv.fraunhofer.de
Claudia Reis | Fraunhofer-Institut für Experimentelles Software Engineering IESE | Telefon +49 631 6800-92296 | Fraunhofer-Platz 1 | 67663 Kaiserslautern | www.iese.fraunhofer.de | claudia.reis@iese.fraunhofer.de

erfassen: Welche Vorfahrtregeln gelten, ist die Ampel rot oder grün, befinden sich Fußgänger innerhalb des Gefahrenbereichs, kreuzen andere Autos den geplanten zukünftigen Fahrweg? Dies können die Algorithmen des Safety Supervisors zwar nicht, doch setzen sie stattdessen auf bestimmte Metriken. Solche wären beispielsweise die »General-time-to-collision (GTTC)«, also die Zeit bis zu einem Zusammenprall unter Berücksichtigung der voraussichtlichen Trajektorie oder die »Worst Case Impact Speed«-Metrik zur Beurteilung der Schadensschwere auf Basis der voraussichtlichen Kollisionsgeschwindigkeit. Steuert das Auto nun auf einen anderen Verkehrsteilnehmer zu, welcher dem neuronalen Netz entgangen sein sollte, erkennen die Algorithmen des Safety Supervisors, dass der Abstand zu den anderen Verkehrsteilnehmern in gefährlichem Maße schrumpft. Sie können das Kommando übernehmen und bremsen das Auto, falls die autonome Steuerung versagt. »Wir haben verschiedene Metriken untersucht: Wie gut können wir über diese die aktuelle Gefahrenlage bewerten?«, sagt Akram. In einer Simulation haben die Forscherinnen und Forscher die Tauglichkeit dieser Metriken für verschiedene Gefahrensituationen evaluiert. Das Ergebnis kann sich sehen lassen. »Der Ansatz, die neuronalen Netze über klassische Ansätze jederzeit und live zu überprüfen, kann zusammen mit einem dynamischen Risikomanagement die Sicherheit deutlich erhöhen«, fasst Akram zusammen.

Mehr Datenschutz oder mehr Service?

Hat ein anderer Fahrer das Auto genutzt, heißt es vielfach: Sitz und Spiegel wieder passend einstellen, die eigene Lieblingsmusik heraussuchen, die persönlichen Lieblingsorte im Navigationssystem eintragen und ähnliches – erst dann kann es losgehen. Zwar ist es möglich und praktisch, solche Angaben abzuspeichern, sodass automatisch alle Einstellungen passen. Doch während einige Menschen dies gerne nutzen, scheuen andere aus Gründen des Datenschutzes davor zurück. Noch heikler wird es, wenn das Auto auch medizinische Daten erfasst, etwa den Blutzuckerspiegel oder die Herzfrequenz – um im Bedarfsfall eine entsprechende Warnung an den Fahrer auszugeben oder Hilfe zu holen. Denn für den Nutzer ist bisher kaum nachzuvollziehen, ob die Daten im Auto bleiben oder in einer Cloud verarbeitet werden. »One-fits-it-all ist hier daher kaum eine Lösung«, sagt Arghavan Hosseinzadeh da Silva, Software-Entwicklerin am Fraunhofer IESE. »Generell gilt: Je mehr Daten man freigibt, desto mehr Service erhält man. Wie viele Daten jemand in welchem Fall freigeben möchte, ist von Mensch zu Mensch jedoch sehr unterschiedlich.«

Unter dem Namen »IND²UCE« (Produktname: MYDATA Control Technologies) entwickeln die Forscherinnen und Forscher daher ein Framework, über das sich die Nutzung aller persönlichen Einstellungen je nach Situation und Belieben einschränken lässt. Man möchte die Whatsapp-Nachrichten gerne auf dem Display des Autos angezeigt bekommen – es sei denn, man ist nicht alleine im Auto? Im Mietauto sollen die gleichen Kontakte und Playlists angezeigt werden wie im eigenen Fahrzeug und Sitz, Lenkrad und Spiegel direkt passend eingestellt sein? Die Gesundheitsdaten, etwa die Messung der Herzfrequenz, sollen im Auto verbleiben und nicht an eine Cloud geschickt werden – es sei denn, es ist dringende Hilfe geboten, die dann automatisch

herbeigerufen werden soll, etwa nach einem Unfall? Solche Dinge soll der Nutzer künftig über eine App selbst einstellen können, und diese Privacy-Vorgaben werden per Smartphone in jedes Fahrzeug übertragen, das der Anwender gerade nutzt, egal ob Dienstwagen, Mietfahrzeug oder Privatwagen.

Die erforderlichen Framework-Komponenten dazu werden ins Auto integriert. Eine Anfrage – beispielsweise, ob die Daten über die Herzfrequenz des Nutzers an die Cloud gesendet werden dürfen – läuft zunächst über den »Policy Decision Point PDP«. Dieser prüft, ob sie zulässig ist. Falls ja, sendet der PDP eine Freigabe an das »Enforcement« oder aber gibt diesem die Information, welche Daten vor dem Verschicken zu löschen oder zu anonymisieren sind. Im Rahmen von SECREDAS wollen die IESE-Forscherinnen und -Forscher einen Prototypen für das Framework entwickeln, Ende 2020 soll er fertig sein. Langfristig möchte das SECREDAS-Konsortium einen Standard für Datennutzungskontrolle im Auto etablieren, der möglichst von allen Autoherstellern übernommen werden soll, um die informationelle Selbstbestimmung der Fahrzeugnutzer zu ermöglichen.

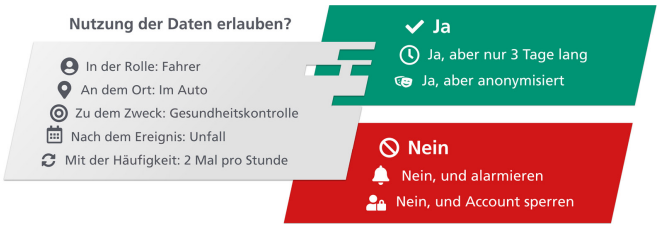

Abb. 1 Ein neuartiges System entscheidet, welche Daten in welchem Fall wohin weitergegeben werden dürfen.

© Fraunhofer IESE